ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
6-бөлім
Тұтастық негіздері

Информационная технология
ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ
Основы безопасности для открытых систем
Часть 6
Основы целостности

ҚР СТ ИСО/МЭК 10181-6-2008

(ИСО/МЭК 10181-6:1996 «Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелерге арналған қауіпсіздік негіздері. Тұтастық негіздері», IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті (Мемстандарт)

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ

Ашық жүйелерге арналған қауіпсіздік негіздері
6-бөлім
Тұтастық негіздері

ҚР СТ ИСО/МЭК 10181-6-2008
(ИСО/МЭК 10181-6:1996 «Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелерге арналған қауіпсіздік негіздері. Тұтастық негіздері», IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасы Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитетінің 2007 жылғы 25 ақпандағы № 107-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт Қазақстан Республикасы экономикасының қажеттіліктерін білдіретін қосымша талаптар мәтін бойынша көлбеу қаріппен белгіленіп ИСО/МЭК 10181-6:1996 “Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелерге арналған қауіпсіздік негіздері. Тұтастық негіздері” («Information technology. Open Systems Interconnection. Security frameworks for open systems. Integrity framework»), IDT халықаралық стандартына балама.

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

Осы *ҚР СТ ИСО/МЭК 10181* “Ақпараттық технология. Ашық жүйелердің өзара әрекеттесуі. Ашық жүйелерге арналған қауіпсіздік негіздері. Тұтастық негіздері” стандарты мынандай бөлімдерден тұрады:

– I Бөлім. Шолу

– 2 Бөлім. Сәйкестендіру негіздері

– 3 Бөлім. Мүмкіндікті басқару негіздері

– 4 Бөлім. Бас тартпаушылық негіздері

– 5 Бөлім. Құпиялық негіздері

– 6 Бөлім. Тұтастық негіздері

– 7 Бөлім. Қауіпсіздік оқиғаларын есепке алу және оперативтік баяндау негіздері

Көптеген ашық жүйелерді пайдалану кезінде деректердің тұтастығымен анықталатын қорғаныс талаптары пайда болады. Осындай нұсқаулықтардың ішіне басқа қорғаныс қызметтерін (мысалы, “қаскүнем” өзгертуге талпыныс жасаған кезде олардың тиімділігі азаятын немесе жойылатын сәйкестендіру, мүмкіндікті басқару, құпиялық, қорғанысты тексеру және авторлықты растау) қамтамасыз ету кезінде қолданылатын деректер қорғанысы кіруі мүмкін.

Заңсыз кіру кезіндегі деректердің өзгермеу және сақталу қасиеті тұтастық деп аталады.

Осы стандарт тұтастық қызметтерін қамтамасыз етуге арналған жалпы негіздерді белгілейді.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
6-бөлім
Тұтастық негіздері

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт ашық жүйелер ортасында қорғаныс қызметтері жұмыс істеуі туралы мәселелерді қамтиды, осы ретте “ашық жүйелер” түсінігінің ішіне деректер базасы, бөлінген қосымшалар, ашық бөлінген өңдеу және OSI секілді салалар кіреді. Қорғаныс негіздері ішкі жүйелер мен нысандарға арналған қорғанысты қамтамасыз ету құралдары белгіленуімен, және де жүйелер арасындағы өзара байланыстармен байланысты. Қорғаныс негіздері жүйелерді құру әдістемесіне және олардың тетіктеріне қатысы жоқ.

Қауіпсіздіктің негізгі ережелері белгілі бір қорғаныс қызметтерін алу үшін қолданылатын деректердің элементтерін және операциялардың кезектілігін (бірақ, хаттаманың элементтерін емес) қамтиды. Бұл қызметтер жүйелердің коммуникативтік нысандарына, және де жүйелер арасындағы алмасу деректері мен жүйелерді басқару деректеріне қатысты болуы мүмкін.

Осы стандарт:

– деректер тұтастығының негізгі тұжырымдамасын;

– деректердің тұтастығын қамтамасыз ету тетіктерінің ықтималды класстарын;

– деректердің тұтастығын қамтамасыз ету тетіктерінің әр классына арналған құралдарды;

– деректердің тұтастығын қамтамасыз ету тетіктерінің осы классын қолдауға қажетті басқару процедураларын;

– деректердің тұтастығын қамтамасыз ету тетігі мен қолдау қызметтерінің басқа қорғау қызметтерімен және тетіктермен өзара әрекеттесуін белгілейді.

Осы стандарт түрлі стандарт түрлерімен қолданылуы мүмкін, оның ішіне мыналар кіреді:

1) тұтастық тұжырымдамасын қамтитын стандарттар;

2) абстрактты сервистік құралдарды, оның ішінде деректердің тұтастығын қамтамасыз ету құралдарын сипаттайтын стандарттар;

3) тұтастықты қамтамасыз ету сервистік құралдары қолданылуын сипаттайтын стандарттар;

4) ашық жүйе сәулетінің шегінде тұтастықты қамтамасыз ету құралдарын сипаттайтын стандарттар;

5) деректердің тұтастығын қамтамасыз ету тетіктерін сипаттайтын стандарттар.

Осы аталған стандарттар осы стандартты мынандай түрде қолданылуы мүмкін:

– 1), 2), 3), 4) және 5) түріндегі стандарттар осы стандарттың терминологиясын қолдана алады;

– 2), 3), 4) және 5) түріндегі стандарттар 7-бөлімде сипатталған құралдарды пайдалана алады;

– 5) түріндегі стандарттар 8-бөлімде көрсетілген тетік класстарына негізделуі мүмкін.

Осы қорғаныс негіздерінде сипатталған кейбір процедуралар криптографиялық әдістердің көмегімен деректердің тұтастығын қамтамасыз етуге қабілетті. Бұл негіздер нақты криптографиялық немесе басқа да стратегиялар қолданылуына тәуелді, бірақ, тұтастық тетіктерінің белгілі бір класстары стратегияның өзгеше қасиеттеріне тәуелді болуы мүмкін. *Ақпаратты криптографиялық қорғаудың нақты түрлерін таңдау және қолдану Қазақстан Республикасының заңнамасымен регламенттеледі.*

Ескертпе – ИСО криптографиялық стратегияларды стандарттамайтынына қарамастан, ол *[6]* стандартында тіркелген процедураларды стандарттайды.

Осы стандартта сипатталған деректер тұтастығы деректер мәндерінің тұтастығымен белгіленеді. Бұл түсінік (деректер мәндерінің тұрақтылығы) деректер мәндерінің түрлі көрсетулері (мысалы, ASN.1 мәнінің түрлі кодталуы) баламалы болып түсінілетін деректер нұсқаларының барлығын қамтиды. Басқа өзгеру формалары болмайды.

Осы стандартта деректер элементтерінің қолданылуы деректер құрылымдарының барлық түрлерін (мысалы, файлдар немесе деректер жиынтықтары, ақпараттық кезектіліктер, файл жүйелері және деректер базасы) қамтиды.

Осы стандартта сипатталған негіздер ықтималы «қаскүнемдер» тарапынан болатын жазулар қорғалған болып есептелетін деректер тұтастығы қамтамасыз етілуін қамтиды. Сондықтан, мүмкіндікті басқаруға ғана негізделмеген криптографиялық және криптографиялық емес арнайы тетіктер арқылы тұтастық қамтамасыз етілуіне негізгі назар аударылады.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ ГОСТ Р ИСО/МЭК 7498-1:1994 Ақпараттық технология. Ашық жүйелердің өзара әрекеттесуі. Базалық эталондық үлгі. 1-Бөлім. Базалық модель.

ҚР СТ ИСО/МЭК 10181-1:1996 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ашық жүйелердің өзара әрекеті. Ашық жүйелердің қауіпсіздік негіздері. 1-Бөлім. Шолу.

ҚР СТ ИСО/МЭК 10181-2:1996 Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелердің қауіпсіздік негіздері. 2-Бөлім. Сәйкестендіру негіздері.

ҚР СТ ИСО/МЭК 10181-3:1996 Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелердің қауіпсіздік негіздері: құрылым. - Бөлім. Мүмкіндікті басқару негіздері.

ГОСТ ИСО 7498-2-2002 Ақпараттық технология. Ашық жүйелердің өзара әрекеттесуі. Базалық эталондық үлгі. 2 Бөлім. Ақпаратты қорғау сәулеті.

3 Терминдер мен анықтамалар

Осы стандартта ҚР *СТ ГОСТ Р ИСО/МЭК 7498-1, ҚР СТ ИСО/МЭК 10181-1, ҚР СТ ИСО/МЭК 10181-2-2008,* ГОСТ ИСО 7498-2 бойынша терминдер, сондай-ақ сәйкес анықтамаларымен мынадай терминдер қолданылады.

3.1 Тұтастық қорғалған деректер (integrity-protected data): Тұтастық қорғалған орта шегіндегі деректер және соларға қатысты атрибуттар.

3.2 Қорғалған қайта құру (shield): Қарапайым деректерді тұтастығы қорғалған деректерге қайта құру.

3.3 Тұтастық қорғалатын арна (integrity-protected channel): Тұтастықты қамтамасыз құралдар қолданылатын байланыс арнасы.

Ескертпе – Байланыс арналарына арналған тұтастықты қамтамасыз ету қызметінің екі түрі ГОСТ ИСО 7498-2 стандартында көрсетілген. Осы қызмет түрлері (қосылыс және қосылыс орнатылмаған тұтастық) А қосымшасында сипатталған.

3.4 Кері қорғалған қайта құру (unshield): Қорғалған деректерді бастапқы экрандалған деректерге қайта құру.

3.5 Дұрыстығын тексеру (validate): Тұтастық жоғалуын табу мақсатында тұтастығы қорғалған деректерді тексеру.

3.6 Тұтастық қорғалған орта (integrity-protected environment): Заңсыз дерек өзгертулер (оның ішінде деректер жасау және өшіру) болдырмайтын және анықталатын орта.

4 Қысқартулар

Осы стандартта мынадай қысқартулар белгіленген:

4.1 Ашық жүйелердің өзара әрекеті (OSI, Open System Interaction); АЖБ.

4.2 Хаттамалық деректер блогы (Protocol Data Unit); PDU.

4.3 Сервистік деректер блогы (Service Data Unit); SDU.

4.4 Тұтастықты қорғап қайта құруға арналған ақпарат (Shield Integrity Information); SII.

4.5 Тұтастықтағы өзгерістерді табуға арналған ақпарат (Modification Detection Integrity Information); MDII.

4.6 Тұтастықты кері қорғап қайта құруға арналған ақпарат (Unshield Integrity Information); UII.

5 Тұтастық негіздері

Тұтастықты қамтамасыз ету қызметінің мақсаты – төменде көрсетілген түрлі тәсілдермен қауіп-қатерге ұшыратылуы мүмкін деректердің және соларға қатысты атрибуттардың тұтастығын қорғау:

– заңсыз деректерді түрлендіру;

– заңсыз деректерді өшіру;

– заңсыз деректер жасау;

– заңсыз деректер енгізу;

– заңсыз деректерді көшіру.

Тұтастықты қамтамасыз ету қызметтері осы факторлардың алдын алу немесе қалпына келтірумен немесе онсыз тауып, олардан деректерді қорғайды. Егер қажетті басқару ақпаратында (мысалы, кілттер және SII) тұтастық және/немесе құпиялық қорғалуы болмаса, тұтастықтың тиімді қорғалуы мүмкін емес; осындай қорғаныс деректерді қорғау механизміне енгізілген принциптерден басқа принциптерге негізделген.

Тұтастықты қорғау түсінігі деректерді заңсыз жасаудан және/немесе өшіруден қорғауды қамтитына туралы идеяға назар аудару үшін осы негіздерде қорғалған орталар түсінігі қолданылады. Сөйтіп, деректерді заңсыз жасау/өшіру белгілі бір қорғалған ортаны заңсыз жаңарту ретінде қарастырылады. Сол секілді, деректерді енгізу немесе көшіру құрылымдалған деректер жиынтығын (мысалы, ақпарат кезектілігін немесе деректер құрылымын) жаңарту ретінде қарастырылады.

Деректердің кейбір өзгеруі олардың тұтастығына ешбір әсер етпейтін болып қарастырылатынын атап өту керек. Мысалы, ASN.1 сипаттамасында белгілі бір түрдегі деректер ЖИНАҒЫ болса, осы түрдегі деректердің компоненттері қайта реттелгенінде ешқандай тұтастық бұзылуы жоқ. Тұтастықты қамтамасыз ететін күрделі тетіктер құрылымдалған деректердің кейбір қайта құрылуы деректердің тұтастығына қауіпті еместігін көрсетуі мүмкін. Ондай тетіктер пломбалаған немесе таңбалы деректерді сәйкесінше электронды қолтаңбаларды қайталап есептеу немесе қайталап нығыздау қажеттігісіз қайта құруға мүмкіндік береді.

Тұтастықты қамтамасыз ету қызметтерінің мақсаты – ақпаратты заңсыз жаңартулардан, оның ішінде деректерді заңсыз жасаудан және

өшіруден қорғау, және де осындай заңсыз жаңартуларды табу. Деректердің тұтастығын қамтамасыз ету қызметі орындалуының қамтамасыз етілуі мынандай қызмет түрлерімен жүзеге асырылады:

– **қорғалған қайта құру**: қарапайым деректерді тұтастығы қорғалған деректерге қайта құру;

– **дұрыстығын тексеру**: тұтастық жоғалуын табу мақсатында тұтастығы қорғалған деректерді тексеру;

– **кері қорғалған қайта құру**: қорғалған деректерді бастапқы қарапайым деректерге қайта құру.

Бұл қызмет түрлері криптографиялық әдістерді қолдануы міндетті емес. Егер ондай әдістер қолданылған болса, олар деректер өзгеруін шақыруы міндетті емес. Мысалы, **қорғалған қайта құру** операциясын деректерге мөр немесе электронды қолтаңба қосу арқылы қамтамасыз етуге болады. Бұл жағдайда сәтті **дұрыстығын тексеруден** кейін **кері қорғалған қайта құру** мөрді/электронды қолтаңбаны жою жолымен орындалады.

Тұтастықты қамтамасыз ету қызметі ақпараттық іздеу, деректердің орнын ауыстыру және басқару үшін мынандай түрде қолданылады:

1) OSI ортасында орны ауыстырылатын ақпарат үшін, тұтастықты қамтамасыз ету қызметтері (N)-қызмет деректер жөнелту циклін қалыптастыру мақсатында **қорғалған қайта құру**, (N-1)-құралы қолданылуымен деректердің орын ауыстыру және **кері қорғалған қайта құру** біріктірілуімен қамтамасыз етіледі.

2) Деректерді сақтау және іздеу үшін, тұтастықты қамтамасыз ету қызметтері **қорғап қайта құру** және ақпаратты сақтау функциясын іздеу және **кері қорғалған қайта құру** функциясын біріктірілуімен қамтамасыз етіледі**.**

Қорғалған қайта құру да, кері қорғалған қайта құру да осындай деректері (мысалы, барлық (N)-қосылу деректері) бар қатарлас операциялар ретінде қамтамасыз етілуі мүмкін, олар бір уақытта **қорғалған қайта құруға** ұшырамаған бөліктерден, тұтастығы қорғалған деректер ретінде белгіленген бөліктерден және **кері қорғалған қайта құруға** ұшыраған бөліктерден тұруы мүмкін.

Тұтастықты қамтамасыз ету тетіктері қорғалған орталарды қолдайды, яғни, **қорғап қайта құру** және **кері қорғап қайта құру** кезеңдерінің ішіне қорғалған орталар арасында деректердің орнын ауыстыру кіреді. Егер тұтастығы қорғалған деректер бір тұтастықты қамтамасыз ету механизмімен қорғалған ортадан басқасына жіберілген болса, деректер қорғалуының үзіліссіздігін қамтамасыз ету мақсатында екінші механизмнің **қорғап қайта құрылуы** бірінші механизмнің **кері қорғап қайта құрылуынан** бұрын жүзеге асырылуы керек.

5.1 Негізгі тұжырымдамалар

Тұтастықты қамтамасыз ету қызметтерінің бірнеше түрлері қандай қызмет түрлері (деректерді жасау, өшіру, жаңарту, енгізу және/немесе қалпына келтіру) қамтылғанына қарай, немесе деректердің тұтастығы бұзылуының алдын алу әлде тек ғана оларды табу қажет етілуіне қарай және тұтастық бұзылғаны табылған жағдайда олар деректер қалпына келтірілуін қолдайтындығына қарай түрлендіріледі. Деректердің тұтастығын қамтамасыз ету қызметтерінің түрлері 5.2. тармағында сипатталған.

Осы қызметтерді қамтамасыз ету құралдары ретінде қолданылуы мүмкін тетіктер жасалынған тұтастықты бұзуларға негізделген жүйелі қызметтің деңгейіне қарай кең ауқымды категорияларға бөлінуі мүмкін. Осы тетіктердің түрлері 5.3. тармағында сипатталған.

5.2 Тұтастықты қамтамасыз ету қызметтерінің түрлері

Деректердің тұтастығын қамтамасыз ету қызметтері мынандай категориялар бойынша жіктеледі:

1) Олар қорғайтын деректердің тұтастығын бұзу түрі. Бұзылыс түрлері:

– заңсыз деректерді жаңарту;

– заңсыз деректерді жасау;

– заңсыз деректер өшіру;

– заңсыз деректер енгізу;

– заңсыз деректерді қалпына келтіру болып табылады.

2) Олар қолдайтын қорғаныс түрі. Қорғаныс түрлері:

– тұтастық бұзылысының алдын алу;

– тұтастық бұзылуын табу болып табылады.

3) Осындай қызметтер қалпына келтіру тетіктерін қамтитына/қамтымайтынына қарай:

Бірінші жағдайда (қалпына келтірілуімен), деректердің дұрыстығын тексеру операциясы деректер бұзылуы пайда болғанын көрсеткен сайын кері қорғап қайта құру операциясы алғашқы деректерді қалпына келтіру (және, мүмкін, қорғаныс аудиті мақсатында қалпына келтіру немесе қате туралы хабарлау) мүмкіндіктеріне ие болуы мүмкін.

Соңғы жағдайда (қалпына келтірусіз), деректердің дұрыстығын тексеру операциясы деректер бұзылуы пайда болғанын көрсеткен кезде кері қорғап қайта құру операциясы алғашқы деректерді қалпына келтіруге қабілетсіз болады.

5.3 Тұтастықты қамтамасыз ету тетіктерінің түрлері

Әдетте, деректерді қорғау қабілеті қолданылған ортаға тәуелді болады. Кейбір құралдарды өз табиғаты бойынша қауіпсіздендіру қиын (ауыспалы дерек тасығыштар немесе байланыс құралдары), нәтижесінде құқығы жоқ

тұлғалар деректерге мүмкіндік алып, оларды өз қалауы бойынша өзгерте алады. Ондай құралдар үшін тұтастықты қамтамасыз ету механизмінің мақсаты - өзгертулерді тауып, мүмкіндігінше бұзылған деректерді қалпына келтіру. Төменде деректердің тұтастығын қамтамасыз ету тетіктерінің мысалдары тізілген:

1) Ортаға кіру мүмкіндігін болдырмайтын тетіктер. Ондай тетіктердің ішіне мыналар кіреді:

– шуылдан қорғалған оқшауланған арналар;

– маршруттауды басқару;

– мүмкіндікті басқару.

2) Деректер немесе деректер элементтерінің кезектілігі заңсыз жаңартылуын, оның ішінде деректер заңсыз жасалуын, жойылуын және қосарлануын табу тетіктері. Ондай тетіктердің ішіне мыналар кіреді:

– мөрлеу;

– электронды қолтаңбалар;

– деректерді қосарлау (басқа бұзылыс түрлерімен күресу құралы ретінде қолданылады);

– цифрлы бармақ таңбасы криптографиялық қайта құрулармен бірге;

– хабарлардың реттік нөмірлері.

Қорғаныс тиімділігі терминдерінде бұл тетіктер мынандай түрде жіктелуі мүмкін:

– қорғаныс болмауы;

– деректер жаңартылуын және жасалуын табу;

– деректер жаңартылуларын, жасалуларын, жойылуын және қосарлануларын табу;

– деректер қалпына келуімен бірге жаңартылуын және жасалуын табу;

– деректер қалпына келуімен бірге жаңартылуын, жасалуын, өшірілуін және қосарлануын табу.

5.4 Тұтастық бұзылуының қаупі

Қамтамасыз етілетін қызметтердің терминдерінде тұтастық бұзылуының қауіптері мынандай болуы мүмкін:

1) Деректерін бұзылыстарын болдырмау арқылы олардың тұтастығын қолдайтын орталарда деректердің рұқсатсыз жасалуы/жаңартылуы/ жойылуы/ енгізілуі/көшірілуі.

Мысал – Қорғалған арнаға қосылу.

2) Деректерін бұзылыстарын табу арқылы олардың тұтастығын қамтамасыз ететін орталарда деректердің рұқсатсыз және табылмайтын жасалуы/жаңартылуы/жойылуы/енгізілуі/көшірілуі.

Мысал – деректердің тұтастығы [8] стандартында сипатталғандай, қорғалған деректер және соларға сәйкес бақылаулы сомаларды шифрлануымен қамтамасыз етілуі мүмкін. Егер қатынастағы А және В нысандар кодтау операциясын қолдау үшін бір кілтті қолданатын болса, және деректердің шығу

тегінде тұтастық қорғалмаса, А-дан В-ге берілген тұтастығы қорғалған деректер кейін А нысанына шыққан көзі В нысаны болып ұсынылуы мүмкін (тұтастықты бұзу әрекеттерін қайтару).

Деректері тұрақты орналасқан орталардың терминдерінде тұтастық бұзылуының қауіптері мынандай болуы мүмкін:

– ішінде деректер қорғалған ортаға қатысы барлар;

– ішіне деректер берілген ортаға қатысы барлар;

– ортадан тәуелсіздер.

Осы стандартта тұтастық бұзылуын заңсыз әрекеттер ретінде қарастыратындықтан, ол Б Қосымшасында сипатталғандай, деректердің сыртқы келісушілігін бұзуы мүмкін рұқсат етілген жаңарту мәселелерін қарастырмайды (мысалы, бұзылыстар есепке алынуы). Яғни, осы стандарттың осы бөлімі, құпиялық негіздеріне қарағанда, ішкі бұзылыстар мәселелерін қамтымайды (құпиялық негіздері ақпарат үзіліссіз қорғалуына қатысты мәселелерді, мысалы, рұқсат етілген мүмкіндікке қасақана немесе кездейсоқ заңсыз құпиялығы қорғалуы ақпарат ашылуы еріп жүретін мүмкіндікке қатысты мәселелерді қамтиды).

5.5 Тұтастық қорғалуын бұзу әрекеттерінің түрлері

Жоғарыда тізілген әр тұтастық бұзылуы қауіпіне бер немесе одан көп шабуыл, яғни қарастырудағы қауіпті жүзеге асыру әрекеттері сәйкес келеді. Осындай шабуылдардың мақсаты – тұтастықты қамтамасыз ету механизмін (тетіктерін) бұзу, және олар мынандай түрлерге бөлінеді:

1) криптографиялық тетіктерді бұзуға немесе осындай тетіктердің босаң жақтарын пайдалануға бағытталған шабуылдар. Олардың ішіне мыналар кіреді:

– криптографиялық тетіктің ішіне ену;

– (іріктеп) өшіру және қосарлау.

2) Қолданыстағы контексттік тетікті (нақты уақытта нақты орналасуда контекстті тетікті ауыстыру деректерін) бұзуға бағытталған шабуылдар. Олардың ішіне мыналар кіреді:

– дерек элементтерінің көшірмелерін көлемді үйлесімді өзгерту;

– контексті орнату тетігінің ішіне кіру.

3) Бұзылыстарды табу және жою тетіктерін бұзуға бағытталған шабуылдар, олардың ішіне мыналар кіреді:

– жалған бұзылыстар;

– бұзылыс тетігі мен алынған деректер өңделуі арасында қате кезектілікті пайдалану.

4) Бұзылыстардың алдын алу тетіктерін бұзуға немесе өзіне тартуға бағытталған шабуылдар. Олардың ішіне мыналар кіреді:

– тікелей тетікке жасалған шабуылдар;

– тетікке қызмет көрсету жеріне ену;

– қасақана емес жанама әсерлері бар кәдеге жаратуларды пайдалану.

6 Тұтастықты қамтамасыз ету саясаты

Тұтастықты қамтамасыз ету саясаты – жүйені қорғау стратегиясының бөлігі, ол тұтастықты қамтамасыз ету қамтамасыз етумен және пайдаланумен байланысты.

Тұтастығы қорғалған деректер жүйенің нысандары оларды жасайтын, өзгертетін және жоятын бақылауға ұшырайды. Яғни, тұтастықты қамтамасыз ету стратегиясы осындай бақылауға ұшыраған деректерді сәйкестендіріп, деректер жасауды, өзгертуді немесе жоюды қолдауға арналған нысандарды белгілеуі керек.

Түрлі типті деректердің тұтастылығының салыстырмалы маңыздылығына қарай тұтастықты қамтамасыз ету саясаты деректердің әр түріне тұтастықты қамтамасыз ету сервистерін қолдау үшін пайдаланылуы керек тетіктер түрі мен санын көрсете алады.

Тұтастықты қорғау стратегияларын басқару осы стандартта қарастырылмайды.

6.1 Саясатты таныстыру

Тұтастықты қамтамасыз ету стратегияларын көрсету үшін іске қосылған ақпарат пен жүйенің нысандарын сәйкестендіру құралдары талап етіледі.

Қорғау стратегиясы ережелер жинағы ретінде қарастырылуы мүмкін. Әр тұтастықты қамтамасыз стратегиясының ережесі деректердің, нысанның сипаттамаларын, және де деректерге жасалатын рұқсат етілген операциялар түрлерін (әдетте, ол деректерді жасау, өзгерту және жою) байланыстыруы мүмкін. Кейбір стратегияларда ол ережелер анық белгіленбеген, бірақ стратегия көрсетулерінен алынуы мүмкін.

Келесі бөлімшелер тұтастықты қамтамасыз ету стратегиясын сипаттауға болатын көптеген тәсілдерді сипаттайды. Кейбір тұтастық тетіктері белгілі бір стратегия көрсетулерінде ұқсас болуы мүмкіндігіне қарамастан, стратегияны сипаттау тәсілі белгілі бір механизм стратегияны жүзеге асыру үшін қолданылуын қарастырмайды.

6.1.1 Деректердің сипаттамалары

Стратегия деректерді түрлі тәсілдермен сәйкестендіруі мүмкін, мысалы:

– деректерді жасауға/жоюға рұқсаты бар нысандарды сәйкестендіру;

– олардың рұқсаты бойынша;

– ішінде деректер көрсетілген контекстті сәйкестендіру (мысалы, берілген қызмет бойынша).

6.1.2 Нысан сипаттамалары

Тұтастықты қамтамасыз ету стратегиясы қолданылатын нысандарды сипаттау тәсілдері көп. Төменде екі негізгі мысал келтірілген.

6.1.2.1 Ұқсастылық негізінде құрылған стратегиялар

Стратегияны көрсетудің осы формаларында нысандар жеке сәйкестендіріледі, немесе баламалы нысандар тобының бөлігі ретінде сәйкестендіріледі (тұтастықты қамтамасыз ету стратегиясының мақсатында), немесе олар орындайтын қызметпен сәйкестендіріледі. Сөйтіп, деректермен операциялар орындау рұқсат етілген әр нысанның жеке сәйкестігі, топтық сәйкестігі немесе атқарымдық сәйкестігі болады, ол осы нысанды сипаттау үшін қолданылады.

Қызметтерге қатысты тұтастықты қамтамасыз ету стратегиясы әр нысанның мүмкіндігі бар функциялардың ерекше топтарын белгілей алады, сол арқылы түрлі топтардағы функциялар бір уақытта талап етілуі мүмкін.

6.1.2.2 Рөлдік модельге негізделген стратегиялар

Стратегияларды көрсету формаларының осысында атрибуттар тұтастығы қорғалған әр нысанға және әр нысан элементіне қатысты. Нысандардың және деректердің белгілерімен жұмыс істейтін ғаламдық ережелер рұқсат етілген әрекеттерді белгілейді. Ережелерге негізделген стратегиялар қорғаныс негіздері шолуында екжей-текжейлі талқыланған (*ҚР СТ ИСО/МЭК 10181-1* қараңыз).

7 Ақпарат және тұтастықты қамтамасыз ету құралдары

Осы бөлім тұтастықты қамтамасыз ету қызметтерін дұрыс орындау үшін, және де қарастырудағы ақпаратты пайдаланатын немесе қалыптастыратын құралдар үшін қажетті ақпаратты жіктейді.

7.1 Тұтастық туралы ақпарат

Деректерді қорғап қайта құруды, дұрыстық тексерілуін немесе кері қорғап қайта құруды қамтамасыз ету үшін қосымша ақпарат тартылуы мүмкін. Бұл қосымша ақпарат тұтастық туралы ақпарат ретінде таныс. Тұтастық туралы ақпарат мынандай түрде жіктелуі мүмкін.

7.1.1 Тұтастықты қорғап қайта құруға арналған ақпарат

Тұтастықты қорғап қайта құруға арналған ақпарат (SII) – деректерді қорғап қайта құруға арналған ақпарат. Осындай ақпараттың мысалдары:

– жеке кілттер;

– құпия кілттер;

– стратегияның сәйкестендіргіші және соған қатысты криптографиялық параметрлер;

– уақытта өзгеретін параметрлер (мысалы, уақыт таңбалары).

7.1.2 Тұтастықтағы өзгерістегі табуға арналған ақпарат

Тұтастықтағы өзгерістегі табуға арналған ақпарат (MDII) – тұтастығы қорғалған деректердің дұрыстығы тексерілуін қамтамасыз ету үшін қолданылатын ақпарат. Осындай ақпараттың ішіне мыналар кіреді:

– жалпы рұқсаттағы кілттер;

– құпия кілттер.

7.1.3 Тұтастықты кері қорғап қайта құруға арналған ақпарат

Тұтастықты кері қорғап қайта құруға арналған ақпарат (UII) – тұтастығы қорғалған деректердің кері қорғап қайта құрылуын қамтамасыз ету үшін қолданылатын ақпарат. Осындай ақпараттың ішіне мыналар кіреді:

– жалпы рұқсаттағы кілттер;

– құпия кілттер.

7.2 Тұтастықты қамтамасыз ету құралдары

Тұтастықты қамтамасыз ету құралдарының көпшілігі В қосымшасында көрсетілген. Олар атқарымдық аспектілерге және басқару аспектілеріне қатысы бар құралдарға бөлінуі мүмкін.

7.2.1 Жұмыспен байланысты құралдар

Олар мынандай құралдар:

1) қорғап қайта құру

Бұл құрал деректердің тұтастығын қорғау үшін қолданылады. Енгізілетін ақпараттың ішіне мыналар кіруі мүмкін:

– қорғанысқа арналған деректер;

– SII;

– тұтастықты қамтамасыз ету тетіктерін белгілейтін сәйкестендіргіштер, мысалы, В Қосымшасында аталған.

Шығатын ақпараттың ішіне мыналар кіруі мүмкін:

– тұтастығы қорғалған деректер;

– аяқтау/қайтару кодтары.

2) деректердің дұрыстығын тексеру

Бұл құрал тұтастығы қорғалған деректерде өзгерістер болған-болмағанын тексереді. Енгізілетін ақпараттың ішіне мыналар кіруі мүмкін:

– тұтастығы қорғалған деректер;

– - MDII;

– тетікті белгілейтін сәйкестендіргіштер, мысалы, В Қосымшасында аталған.

Шығатын ақпараттың ішіне мыналар кіруі мүмкін:

– деректер тұтастығы бұзылуына қатысты көрсетілімдер.

3) кері қорғалған қайта құру

Бұл құрал тұтастығы қорғалған деректерді алғашқыда *қорғап қайта құруға* ұшыратылған деректерге қайта құрады.

Ықтималды енгізілетін ақпараттың ішіне мыналар кіруі мүмкін:

– тұтастығы қорғалған деректер;

– MDII;

– С қосымшасында көрсетілгендей нақты тетікті белгілейтін сәйкестендіргіштер.

Ықтималды шығатын ақпараттың ішіне мыналар кіреді:

– деректер;
– аяқтау/қайтару кодтары.

7.2.2 Басқарумен байланысты құралдар

Тұтастықты басқару құралдары пайдаланушыға деректердің тұтастығын қамтамасыз ету үшін қажетті ақпаратты (мысалы, кілттерді) алуға, жаңартуға және жоюға мүмкіндік береді. Кең мағынада бұл құралдарың арнауы:

– басқару ақпаратын орнату;
– басқару ақпаратын түрлендіру;
– басқару ақпаратын жою;
– басқару ақпаратының тізімін жасау;
– басқару ақпаратын блоктау;
– басқару ақпаратының блогын ашу.

8 Тұтастықты қамтамасыз ету тетіктерінің жіктелуі

Бұл бөлім тұтастықты қамтамасыз ету қызметтерін жүзеге асыру үшін қолданылатын құралдармен тұтастық тетіктерін жіктейді.

8.1 Криптографиялық әдістермен тұтастықты қамтамасыз ету

Тұтастықты қамтамасыз ету криптографиялық тетіктерінің екі классы бар, олар төменде қарастырылады:

1) симметриялық криптографиялық әдістерге негізделген тұтастықты қамтамасыз ету тетіктері, оларда деректерді қорғап қайта құру үшін қолданылған кілтті білу арқылы деректердің дұрыстығын тексеруге болады;

2) асимметриялық криптографиялық әдістерге негізделген тұтастықты қамтамасыз ету тетіктері, оларда деректерді қорғап қайта құру үшін қолданылған жеке кілтке сәйкес келетін жалпы рұқсат етілген кілтті білу арқылы деректердің дұрыстығын тексеруге болады.

Тетіктердің бірінші түрі деректерді мөрлеуге сәйкес келеді, ал екінші түріндегі тетіктер электронды қолтаңбаларға сәйкес келеді.

Түрлі уақыт параметрлері деректерді көшіруден қорғау үшін криптографиялық әдістерге негізделген тұтастық тетіктерімен бірге қолданылуы мүмкін.

8.1.1 Мөрлеу арқылы тұтастықты қамтамасыз ету

Мөрлеу қорғауға жататын деректерге криптографиялық бақылау көрсеткішін қосу арқылы тұтастықты қамтамасыз етеді. Мөрлеу кезінде бір кілт қорғаныс үшін де, деректердің тұтастығын тексеру үшін де қолданылады. Егер тұтастықты қамтамасыз ету тетіктерінің осы түрі қолданылған болса, деректердің дұрыстығын тексеру құралдарының барлық әлеуеті алдын-ала белгілі болады, немесе оларда құпиялы кілтке мүмкіндік құралы болуы керек.

Деректерді мөрлеуге қабілетті нысандардың жиынтығы, және деректердің дұрыстығын тексеруге қабілеті бар нысандар жиынтығы механизмнің анықтауы бойынша сәйкес келетін болып табылады.

Ондай тетік жаңартулар табылуын мынандай түрде қамтамасыз етеді:

– *Қорғап қайта құру* тұтастықты қорғауға жататын деректерге криптографиялық бақылау көрсеткішін қосу арқылы жүзеге асырылады (мысалы, біржақты қызмет қорғалатын деректер бойынша есептелді, сол мағына шифрлау тетігінің көмегімен қайта құрылады).

– *Деректердің дұрыстығын тексеру* криптографиялық бақылау көрсеткіші және құпиялы кілті бар деректер қолданылуы арқылы жүзеге асырылады (мысалы, белгілі бір құрал деректер мен құпиялы кілтті қорғап қайта құру функциясының әсеріне ұшыратады, алынған мөр деректерге берілген мағынамен салыстырылады). Егер ол мағына тура келсе, ондай деректер жаңартылмаған ретінде қарастырылады.

– *Кері қорғап қайта құру* криптографиялық бақылау көрсеткішін жою арқылы жүзеге асырылады, егер деректердің дұрыстығын тексеру кемінде бір рет жасалынған болса.

8.1.2 Электронды қолтаңбалар көмегімен тұтастықты қамтамасыз ету

Электронды қолтаңбалар жеке кілт және ассиметриялық криптографиялық алгоритм қолданылуымен есептеледі. Қорғап қайта құруға ұшыратылған деректердің (электронды қолтаңба қосылған деректердің) дұрыстығы сәйкес жалпы рұқсаты бар кілт қолданылуымен тексерілуіне болады. Жалпы алғанда, жалпыға рұқсат етілген кілт барлық пайдаланушылар үшін рұқсат етілген болып жасалуы мүмкін.

Электронды қолтаңбалар еркін мөлшері және құрамы бар деректердің *дұрыстығын тексере* алатын нысандар жиынтығын пайдалануға мүмкіндік береді.

Бұл тетік жаңарту табылуын мынандай түрде қолдайды:

– *Қорғап қайта құру* деректерге тұтастықты қорғау мақсатында криптографиялық бақылау деректері берілуі арқылы жүзеге асырылады (мысалы, қорғауға жататын деректерге компьютерленетін цифрлы бармақ таңбасы беріліп, алынған мағына электронды қолтаңбаны құрайтын бір немесе бірнеше мағыналар жасау үшін жеке кілтке және, мүмкін, басқа да параметрлерге қосылады).

– *Дұрыстықты тексеру* алынған мәліметтердің бармақ таңбасы, электронды қолтаңба және электронды қолтаңбаны тексеру алгоритмі бар жалпыға рұқсат кілт қолданылуы арқылы жүзеге асырылады. Егер электронды қолтаңба аудиті қате тапса, оған сәйкес деректер өзгеріске ұшыраған болып қарастырылады.

– *Кері қорғап қайта құру* деректердің дұрыстығы тексерілгеннен кейін криптографиялық бақылау көрсеткішін жою арқылы жүзеге асырылады.

Бұл тетік, оған қоса, алғашқы аутентификация және берілетін ақпараттың өзгерместігі режимдерін қолдай алады.

8.1.3 Артық деректерді шифрлау арқылы тұтастықты қамтамасыз ету

Артық деректердің (мысалы, кәдімгі сөздің) тұтастығы шифрлау арқылы қамтамасыз етілуі мүмкін. Құрамына қателерді іздеу кодтары мен цифрлы бармақ таңбалары кіретін деректер артық болып табылады, және олардың тұтастығы шифрлау арқылы қорғалуы мүмкін (осы ретте қолданыстағы шифрлау стратегиясы шифрланған деректер дешифрлаудан кейін алғашқы деректерге әсер етуін болдырмауы шарт).

Төменгі деңгейдегі қорғаныс хаттамалары (*[8], [9]* қараңыз)

Бұл механизм ақпарат өзгеруі табылуын мынандай түрде қамтамасыз етеді:

1) Қорғап қайта құру артық деректерді шифрлау арқылы жүзеге асырылады.

2) Дұрыстықты тексеру қорғап қайта құруға ұшыраған деректерді декодтау, және олар алғашқы деректерді қанағаттандыратын қандай да болмасын түрлендірулерге сәйкес келетіндігін анықтау арқылы жүзеге асырылады.

Мысалдар:

– егер алғашқы деректер ASCII форматындағы символдар кезектілігі болып табылса, қалпына келтірілген деректердің дәл сондай сипаттамалары болуы керек;

– егер алғашқы деректер, жорамалға сәйкес, осы тілдегі адам сөзі ретінде қарастырылатын болса, қалпына келтірілген деректер сол тілде сөйлейтін адамдардың көпшілігіне түсінікті болу үшін керек (немесе минималды жаңартулармен қайта құрылуы керек);

– егер алғашқы деректердің құрамында бақылау самалары бар болса, қорғалған деректер бөлігі үшін сондай бақылау сомаларын есептеп, нәтижелер декодталған деректерге енгізілген бақылау сомаларының мағынасына сәйкес келуін тексеру керек.

3) Кері қорғап қайта құру шифрланған деректерді декодтау арқылы орындалады.

Ескертпе – Сипатталған тетік, біз білетініміздей, кең тараған шифрлау тәсілдерімен (мысалы деректер тізбегі қалыптастырылуымен немесе онсыз DES (деректерді шифрлау стандарты) түріндегі блоктық шифрлау) бірге қолданылатын кейбір кең тараған артықтық формаларына (мысалы, қателер іздеу кодтары бар деректерге) сай емес болып табылады. Ықтималды қақпандардың қарапайым мысалы мынандай.

Егер ASCII тексті (мысалы, электронды пошта) DES-кодтау көмегімен қорғалуы керек болса, хабарландыруға ұзындығын кесу арқылы табылмайтын өзгертулер енгізілуі мүмкін (егер, әрине, поштаның басында, әдеттегідей, деректер кезектілігі ұзындығының индикаторы болмаса).

8.2 Контексттің көмегімен тұтастықты қамтамасыз ету

Тұтастық бір немесе бірнеше алдын-ала келісілген контексттерде деректерді сақтау немесе жіберу тетіктерінің көмегімен қамтамасыз етілуі мүмкін. Осындай тетіктер деректерді де, деректердің құрылымдарын да

(мысалы, деректер модельдерінің кезектіліктерін) қорғай алады. Олардың ішіне мыналар кіреді:

8.2.1 Деректерді қосарландыру

Тұтастық тетіктерінің осы классы деректерді уақытта (мысалы, зейіннің бірнеше салаларында) немесе уақытта (мысалы, түрлі уақытта) қосарландыруға негізделген. Ықтималды «қаскүнемдер» көшірмелердің шектелген санынан көбісіне қатер туғыза алмайды, және шабуылдар анықталған сайын деректер түпнұсқалы көшірмелерден қалпына келтіріледі деп қабылданады.

Мысал ретінде, осындай тетік шабуылдарға төзімді деректер базаларымен қолданылуы мүмкін.

Бұл тетіктер қалпына келтіру арқылы тұтастық өшірілуі табылуын қамтамасыз етеді және басқа да қорғаныс құралдарымен бірге қолданылуы мүмкін. Олар деректердің тұтастығын мынандай түрде қамтамасыз етеді:

– Қорғап қайта құру бір уақытта немесе зейіннің түрлі салаларында бір деректердің бір қатар көшірмелерін жасау жолымен жүзеге асырылады.

– Дұрыстықты тексеру әр берілген уақытта немесе әр берілген орында көшірмелер жинаумен қамтамасыз етіледі. Олар салыстырылады, және барлығы барабар болмаса, тұтастық бұзылған болып есептеледі.

– Кері қорғап қайта құру (қалпына келтірумен бірге) белгілі бір алдын-ала белгіленген критерийге қол жеткізілген болса (мысалы, «мағыналар 90 және одан көп пайызға сәйкес келуі»), белгілі бір берілген мағынаны (мысалы, қате қалпына келтіру ықтималдығы) минимумдайтын дұрыс мағынаны таңдау арқылы жүзеге асырылады.

Осы ретте атап өту қажет, барлық мағыналар алғашқы мағынамен үйлесетін болса, және осы жағдайда осы параметрді минимумдайтын мағына жалпы қабылданған мағына болса, қалпына келтірудің қажетті критерийіне қол жеткізілуі керек.

8.2.2 Алдын ала келісілген контекст

Бұл тетіктер тұтастығы қорғалған деректер өшірілуі табылуын қамтамасыз етеді және жиі басқа да тетіктермен бірге қолданылады:

– *Қорғап қайта құру* деректер жаңартылуының берілген деңгейінің шегінде белгілі бір уақытта және/немесе белгілі бір орналастырылуымен деректер беру арқылы жүзеге асырылады.

– *Дұрыстықты тексеру* белгілі бір уақытта және/немесе белгілі бір орналастырылуымен деректерді күту арқылы жүзеге асырылады. Егер ол болмаса, тұтастық бұзылған болып есептеледі.

Баламалы деректердің ауыстырылуын болдырмау үшін бұл механизм, жоғарыда аталғандай, басқа да тұтастықты қамтамасыз ету тетіктерімен біріктірілуі керек.

8.3 Бұзылыстарды табу және растау арқылы тұтастықты қамтамасыз ету

Бұл тетіктер оңды кері байланысы бар идемпотентті операцияларды орындау кезінде тұтастық табылуын пайдаланады (бір операцияның бірнеше ойдағыдай орындалуы бір нәтиже берген болса, операция идомпотентті болып есептеледі). Осындай тетіктердің мысалдары - оңды растауы бар операциялардың орны ауыстырылуы (мысалы, *[7]* стандартында сипатталған 4 көлік классы) және кері байланыспен дистанциялық операциялар. Бұл тетіктер қорғап қайта құру және дұрыстықты тексеру/кері қорғап қайта құру процедуралары бір уақыт ұзақтығымен жұмыс істейді және деректерді сақтауға жарамайды деп қарастырады:

– *Қорғап қайта құру* тұтастықты қамтамасыз ету стратегиясында басқа нұсқамалар болғанша дейін немесе оңды расталғанға дейін бір әрекеттерді қайталау жолымен жүзеге асырылады.

– *Дұрыстықты тексеру* қорғап қайта құруға ұшыраған әр дерек нұсқасы үшін орындалады (тұтастықты қамтамасыз ету стратегиясында басқа нұсқамалар болмаса); дұрыстықты ойдағыдай тексерулер қорғап қайта құру операциясын орындайтын нысан үшін оңды растаулар қалыптастырылуына әкеп соғады.

Әрекеттегі тұтастықты қорғау механизмі қолданылған кезде кері қорғап қайта құруға ұшыраған деректерден дұрыс ақпарат жіберу үшін түзету орындау мүмкін болса, осы тетіктің кері қорғап қайту құруы оңды растауды қалыптастыра алады.

Егер дұрыстықты тексеру теріс нәтиже берген болса (немесе деректер жаңартылса не өшірілсе), қорғап қайта құру операциясының теріс растауы кезінде тиімділік төмендеуі мүмкін.

Бұл тетіктер деректердің жаңартылуы басқа құралдар қолданылған кезде табылуы мүмкін деп болжайды, яғни, бұл тетіктер деректер жаңартылуынан қорғау құралдарын кеңейту ретінде қарастырылуы мүмкін.

8.4 Бұзылыстардың алдын алу арқылы тұтастықты қамтамасыз ету

Тұтастықты сақтаудағы деректерге және ақпаратты жіберу құралдарына мүмкіндіктерді болдырмау арқылы, және де ақпаратқа мүмкіндікті басқару көмегімен қамтамасыз етуге болады.

Мүмкіндіктерді болдырмау құралдарының сипаттамасы осы негіз әрекет етуі аясынан ішіне кірмейді. Мүмкіндікті басқару мүмкіндікті басқару құрылымында сипатталған.

9 Басқа да қызметтермен және қорғаныс тетіктерімен байланысу

Бұл бөлім басқа қорғаныс қызметтері мен тетіктер деректердің тұтастығын қамтамасыз ету үшін қолданылуын сипаттайды. Деректердің

тұтастығын басқа қорғаныс қызметтерін қолдау үшін қолданылуы бұл жерде қарастырылмайды.

9.1 Мүмкіндікті басқару

Мүмкіндікті басқару деректердің тұтастығы қорғалған орталар жасау үшін қолданылуы мүмкін.

9.2 Деректер шығу тегін сәйкестендіру

Деректер шығу тегін сәйкестендіру олардың тұтастығын қамтамасыз ету үшін қолданылуы мүмкін, мысалы, PDU координаттарының шығу тегі сәйкестендірілуі мүмкін болмаса, ондай PDU деректер тұтастығы бұзылу қауіпіне ұшыраған болып есептеледі. Соған сәйкес, егер болжамды PDU көзінде PDU жасауға уәкілеттігі болмаса, тұтастық бұзылуы орын алған болып есептеледі.

9.3 Құпиялық

Ақпараттың артықтығы кейбір жағдайларда табылмай жаңартылуы мүмкін емес деректерді алу мақсатында шифрлаумен біріктірілуі мүмкін.

Расында, артық деректердің (мысалы, қарапайым сөз және құрамына бақылау сомалары мен хеш-функциялар кіретін деректер) инвариантты қасиеттері бар. Әдетте, егер өзгертілген деректер кемінде бір декодтауға ұшыраған болса, шифрланған деректердегі өзгерістер бұл қасиеттерді сақтамайды.

(Басқа сөзбен айтқанда, егер «к» бит ақпараттар «к+м» топтық кезектілікке кодталған болса, әрекеттегі кодтау барлық мүмкін болатын топтық кезектіліктердің сиретілген көпшілігін құрайды; егер шифрланған деректердің жаңартылуы дешифрланғаннан кейін «қаскүнемнің» ойынша кездейсоқ болып табылатын өзгерістерге әкеп соқса, өзгертілген деректер декодталуының ықтималдығы шамамен $2^{-т}$ болады).

Сөйтіп, артықтық (оның ішінде бақылау сомалары мен хеш-функциялар) криптографиямен бірге және құпиялық негізінде деректердің тұтастығын қамтамасыз ете алады.

А қосымшасы
(ақпараттық)
АЖБ базалық эталонды моделінің шеңберінде тұтастықты қамтамасыз ету

Қорғаныс қызметтері мен АЖБ эталонды модель арасындағы өзара әрекеттесулер ГОСТ ИСО/МЭК 7498-2 стандартында көрсетілген. Бұл қосымшалар осы ақпараттан деректердің тұтастығына қатыстыны жинақтайды.

Түрлі қорғаныс қызметтері мынандай болып қарастырылады:

– Қалпына келумен бірге қосылыс тұтастығы;

– Қалпына келусіз қосылыс тұтастығы;

– Таңдамалы қосылыс алаңы деректерінің тұтастығы;

– Қосылыссыз деректердің тұтастығы;

– Қосылыссыз таңдамалы алаң деректерінің тұтастығы.

А.1 Қалпына келумен бірге қосылыс тұтастығы

Қосылыстың тұтастығы қосылыстардың (N) тұтынушыларының барлық (N) деректерінің тұтастығын қамтамасыз етеді, және SDU кезектілігінің шегінде кез келген деректердің кез келген жаңартылуын, енгізілуін, өшірілуін және көшірілуін табуға мүмкіндік береді (қалпына келтіру әрекеттерімен).

А.2 Қалпына келусіз қосылыс тұтастығы

Қосылыстың тұтастығы қосылыстардың (N) тұтынушыларының барлық (N) деректерінің тұтастығын қамтамасыз етеді, және SDU кезектілігінің шегінде кез келген деректердің кез келген жаңартылуын, енгізілуін, өшірілуін және көшірілуін табуға мүмкіндік береді (қалпына келтіру әрекеттерінсіз).

А.3 Таңдамалы қосылыс алаңы деректерінің тұтастығы

Таңдамалы алаң бойынша тұтастық SDU қосылысы арқылы (N) жіберілген (N) қосылыстар кезінде (N) тұтынушылар деректерінің шеңберінде таңдамалы алаңдардың тұтастығын қамтамасыз етеді, және де таңдамалы алаңдармен деректерді жаңарту, енгізу, өшіру және көшіру операциялары жүргізілген/жүргізілмегенін табуға мүмкіндік береді.

А.4 Қосылыссыз деректердің тұтастығы

(N) деңгейлерде қолдау алатын қосылыссыз тұтастық (N+1) нысандарынан сауалдар үшін тұтастық кепілдігін қамтамасыз етеді.

А.5 Қосылыссыз таңдамалы алаң деректерінің тұтастығы

Таңдамалы алаң бойынша деректердің тұтастығы қосылыссыз оңаша SDU таңдамалы алаңдарының тұтастығын қамтамасыз етеді, және таңдамалы файлдардың жаңартылуларын табуға мүмкіндік береді.

А.6 OSI деңгейлерінің шегінде тұтастықты пайдалану

Тұтастықты қамтамасыз ету қызметтері мынадай OSI деңгейлеріне қатысы бар:

– арналы деңгей (2 деңгей);

– желілік деңгей (3 деңгей);

– көліктік деңгей (4 деңгей);

– қолтаңбалы деңгей (7 деңгей).

А.6.1 Арналы деңгейде тұтастықты пайдалану

Тұтастықты қамтамасыз ету қызметтері IEEE 802.10 сипаттамасына сәйкес арналы деңгейде қолдануы мүмкін.

А.6.2 Желілік деңгейде тұтастықты пайдалану

Қалпына келтірусіз қосылыстың тұтастығын және қосылыс орнатылусыз тұтастықты қамтамасыз ету – желілік деңгейде қамтамасыз етілген жалғыз тұтастықты қамтамасыз ету қызметтері. Қалпына келтірусіз қосылыстың тұтастығын және қосылыс орнатылусыз тұтастықты деректердің тұтастығын қамтамасыз ету механизмімен, кейде шифрлау механизмі қолданылуымен қамтамасыз етуге болады. Бұл қызметтер желілік тораптар, кіші желі тораптары және реле құрылғылары арасындағы келісімділікті қамтамасыз етуге мүмкіндік береді.

А.6.3 Көлік деңгейінде тұтастықты пайдалану

Қалпына келтірумен бірге қосылыстың тұтастығын, қалпына келтірусіз қосылыстың тұтастығын және қосылыс орнатылусыз тұтастықты қамтамасыз ету – көлік деңгейінде қамтамасыз етілген жалғыз тұтастықты қамтамасыз ету қызметтері. Қалпына келтірумен бірге қосылыстың тұтастығын, қалпына келтірусіз қосылыстың тұтастығын және қосылыс орнатылусыз тұтастық деректердің тұтастығын қамтамасыз ету механизмімен, кейде шифрлау механизмі қолданылуымен қамтамасыз етуге болады. Бұл қызметтер жүйе ұштары арасындағы келісімділікті қамтамасыз етуге мүмкіндік береді.

А.6.4 Қолданбалы деңгейде тұтастықты пайдалану

Барлық тұтастық қызметтерін нақты айтқанда, қалпына келтірумен бірге қосылыстың тұтастығын, қалпына келтірусіз қосылыстың тұтастығын, таңдамалы қосылыс алаңының тұтастығын, қосылыс орнатылусыз тұтастықты және қосылыс орнатылусыз таңдамалы алаңның тұтастығын қамтамасыз ету қолданбалы деңгейде қамтамасыз етілуі мүмкін. Қалпына келтірумен және онсыз қосылыс тұтастығы және қосылыс орнатылмаған тұтастық төменгі деңгейлі деректер тұтастығын қамтамасыз ету механизмінің көмегімен (кейде – шифрлау механизмімен бірге) қамтамасыз етілуі мүмкін. Таңдамалы алаңның тұтастығы көрсету деңгейінде төменгі деңгейлі деректер тұтастығын қамтамасыз ету механизмінің көмегімен (кейде – кодтау механизмімен бірге) қамтамасыз етілуі мүмкін.

Б қосымшасы
(ақпараттық)
Деректердің сыртқы үйлесімділігі

Төменде көрсетілген [7], [8], [9] нормативтік емес сілтемелердің ішінде Д.Д.Кларкпен және Д.Р.Вильсонмен ұсынылған тұтастық моделіне көптеген сілтемелер бар. Пайда болғаны – модельді жинақтап, осы құрылымға әсер етуі мүмкін тармақтарын сипаттау.

Бұл негіздер тұтастықты деректерге белгілі бір түрлерді (олардың тұрақты мағынасын) қолдау мағынасында қарастырады. Кларк пен Вильсонның моделі қосымша нұсқаларды қарастырады. Нақты айтқанда, компьютерлік жүйе осы компьютер үшін сыртқы болып табылатын деректер мен процесстерді көрсетеді және эмульдейді. Яғни, тұтастықтың тұжырымды аудиті компьютердің ішіндегі деректер өздері білдіретін ортамен үйлесетінін кепілдендіруі керек. Осыдан тұжырымдайтынымыз, тұтастықты басқару құралдары осы компьютер үшін ерекше ішкі болуы мүмкін емес.

Нәтижесінде, Кларк-Вильсон моделінде деректердің тұтастығы қамтамасыз етілуі екі қадамды әдіс ретінде қарастырылуы мүмкін:

– деректердің сыртқы үйлесімділігіне қол жеткізілуі үшін қажет болған жағдайда өзгерістер инициализациясы үшін сайма-сай тетіктер болуы керек;

– дұрыс құрылған транзакцияның автоматты операциясы ретінде жүзеге асырылатын өзгерістер инициализациясы үшін сайма-сай тетіктер болуы керек.

Жоғарыда аталған қағидалар біздің тұтастық туралы түсінігімізді нақты білдіретінін қабылдай отырып, біз мынандай семантикалық айырмашылықтар туралы тұжырым жасаймыз:

– Деректердің ішкі келістілігі: осы мөлшер егер жоғарыда аталған түсінік қабылданған болса, ол іштей келісілген болып табылады, егер осы элементтің барлық жаңартулары сәйкес тұтастықты қорғау стратегияларын қанағаттандыратын болса.

- Деректердің сыртқы келістілігі: осы мөлшер сырттай келісілген болып табылады, егер оның мағынасы сипатталатын нақты ахуалға сәйкес келетін болса. Ол мынандай тұтастықты қорғау тиімділігінің жіктелуімен біріктірілуі мүмкін:

– күшті қорғаныс деректердің ішкі және сыртқы келістілігін қолдайды;

– әлсіз қорғаныс деректердің ішкі және/немесе сыртқы келістілігі бұзылғанын анықтайды.

Оған қоса, тексерілген процесстердің автоматты операциялары ретінде деректердің өзгертулерін кеңейту кезінде осы операциялардың кейбір қасиеттерін көрсетуге болады, мысалы:

1) операциялардың автоматтығы бұзылуы мүмкін бе?;

2) операция орындалатындығына кепілдік бар ма?

Ақыр соңында, тұтастықты қамтамасыз ету тетіктерін мынандай қасиеттерді қамтамасыз етуі бойынша жіктеуге болады:

– Ішкі/сыртқы келістілік;

– Әлсіз/күшті қорғаныс;

– Қорғалған деректерге жасалынған операциялардың автоматтығы/кепілдендірілуі.

Сөйтіп, тұтастықты қамтамасыз ету механизмін анықтау кезінде мынандай мәселелерді қарастыру қажет:

1) Осы тетіктермен келістілік формаларының қандайлары қамтылады (ішкі, сыртқы, екеуі де)?

2) Ол деректер тұтастығының әлсіз немесе күшті қорғанысын қамтамасыз етеді ме? Ол жобалау кезіндегі бұзылыстарға, кездейсоқ өзгерістерге, екі нұсқаға да төзімді ме? Ол деректер қалпына келуін қамтамасыз етеді ме?

3) Ол операциялардың автоматтығын қорғайды ма, немесе ол операция орындалуын қамтамасыз етеді ме?

В қосымшасы
(ақпараттық)
Тұтастықты қамтамасыз ету мүмкіндіктерінің сұлбасы

<table>
<tr><td colspan="3" rowspan="3">Қорғаныс құралдарының схемасы</td><td>Элемент</td><td colspan="3">Нысан: Бастамашы, Верификатор, Тұтастық - ДТС</td></tr>
<tr><td></td><td colspan="3">Функция:</td></tr>
<tr><td></td><td colspan="3">Ақпарат нысаны: тұтастығы қорғалған деректер</td></tr>
<tr><td colspan="3"></td><td>Қызмет-тің мақсаты</td><td colspan="3">Деректерді заңсыз жағартулардан/жоюдан/жасаудан/енгізуден/көшіруден қорғау</td></tr>
<tr><td rowspan="5">ҚЫЗМЕТ</td><td colspan="2">Нысан</td><td colspan="4">Домен қорғанысының рұқсаты (SDA)</td></tr>
<tr><td colspan="2">Функция</td><td colspan="4"></td></tr>
<tr><td colspan="2">Басқарумен байланысты қызмет</td><td colspan="4">- Басқару ақпаратын орнату - Басқару ақпаратының тізімін жасау
- Басқару ақпаратын жаңарту - Басқару ақпаратын блоктау
- Басқару ақпаратын жою - Басқару ақпаратының блогын ашу</td></tr>
<tr><td colspan="2">Нысан</td><td>Бастамашы</td><td>Верификатор</td><td>Тұтастық</td></tr>
<tr><td colspan="2">Функция</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Жұмыспен байланысты қызмет</td><td>-Қорғап қайта құруға ұшыраған деректер
ACL таңбасы
Бақылау сомасы
Бақылау көрсеткіші
Электронды қолтаңба</td><td>-Тұтастық аудиті
ACL таңбасы
Бақылау сомасы
Бақылау көрсеткіші
Электронды қолтаңба
- Кері қорғап қайта құр (деректерді қалпына келтіру)
Бақылау көрсеткіші
Электронды қолтаңба</td><td>- ACL Қағазы (басқару мүмкіндігінің тізімі)
Бақылау көрсеткіші
Бақылау сомасы
Сертификат</td></tr>
<tr><td rowspan="3">АҚПАРАТ</td><td colspan="2">Енгізу/шығару деректерінің басқарылатын SDA элементі</td><td colspan="4">- Сәйкестендіргіштер (бастамашы, верификатор, тұтастық - ДТС)
- Криптографиялық кілттер
- Уақытта өзгеретін мағына</td></tr>
<tr><td colspan="2">Қоладнылатын ақпарат түрі</td><td colspan="4">- Тұтастықты қорғап қайта құруға арналған ақпарат (SII)
- Тұтастықтағы өзгерістерді табуға арналған ақпарат (MDII)
- Тұтастықты кері қорғап қайта құруға арналған ақпарат (UII)</td></tr>
<tr><td colspan="2">Басқару ақпараты</td><td colspan="4">- Уақыт кезеңі - Орналастыру
- Маршруттау - Жүйелі мәртебе</td></tr>
</table>

Осы қосымшада мынандай түсініктер қолданылады

В.1 Тұтастық нысандары

Ашық жүйелердегі тұтастық кейбір базалық нысандарды қамтиды:

– бастамашы; верификатор

– тұтастықты қамтамасыз ету үшін сенімді үшінші тарап.

В.1.1 Бастамашы

Деректерді қорғап қайта құру не жіберу, немесе сақтау арқылы тұтастығы қорғалған деректер қалыптастыратын нысан.

В.1.2. Верификатор

Бастамашыдан жіберілген деректерді алады және табады, тұтастығы бұзылуын тексергеннен кейін оларды бақылайды және, қажет болған жағдайда, олардың мәндерін қалпына келтіреді.

В.1.3 Тұтастықты қамтамасыз ету үшін сенімді үшінші тарап

SII немесе MDI бөлетін және/немесе тұтастыққа қатысты операцияларды бастамашының немесе верификатордың атынан орындайтын нысан.

Қосымша
(анықтамалық)
Библиография

[1] ITU-T X.224 нұсқаулығы (1993) Қосу режимінде АЖБ (OSI) үшін көлік құралдарымен қамтамасыз ету үшін хаттама.

[2] МККТТ X.800 нұсқаулығы (1991) МККТТ қосымшалары үшін ашық жүйелер өзара әрекеттесуі үшін ақпаратты қорғау сәулеті.

[3] CLARK, David and WILSON, David: Коммерциялық және әскери компьютерлердің қорғаныс стратегияларын салыстыру. 1987 жылғы IEEE Қорғаныс және Құпиялық бойынша Симпозиумының жинағы.

[4] NIST 500-160 арнайы жарияланымы: (WIPCIS) Компьютерлік ақпарат жүйелеріндегі тұтастық стратегиялары бойынша симпозиумға шақыру туралы хабарландыру; Stuart W.Katzke and Zella G.Ruthberg шығарған.

[5] NIST 500-168 арнайы жарияланымы: Деректердің тұтастығы бойынша симпозиумға шақыру туралы хабарландыру, Zella G. Ruthberg and William T.Polk шығарған.

[6] ИСО/МЭК 9979:1999 Ақпараттық технология. Деректерді қорғау әдістері. Криптографиялық алгоритмдерді тіркеу процедуралары.

[7] ИСО/МЭК 8073:1992 Ақпараттық технология. Қосылыс болуы режимінде желілік сервистерді қамтамасыз ету хаттамасы.

[8] ИСО/МЭК 10736:1995 ИСО/МЭК 10736:1995 Ақпараттық технология. Телекоммуникациялар және жүйелер арасындағы ақпарат алмасу. Көлік деңгейіндегі қорғау хаттамасы.

[9] ИСО/МЭК 11577:1995 Ақпараттық технология. Ашық жүйелердің өзара әрекеттесуі. Желілік деңгейдегі қорғау хаттамасы.

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: деректерді өңдеу, ақпаратпен алмасу, желілердің өзара әрекеттесуі, ашық жүйелердің өзара әрекеті, коммуникациялық процедуралар, ақпаратты қорғау, қауіпсіздік технологиялары, шолу

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ

Основы безопасности для открытых систем

Часть 6
Основы целостности

СТ РК ИСО/МЭК 10181-6-2008
(ИСО/МЭК 10181-6:1996 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы целостности», 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 10181-6:1996 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы целостности» («Information technology. Open Systems Interconnection. Security frameworks for open systems. Integrity framework»), 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

Введение

Стандарт *СТ РК ИСО/МЭК 10181-2008* под общим названием «Информационная технология. Методы и средства обеспечения безопасности. Взаимодействие открытых систем. Основы безопасности открытых систем» состоит из следующих частей:

– Часть 1. Обзор
– Часть 2. Основы аутентификации
– Часть 3. Основы управления доступом
– Часть 4. Основы неотказуемости
– Часть 5. Основы конфиденциальности
– Часть 6. Основы целостности
– Часть 7. Основы учета событий безопасности и оперативного оповещения.

При использовании многих открытых систем возникают требования защиты, определяющиеся целостностью данных. Эти требования могут включать защиту данных, используемых при обеспечении других сервисов безопасности, например, аутентификации, управления доступом, конфиденциальности, учета событий безопасности и обеспечения неотказуемости, изменение которых «злоумышленником» может снизить эффективность этих сервисов или полностью свести к нулю.

Свойство неизменности и сохранности данных при неправомочном доступе называется целостностью.

Настоящий стандарт определяет общие основы для предоставления сервисов обеспечения целостности.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология. ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ. ОСНОВЫ БЕЗОПАСНОСТИ ДЛЯ ОТКРЫТЫХ СИСТЕМ Часть 6 Основы целостности

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт устанавливает основные положения 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 и взаимодействие открытых систем (ВОС). Основные положения безопасности не имеют отношения к методологии построения систем и их механизмам.

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

Настоящий стандарт устанавливает:

– основную концепцию целостности данных;

– возможные классы механизмов обеспечения целостности данных;

– средства для каждого класса механизмов обеспечения целостности данных;

– процедуры управления, необходимые для поддержания данного класса механизма обеспечения целостности данных;

– взаимодействие механизма обеспечения целостности данных и сервисов, обеспечивающих его с другими сервисами защиты и механизмами.

Настоящий стандарт может быть применен в различных типах стандартов, включая:

1) Стандарты, которые включают концепцию целостности.

2) Стандарты, которые описывают абстрактные сервисные средства, включающие средства обеспечения целостности данных.

3) Стандарты, которые описывают использование сервисных средств обеспечения целостности.

4) Стандарты, которые описывают средства обеспечения целостности в пределах архитектуры открытой системы.

5) Стандарты, которые описывают механизмы обеспечения целостности данных.

Эти стандарты могут применять настоящий стандарт следующим образом:

– стандарты типов 1), 2), 3), 4) и 5) могут использовать терминологию настоящего станадрта;

– стандарты типов 2), 3), 4) и 5) могут использовать средства, описанные в разделе 7;

– стандарты типа 5) могут быть основаны на классах механизмов, представленных в разделе 8.

Некоторые процедуры, описанные в этом стандарте, способны обеспечить целостность данных с помощью криптографических методов. Настоящий стандарт не зависит от использования конкретных криптографических или других алгоритмов, хотя определенные классы механизмов целостности могут зависеть от специфических свойств алгоритмов. *Выбор и применение конкретных средств криптографической защиты информации регламентируется законодательством Республики Казахстан.*

Примечание. Несмотря на то, что ИСО не стандартизирует криптографические алгоритмы, она стандартизирует процедуры, зарегистрированные в *[6]*.

Целостность данных, описываемая в настоящем стандарте, определяется постоянством значений данных. Это понятие (постоянство значений данных) охватывает все образцы данных, в которых различные представления значения данных полагаются эквивалентными (например, различные кодирования одного и того же значения ASN.1). Другие формы инвариантности исключены.

Использование элементов данных в настоящем стандарте включает все типы структур данных (например, файлов или совокупностей данных, информационных последовательностей, файловых систем и баз данных).

Описываемые в настоящем стандарте основы охватывают обеспечение целостности данных, которые считаются защищенными от записи со стороны потенциальных «злоумышленников». Поэтому основное внимание фокусируется на обеспечении целостности данных посредством специальных механизмов, криптографического и некриптографического, которые не основываются только на управлении доступом.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК ГОСТ Р ИСО/МЭК 7498-1-2006 Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

СТ РК ИСО/МЭК 10181-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Взаимодействие открытых систем. Основы безопасности открытых систем. Часть 1. Обзор.

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

СТ РК ИСО/МЭК 10181-3-2008 Информационная технология. Взаимодействие открытых систем. Основы безопасности открытых систем: структура. Часть 3. Основы управления доступом.

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

3 Термины и определения

В настоящем стандарте применяются термины по *СТ РК ГОСТ Р ИСО/МЭК 7498-1, СТ РК ИСО/МЭК 10181-1, СТ РК ИСО/МЭК 10181-2-2008,* ГОСТ ИСО 7498-2, а также следующие термины с соответствующими определениями:

3.1 Данные с защитой целостности (integrity-protected data) - данные и все относящиеся к ним атрибуты в пределах среды с защитой целостности.

3.2 Защитное преобразование (shield): преобразование обычных данных в данные с защитой целостности.

3.3 Канал с защитой целостности (integrity-protected channel) - канал связи, для которого используются средства обеспечения целостности.

Примечание. Два вида сервисов обеспечения целостности для каналов связи указаны в стандарте ГОСТ ИСО 7498-2. Данные виды сервисов (соединение и целостность без установления соединения) описаны в Приложении А.

3.4 Обратное защитное преобразование (unshield) - преобразование данных с защитой целостности в первоначально экранированные данные.

3.5 Проверка правильности (validate) - аудит данных с защитой целостности с целью обнаружения потери целостности.

3.6 Среда с защитой целостности (integrity-protected environment) - среда, в которой неправомочные изменения данных (включая создание и стирание данных) предотвращаются или обнаруживаются.

4 Сокращения

В настоящем стандарте установлены следующие сокращения:

4.1 ВОС - взаимодействие открытых систем (OSI, Open System Interaction);

4.2 PDU - протокольный блок данных (Protocol Data Unit);

4.3 SDU - сервисный блок данных (Service Data Unit);

4.4 SII - информация для защитного преобразования целостности (Shield Integrity Information);

4.5 MDII - информация для обнаружения изменений в целостности (Modification Detection Integrity Information);

4.6 UII - информация для обратного защитного преобразования целостности (Unshield Integrity Information).

5 Основы целостности

Цель сервисов обеспечения целостности состоит в том, чтобы защитить целостность данных и относящихся к ним атрибутов, которые могут быть подвергнуты опасности различными способами:

– неправомочной модификацией данных;

– неправомочным стиранием данных;

– неправомочным созданием данных;

– неправомочной вставкой данных;

– неправомочным воспроизведением данных.

Сервисы обеспечения целостности защищают данные от этих факторов посредством их предотвращения или обнаружения с восстановлением и без него. Эффективная защита целостности невозможна, если необходимая информация управления (например, ключи и SII) не имеет защиты целостности и/или конфиденциальности; такая защита часто основывается, неявно или явно, на принципах, отличных от воплощенных в механизме защиты данных.

Понятие защищенных сред явно используется в данных основах, чтобы обратить внимание на идею о том, что защита целостности включает защиту от неправомочного создания и/или стирания данных. Таким образом, неправомочное создание/стирание данных могут рассматриваться как неправомочные модификации некоторой защищенной среды. Точно так же вставка и воспроизведение данных могут восприниматься как модификации структурированной совокупности данных (например, информационной последовательности или структуры данных).

Некоторые изменения данных могут рассматриваться как не воздействующие никаким образом на их целостность. Например, если описание ASN.1 содержит *НАБОР* данных определенного типа, то нет никакого нарушения целостности в том, что компоненты данных этого типа переупорядочены. Сложные механизмы обеспечения целостности могут определять, что некоторые преобразования структурированных данных не представляют опасности для целостности данных. Такие механизмы позволяют осуществлять преобразования пломбированных или знаковых данных без необходимости, соответственно повторных вычислений электронной подписи или повторного уплотнения.

Цель сервисов обеспечения целостности данных состоит в том, чтобы защитить информацию от несанкционированных модификаций, включая неправомочное создание и стирание данных, а также обнаружить такие неправомочные модификации. Обеспечение выполнения сервисов обеспечения целостности данных реализуется следующими видами деятельности:

– **защитное преобразование** - образование данных с защитой целостности из обычных данных;

– **проверка правильности** - аудит данных с защитой целостности с целью обнаружения ошибок;

– **обратное защитное преобразование** - восстановление обычных данных из данных с защитой целостности.

Эти виды деятельности не обязательно используют криптографические методы. Если же такие методы применяются, они не обязательно вызывают преобразование данных. Например, операцию **защитного преобразования** можно обеспечивать добавлением печати или электронной подписи к данным. В этом случае после успешной **проверки правильности, обратное защитное преобразование** выполняется посредством удаления печати/электронной подписи.

Сервис обеспечения целостности применяется для информационного поиска, перемещения данных и управления следующим образом:

1) Для информации, перемещаемой в среде ВОС, сервисы обеспечения целостности обеспечиваются объединением **защитного преобразования**, перемещения данных с использованием (N-1)-средства и **обратного защитного преобразования** с целью формирования цикла передачи данных (N)-сервиса.

2) Для хранения данных и поиска сервисы обеспечения целостности обеспечиваются объединением функций **защитного преобразования** и хранения информации и функций поиска и **обратного защитного преобразования**.

И **защитное преобразование**, и **обратное защитное преобразование** могут быть обеспечены как параллельные операции с подобными данными (например, со всеми данными (N)-подключения), которые могут состоять одновременно из частей, еще не подвергнутых **защитному преобразованию**, из частей, определенных как данные с защитой целостности, и частей, подвергнутых **обратному защитному преобразованию**.

Механизмы обеспечения целостности поддерживают защищенные среды, и, следовательно, этапы защитного преобразования и обратного защитного преобразования включают перемещение данных между защищенными средами. Если данные с защитой целостности передаются из среды, защищенной одним механизмом обеспечения целостности от другого, защитное преобразование второго механизма должно предшествовать обратному за-

щитному преобразованию первого с целью обеспечения непрерывности защиты данных.

5.1 Базовые концепции

Несколько видов сервисов обеспечения целостности могут различаться между собой в зависимости от того, какие виды деятельности охватываются (создание, стирание, модификация, вставка, и/или восстановление данных), или же от того, требуется ли предотвращение нарушений целостности данных или только их обнаружение, и от того, поддерживают ли они восстановление данных в случае нарушения целостности. Различные виды сервисов обеспечения целостности данных описаны в п.5.2.

Механизмы, которые могут использоваться как средства обеспечения этих сервисов, могут быть разделены на широкие категории в зависимости от уровня систематической деятельности, основанной на предпринятых нарушениях целостности. Эти различные типы механизмов описаны в п. 5.3.

5.2 Виды сервисов обеспечения целостности

Сервисы обеспечения целостности данных классифицируются согласно следующим критериям:

1) Тип нарушения целостности данных, от которых они защищают. Типами нарушений являются:

– неправомочная модификация данных;
– неправомочное создание данных;
– неправомочное стирание данных;
– неправомочная вставка данных;
– неправомочное восстановление данных.

2) Тип защиты, которую они поддерживают. Типами защиты являются:

– предотвращение нарушений целостности;
– обнаружение нарушений целостности.

3) От того, включают ли такие сервисы механизмы восстановления или нет.

В предыдущем случае (с восстановлением) операция обратного защитного преобразования может иметь возможности восстановления первоначальных данных (и возможно, сообщить о восстановлении или об ошибке с целью, например, аудита защиты) всегда, как только операция проверки правильности данных указывает на появление искажения данных.

В последнем случае (без восстановления), операция обратного защитного преобразования не способна восстановить первоначальные данные, если проверка правильности указывает на искажение данных.

5.3 Типы механизмов обеспечения целостности

Как правило, способность защищать данные зависит от используемой среды. Некоторые средства по самой своей природе трудно обезопасить (типа сменных носителей данных или средств связи), и в результате неправомочные лица могут получить доступ к данным и осуществлять их изменения по желанию. Для таких средств цель механизма обеспечения целостности состоит в том, чтобы обеспечить обнаружение изменений и по возможности восстановить поврежденные данные. Ниже перечислены примеры механизмов обеспечения целостности данных:

1) Механизмы, предотвращающие доступ к среде. Такие механизмы включают:

– физически изолированные каналы, защищенные от шума;

– управление маршрутизацией;

– управления доступом.

2) Механизмы обнаружения неправомочных модификаций данных или последовательностей элементов данных, включая случаи неправомочного создания, удаления и дублирования данных. Такие механизмы включают:

– запечатывание;

– электронные подписи;

– репликация данных (используется для противодействия другим типам нарушений);

– цифровые пальцевые отпечатки вместе с криптографическими преобразованиями;

– порядковые номера сообщений.

В терминах эффективности защиты эти механизмы могут быть классифицированы следующим образом:

– отсутствие защиты;

– обнаружение модификаций и создание данных;

– обнаружение модификаций, создание, удаление и дублирование;

– обнаружение модификаций и создание данных с восстановлением;

– обнаружение модификации, создание, стирание и дублирования данных с восстановлением.

5.4 Угрозы нарушения целостности

В терминах обеспечиваемых сервисов виды угрозы нарушения целостности данных могут быть следующими:

1) Неразрешенное создание / модификация / удаление / вставка / воспроизведение данных в средах, поддерживающих целостность данных посредством предотвращения ее нарушений.

Пример. Подключение к защищенному каналу.

2) Неправомочное и необнаруживаемое создание / модификация / удаление / вставка / воспроизведение данных в средах, обеспечивающих целостность данных посредством обнаружения ее нарушений.

Пример. Целостность данных может быть обеспечена шифрованием защищенных данных и соответствующих им контрольных сумм, как описано в [8]. Если сообщающиеся объекты А и В используют один и тот же ключ для поддержки операции шифрования, и если происхождение данных не имеет защиты целостности, то данные с защитой целостности, переданные от А к В, могут быть позже представлены объекту А как имеющие своим источником объект В (отражения попытки нарушения целостности).

В терминах среды, в которой данные постоянно находятся, угрозы могут быть классифицированы как:

– имеющие отношение к среде, в которой хранятся данные;

– имеющие отношение к среде, в которую данные переданы;

– не зависящие от среды.

Поскольку настоящий стандарт рассматривает нарушения целостности как неправомочные действия, он не охватывает вопросы разрешенных модификаций, которые могут нарушить внешнюю согласованность данных, как описано в Приложении Б (например, учет неисправностей). Следовательно, данная часть настоящего стандарта в отличие от пятой части («Основы конфиденциальности») не охватывает вопросов внутренних нарушений (основы конфиденциальности охватывают вопросы, относящиеся к непрерывной защите информации, например, к возможности, при которой разрешенный доступ может сопровождаться намеренным или ненамеренным неправомочным раскрытием информации с защитой конфиденциальности).

5.5 Типы попыток нарушения защиты целостности

Каждому типу перечисленных выше угроз целостности данных соответствуют одна или более атак, т.е. попыток реализации рассматриваемой угрозы. Цель таких атак – повредить механизм (механизмы) обеспечения целостности, и они классифицируются следующим образом:

1) Атаки, нацеленные на повреждение криптографических механизмов или на использование слабых сторон таких механизмов. Они включают:

– проникновение в криптографический механизм;

– (выборочное) стирание и дублирование.

2) Атаки, нацеленные на повреждение используемого контекстного механизма (данные обмена контекстных механизмов в конкретное время с конкретным расположением. Такие атаки включают:

– массивные скоординированные изменения копий элементов данных;

– проникновение в механизм установки контекста.

3) Атаки, нацеленные на повреждение механизмов обнаружения и подтверждения нарушений. Такие атаки включают:

– ложные подтверждения;

– использование ошибочной последовательности между механизмом подтверждения и обработкой полученных данных.

4) Атаки, нацеленные на повреждение, разрушение механизмов предотвращения нарушений, или на подкуп. Такие действия включают:

– атаки непосредственно на механизм;

– проникновение в область обслуживания механизма;

– использование утилит с непреднамеренными побочными эффектами.

6 Политика обеспечения целостности

Политика обеспечения целостности - это часть политики безопасности системы, которая связана с обеспечением и использованием сервисов обеспечения целостности.

Данные с защитой целостности подвергаются тому же контролю, с которым объекты системы могут создавать, изменять и удалять эти данные. Политика обеспечения целостности должна, следовательно, идентифицировать данные, подверженные такому контролю, и указывать, какие объекты предназначены для поддержки создания, изменения или удаления данных.

В зависимости от относительной важности целостности данных различных типов, политика обеспечения целостности может также указывать тип и количество механизмов, которые должны использоваться, чтобы поддержать сервисы обеспечения целостности для каждого из различных типов данных.

Управление политикой защиты целостности не рассматривается в настоящем стандарте.

6.1 Представления политики

Для представления политики обеспечения целостности требуются средства идентификации задействованной информации и объектов системы.

Политика может рассматриваться как набор правил. Каждое правило политики обеспечения целостности может связывать характеристики данных, объекта, а также набор разрешенных типов операций над данными (как правило, это создание, изменение и удаление данных). В некоторых видах политики эти правила явно не определены, но могут быть получены из представления политики.

Следующие подразделы описывают множество способов, которыми может быть описана политика обеспечения целостности. Несмотря на то, что некоторые механизмы целостности могут быть аналогичными в определенных видах представлений политики, способ описания политики непосредственно не подразумевает использования определенного механизма для реализации политики.

6.1.1 Характеристики данных

Политика может идентифицировать данные различными способами, например:

– идентификацией объектов, имеющих разрешение на создание/удаление данных;

– по их размещению;

– идентификацией контекста, в котором представлены данные (например, по назначенной функции).

6.1.2 Характеристики объекта

Имеется много способов характеризовать объекты, к которым применяется политика обеспечения целостности. Далее приводятся два основных примера.

6.1.2.1 Политика, построенная на основе идентичности.

В этой форме представления политики объекты идентифицируются индивидуально, или идентифицируются как часть группы эквивалентных объектов (для целей политики обеспечения целостности), или же идентифицируются функцией, которую они выполняют. Таким образом, каждый объект, которому разрешается выполнять операции над данными, будет обладать индивидуальной идентичностью, групповой идентичностью или функциональной идентичностью, которые используются, чтобы охарактеризовать этот объект.

В отношении функций политики обеспечения целостности может определить исключительные группы функций, доступных каждому объекту, посредством чего функции различных групп не могут быть затребованы одновременно.

6.1.2.2 Политика, основанная на ролевой модели.

В этой форме представления политики атрибуты имеют отношение к каждому объекту и к каждому элементу данных, имеющих защиту целостности. Глобальные правила, работающие с атрибутами объектов и данных, определяют разрешенные действия. Политика, основанная на ролевой модели, обсуждена более подробно в обзоре основ защиты (см. *СТ РК ИСО/МЭК 10181-1-2008*).

7 Информация и средства обеспечения целостности

Этот раздел классифицирует информацию, необходимую для правильного выполнения сервисов обеспечения целостности, а также для средств, использующих или формирующих рассматриваемую информацию.

7.1 Информация о целостности

Для обеспечения **защитного преобразования, проверки правильности** или **обратного защитного преобразования** данных может привлекаться дополнительная информация. Эта вспомогательная информация известна как информация о целостности. Информация о целостности может быть классифицирована следующим образом.

7.1.1 Информация для защитного преобразования целостности

Информация для защитного преобразования целостности (SII) – это информация, использованная для защитного преобразования данных. Примерами такой информации являются:

– персональные ключи;

– секретные ключи;

– идентификатор политики и относящиеся к нему криптографические параметры;

– изменяющиеся во времени параметры (например, временные метки).

7.1.2 Информация для обнаружения изменений в целостности

Информация для обнаружения изменений в целостности (MDII) – это информация, используемая для обеспечения проверки правильности данных с защитой целостности. Примерами такой информации являются:

– общедоступные ключи;

– секретные ключи.

7.1.3 Информация для обратного защитного преобразования целостности

Информация для обратного защитного преобразования целостности (UII) – это информация, использованная для обеспечения обратного защитного преобразования данных с защитой целостности. Примерами такой информации являются:

– общедоступные ключи;

– секретные ключи.

7.2 Средства обеспечения целостности

Множество средств обеспечения целостности представлено в Приложении В. Они могут разделяться на имеющие отношение к функциональным аспектам и к аспектам управления.

7.2.1 Средства, связанные с работой

Это следующие средства:

1) **защитное преобразование**

Это средство используется для защиты целостности данных.

Вводимая информация может включать:

– данные, предназначенные для защиты;

– SII;

– идентификаторы, определяющие механизм обеспечения целостности, например, упомянутые в Приложении В.

Выходная информация может включать:

– данные с защитой целостности;

– коды завершения / возврата.

2) **проверка правильности данных**

Это средство проверяет данные с защитой целостности на предмет наличия изменений.

Входная информация может включать:

– данные с защитой целостности;

– MDII;

– определяющие механизм идентификаторы, например, упомянутые в Приложении В.

Выходная информация может включать:

– указания относительно наличия нарушений целостности данных.

3) **обратное защитное преобразование**

Это средство преобразует данные с защитой целостности в данные, первоначально подвергнутые **защитному преобразованию**.

Входная информация может включать:

– данные с защитой целостности;

– UII;

– определяющие конкретный механизм идентификаторы типа, указанных в приложении В.

Выходная информация может включать:

– данные;

– коды завершения / возврата.

7.2.2 Средства, связанные с управлением

Средства управления целостностью позволяют пользователю получать, модифицировать и удалять информацию (например, ключи), которая необходима для обеспечения целостности данных. В широком смысле это средства для:

– установки информации управления;

– модификации информации управления;

– удаления информации управления;

– составления списка информации управления;

– блокирования информации управления;

– разблокирования информации управления.

8 Классификации механизмов обеспечения целостности

Этот раздел описывает классификацию механизмов целостности средствами, использующимися для реализации сервисов обеспечения целостности.

8.1 Обеспечение целостности криптографическими методами

Имеется два класса криптографических механизмов обеспечения целостности, которые будут рассмотрены ниже:

1) Механизмы обеспечения целостности, основанные на симметричных криптографических методах, в которых проверка правильности данных с защитой целостности становится возможным посредством знания того же секретного ключа, который использовался для защитного преобразования данных.

2) Механизмы обеспечения целостности, основанные на асимметричных криптографических методах, в которых проверка правильности данных с защитой целостности является возможным посредством знания общедоступного ключа, соответствующего персональному ключу, который использовался для защитного преобразования данных.

Механизмы первого типа соответствуют запечатыванию данных, в то время как механизмы второго соответствуют электронным подписям.

Различные временные параметры могут использоваться совместно с механизмами целостности, основанными на криптографических методах, чтобы защитить данные от воспроизведения.

8.1.1 Обеспечение целостности посредством запечатывания

Запечатывание обеспечивает целостность посредством добавления криптографического контрольного признака к данным, подлежащим защите. При запечатывании один и тот же секретный ключ используется и для защиты, и для проверки целостности данных. Если используется этот тип механизмов обеспечения целостности, то либо весь потенциал средств проверки правильности данных известен заранее, либо же они должны иметь средства доступа к секретному ключу.

Набор объектов, способных к запечатыванию данных, и набор объектов, обладающих способностью к проверке достоверности данных, являются по определению механизма совпадающими.

Такой механизм обеспечивает обнаружение модификации следующим образом:

– **Защитное преобразование** достигается посредством присвоения криптографического контрольного признака к данным, подлежащим защите целостности (например, односторонняя функция вычислена по данным, ко-

торые будут защищены, и это значение преобразуется с помощью механизма шифрования).

– **Проверка правильности** данных достигается использованием данных с криптографическим контрольным признаком и секретным ключом, чтобы определить, являются ли данные запечатанными (например, некоторое средство подвергает данные и секретный ключ воздействию функции защитного преобразования, и полученная печать сравнивается со значением, которое было фактически присвоено данным). Если эти значения совпадают, такие данные рассматриваются как немодифицированные.

– **Обратное защитное преобразование** выполняется с помощью удаления криптографического контрольного признака, если только проверка правильности данных выполнялась по крайней мере однажды.

8.1.2 Обеспечение целостности с помощью электронных подписей

Электронные подписи вычисляются с использованием персонального ключа и асимметричного криптографического алгоритма. Данные, подвергнутые защитному преобразованию (данные с добавленной электронной подписью), могут быть проверены на правильность с применением соответствующего общедоступного ключа. Вообще говоря, общедоступный ключ может быть сделан доступным для всех пользователей.

Электронные подписи позволяют использовать набор объектов, которые могут **проверять правильность** данных с произвольными размером и составом.

Этот механизм поддерживает обнаружение модификации следующим образом:

– **Защитное преобразование** достигается посредством присвоения данным криптографических контрольных признаков с целью защиты целостности (например, к подлежащим защите данным прибавляется цифровой отпечаток пальца, который компьютеризируется, и полученное значение присоединяется к персональному ключу, и возможно, к другим параметрам, чтобы образовать одно или более значений, которые совместно формируют электронную подпись).

– **Проверка правильности** достигается использованием цифрового отпечатка пальца полученных данных, электронной подписи, и общедоступного ключа с алгоритмом аудита электронной подписи. Если этот аудит электронной подписи выявляет ошибку, то соответствующие ей данные будут рассматриваться как подвергшиеся изменению.

– **Обратное защитное преобразование** выполняется посредством удаления криптографического контрольного признака после проверки правильности данных.

Данный механизм может также поддерживать режимы первоначальной аутентификации и обеспечения неотказуемости.

8.1.3 Обеспечение целостности посредством шифрования избыточных данных

Целостность избыточных данных (например, обычной речи) может быть обеспечена посредством шифрования. Данные, которые включают коды поиска ошибок и цифровые отпечатки пальцев, являются избыточными, и их целостность может быть защищена с помощью шифрования (при условии, что используемый алгоритм шифрования делает невозможным предсказание о том, как изменения зашифрованных данных будут отражаться на первоначальных данных после дешифрования).

Протоколы защиты нижнего уровня (см. стандарты *[8]*, *[9]*) используют этот тип механизма, чтобы обеспечить защиту целостности и конфиденциальность защищенных данных.

Этот механизм обеспечивает обнаружение изменений информации следующим образом:

1) **Защитное преобразование** достигается шифрованием избыточных данных.

2) **Проверка правильности** достигается расшифрованием данных, подвергнутых защитному преобразованию, и определением того, соответствуют ли они каким-нибудь инвариантностям, которым удовлетворяют первоначальные данные.

Примеры.

– если первоначальные данные являются последовательностью символов в формате ASCII, восстановленные данные должны иметь те же самые характеристики;

– если первоначальные данные, согласно предположению, рассматриваются как человеческая речь на данном языке, то восстановленные данные должны быть (или должны быть преобразованы с минимальными модификациями) пригодным для восприятия большинством людей человеческим произношением на том же самом языке;

– если первоначальные данные содержат контрольные суммы, можно вычислять такие же контрольные суммы для части защищенных данных, и проверить соответствие результатов значениям контрольной суммы, включенным в расшифрованные данные.

3) **Обратное защитное преобразование** выполняется с помощью расшифрования зашифрованных данных.

Примечание. Описанный механизм, как известно, является неподходящим для некоторых распространенных форм избыточности (например, для данных с кодами поиска ошибок), используемых вместе с распространенными способами шифрования (например, блочное шифрование типа DES (стандарта шифрования данных), с формированием цепочек данных или без него). Относительно простой пример потенциальных ловушек следующий.

Если текст ASCII (например, обычная электронная почта) должна быть защищен с помощью DES-шифрования, в сообщение могут быть внесены необнаруживаемые изменения посредством усечения его длины (если, ко-

нечно, заголовок почты не содержит, как обычно, индикатора длины последовательности данных).

8.2 Обеспечение целостности с помощью контекста

Целостность может быть обеспечена с помощью механизмов хранения или передачи данных в одном или более предварительно согласованных контекстах. Такие механизмы могут защищать и данные, и структуры данных (например, последовательности модулей данных). Они включают:

8.2.1 Дублирование данных

Этот класс механизмов целостности основан на дублировании данных в пространстве (например, в нескольких областях памяти) или во времени (например, в разное время). Принимается, что потенциальные «злоумышленники» не могут одновременно ставить под угрозу более ограниченного числа копий и что всякий раз, когда атаки обнаруживаются, данные могут быть восстановлены из подлинных копий.

Например, такой механизм может использоваться базами данных, устойчивыми к атакам.

Эти механизмы обеспечивают обнаружение стирания целостности посредством восстановления и могут использоваться вместе с другими механизмами защиты. Они обеспечивают целостность данных следующим образом:

– **Защитное преобразование** достигается созданием ряда копий одних и тех же данных или в одно время, или в различных областях памяти.

– **Проверка правильности** достигается сбором копий в каждое данное время или в каждом данном месте. Они сравниваются, и если все они не идентичны, то считается, что произошло нарушение целостности.

– **Обратное защитное преобразование** (с восстановлением) осуществляется, если достигается некоторый предустановленный критерий (например, «соответствие значений на 90% или более») посредством выбора в качестве правильного значения того, которое минимизирует некоторое заданное значение (например, вероятность ошибочного восстановления).

Необходимо отметить, что необходимый критерий восстановления должен быть достигнут, если все значения согласуются с первоначальными, а также что при этих обстоятельствах значение, минимизирующее данный параметр, должно быть общепринятым значением.

8.2.2 Предварительно согласованный контекст

Эти механизмы обеспечивают обнаружение стирания данных с защитой целостности данных и часто используются совместно с другими механизмами целостности:

– **Защитное преобразование** достигается предоставлением данных в определенное время и/или с определенным расположением в пределах данного уровня модификаций данных.

– **Проверка правильности** достигается ожиданием данных в данное время и/или с данным расположением. Если она отсутствует, то нарушение целостности считается происшедшим.

Чтобы предотвращать замену альтернативных данных, этот механизм должен, как отмечено выше, быть объединен с другими механизмами обеспечения целостности.

8.3 Обеспечение целостности посредством обнаружения и подтверждения нарушений

Эти механизмы используют обнаружение целостности при выполнении идемпотентных операций с положительной обратной связью (операция считается идемпотентной, если многократные успешные выполнения данной операции дали один и тот же единственный результат). Примеры таких механизмов - перемещения данных с положительными подтверждениями (например, транспортный класс 4, описанный в *[7]*) и дистанционные операции с обратной связью. Эти механизмы предполагают, что процедуры **защитного преобразования** и **проверки правильности/обратного защитного преобразования** данных работают с той же продолжительностью времени и, как правило, не подходят для хранения данных:

– **Защитное преобразование** достигается повторением одних и тех же действий до тех пор, пока в политике обеспечения целостности не будет иных указаний или пока не будет получено положительное подтверждение.

– **Проверка правильности** выполняется для каждого образца данных, подвергнутых защитному преобразованию (если в политике обеспечения целостности отсутствуют иные указания); успешные проверки правильности приводят к формированию положительных подтверждений для объекта, выполняющего операцию защитного преобразования.

Если можно выполнить коррекцию, чтобы передать правильную информацию из данных, подвергнутых обратному защитному преобразованию, при использовании действующего механизма защиты целостности, обратное защитное преобразование этого механизма может сформировать положительное подтверждение.

Если проверка правильности дает отрицательный результат (или происходят модификация, либо стирание данных), возможно снижение эффективности при отрицательном подтверждении операции защитного преобразования.

Эти механизмы предполагают, что модификации данных могут быть обнаружены при использовании других средств, и, следовательно, эти меха-

низмы могут рассматриваться как расширение средств защиты от модификации данных.

8.4 Обеспечение целостности посредством предотвращения ее нарушений

Целостность можно обеспечивать, предотвращая физический доступ к хранимым данным или средствам передачи информации, а также с помощью управления доступом к информации.

Описание средств предотвращения физического доступа находится вне пределов области действия данной основы.

Управление доступом описано в структуре управления доступом.

9 Взаимодействия с другими сервисами и механизмами защиты

Данный раздел описывает, как другие сервисы и механизмы защиты могут использоваться для обеспечения целостности данных. Использование целостности данных для поддержки других сервисов защиты здесь не рассматривается.

9.1 Управление доступом

Управление доступом может использоваться для создания сред с защитой целостности данных.

9.2 Аутентификация происхождения данных

Аутентификация происхождения данных может использоваться для обеспечения их целостности, например, если происхождение координат PDU не может быть идентифицировано, то такой PDU можно считать подверженным угрозе нарушения целостности данных. Аналогично, если предполагаемый источник PDU не обладает полномочиями на создание PDU, то имеет место нарушение целостности.

9.3 Конфиденциальность

Избыточность информации в некоторых случаях может быть объединена с шифрованием с целью получения данных, которые невозможно модифицировать без обнаружения.

Действительно, избыточные данные (например, обычная речь и данные, включающие контрольные суммы и значения хеш-функции) имеют инвариантные свойства. Как правило, изменения в зашифрованных данных не будут сохранять, с высокой вероятностью, эти свойства, если измененные данные подвергались хотя бы однократному шифрованию.

(Иначе говоря, если k бит информации зашифрованы в последовательность k+m бит, действующее шифрование составляет разреженное подмно-

жество всех возможных разрядных последовательностей; если модификации зашифрованных данных приводят после дешифрования к изменениям, которые с точки зрения "злоумышленника" являются случайными, вероятность того, что измененные данные будут расшифрованы как правильно, будет порядка 2^{-m} .)

Таким образом, избыточность (включая контрольные суммы и хеш-функции) совместно с криптографией и на основе конфиденциальности, может обеспечить целостность данных.

Приложение А
(справочное)
Обеспечение целостности в рамках базовой эталонной модели ВОС

Взаимоотношения между сервисами защиты и эталонной моделью ВОС представлены в стандарте ГОСТ ИСО 7498-2. Данное приложение суммирует из этой информации то, что имеет отношение к целостности данных.

Различные сервисы защиты рассматриваются как следующие:

– целостность соединения с восстановлением;

– целостность соединения без восстановления;

– целостность данных выборочного поля соединения;

– целостность данных без соединения;

– целостность данных выборочного поля без соединения.

А.1 Целостность соединения с восстановлением

Целостность соединения обеспечивает целостность всех данных (N) пользователей (N) соединений и позволяет обнаруживать любые модификации, вставки, стирание и воспроизведение любых данных в пределах всей последовательности SDU (с попытками восстановления).

А.2 Целостность соединения без восстановления

Целостность соединения обеспечивает целостность данных всех (N) пользователей (N) соединений и позволяет обнаруживать любые модификации, вставки, стирание и воспроизведение любых данных в пределах последовательности SDU (без попыток восстановления).

А.3 Целостность соединения по выборочному полю

Целостность по выборочному полю обеспечивает целостность выборочных полей в рамках данных (N) пользователей при (N) соединениях для (N) переданных через соединение SDU, а также позволяет обнаруживать, производились ли с выборочными полями операции модификации, вставки, стирания или воспроизведения данных.

А.4 Целостность без установления соединения

Целостность без установления соединения, поддерживаемая на (N) уровнях, обеспечивает гарантию целостности для запросов от (N+1) объектов.

А.5 Целостность по выборочному полю без установления соединения

Целостность данных по выборочному полю обеспечивает целостность выборочных полей одиночного SDU без установления соединения и позволяет обнаруживать модификации выборочных файлов.

А.6 Использование целостности в пределах уровней базовой эталонной модели ВОС

Сервисы обеспечения целостности имеют отношение к следующим уровням базовой эталонной модели ВОС:

– канальному уровню (уровень 2);

– сетевому уровню (уровень 3);

– транспортному уровню (уровень 4);

– прикладному уровню (уровень 7).

А.6.1 Использование целостности на канальном уровне

Сервисы обеспечения целостности могут быть поддержаны на канальном уровне в соответствии с описанием в IEEE 802.10.

А.6.2 Использование целостности на сетевом уровне

Обеспечение целостности соединения без восстановления и целостности без установления соединения - единственные сервисы обеспечения целостности, обеспеченные на сетевом уровне. Целостность соединения без восстановления и целостность без установления соединения можно обеспечивать механизмом обеспечения целостности данных, иногда - с использованием механизма шифрования. Данные сервисы позволяют обеспечить согласованность между сетевыми узлами, узлами подсети и релейными устройствами.

А.6.3 Использование целостности на транспортном уровне

Целостность данных соединения с восстановлением, целостность соединения без восстановления и целостность данных без установления соединения - единственные сервисы целостности, обеспеченные на транспортном уровне. Целостность соединения с восстановлением или без него, и целостности без установления соединения могут быть обеспечены механизмом целостности данных, иногда - совместно с механизмом шифрования. Данные сервисы позволяют обеспечить согласование между концами системы.

А.6.4 Использование целостности на прикладном уровне

Все сервисы обеспечения целостности, а именно, целостность соединения с восстановлением, целостность соединения без восстановления, целостность выборочного поля соединения, целостность без установления соединения и целостность выборочного поля без установления соединения могут быть обеспечены на прикладном уровне. Целостность соединения с восстановлением или без него и целостность без установления соединения могут обеспечиваться с помощью механизма обеспечения целостности данных нижнего уровня (иногда - совместно с механизмом шифрования). Целостность выборочного поля может быть обеспечена посредством механизма обеспечения целостности данных нижнего уровня (иногда - вместе с механизмом шифрования) на уровне представления.

Приложение Б
(справочное)
Внешняя согласованность данных

В [7], [8], [9] содержится множество ссылок к модели целостности, предложенной Д.Д.Кларком и Д.Р.Вильсоном. То, что получается - это попытка суммировать модель и высветить те ее пункты, которые могут воздействовать на эту структуру.

Эти основы рассматривает целостность в смысле поддержания определенной вариации на данных (их постоянное значение). Модель Кларка и Вильсона рассматривает дополнительные варианты. А именно, это предполагает, что компьютерная система отражает и эмулирует данные и процессы, которые являются внешними для данного компьютера. Следовательно, заключительный аудит целостности должен гарантировать, что данные внутри компьютера совместимы со средой, которую они представляют. Отсюда следует, что средства управления целостностью никоим образом не могут быть исключительными внутренними для данного компьютера.

В результате обеспечение целостности данных в модели Кларка-Вильсона может рассматриваться как двухшаговый подход:

– должны существовать адекватные механизмы для инициализации изменений при их необходимости, чтобы таким образом достигалась внешняя согласованность данных;

– должны существовать адекватные механизмы для гарантирования инициализации изменений, которые осуществляются как атомарная операция правильно построенной транзакции.

Принимая, что вышеуказанные положения точно отражают наше интуитивное понимание целостности, мы приходим к выводу о следующих семантических различиях:

– **Внутренняя согласованность данных.** Данная величина является внутренне согласованной тогда и только тогда, когда все модификации данного элемента удовлетворяют соответствующим политикам обеспечения целостности.

– **Внешняя согласованность данных.** Данная величина является внешне согласованной, только если ее значение соответствует реальной ситуации в мировом масштабе, которую она описывает.

В случае, когда перечисленные выше особенности имеют место, можно дополнительно использовать следующую классификацию эффективности защиты целостности:

– сильная защита поддерживает внутреннюю и внешнюю согласованность данных;

– слабая защита обнаруживает нарушение внутренней и/или внешней согласованности данных.

Более того, при расширении изменений данных в качестве атомарных операций проверенных процессов, можно указать некоторые свойства этих операций, например:

1) может ли атомарность операции быть нарушенной;

2) имеются ли гарантии того, что операция будет действительно выполнена.

Наконец, можно классифицировать механизмы обеспечения целостности в плане обеспечения следующих свойств:

– внутренняя/внешняя согласованность;

– слабая/сильная защита;

– атомарность/гарантия операций над защищенными данными.

Таким образом, при определении механизма обеспечения целостности, необходимо рассмотреть следующие вопросы:

1) Какая форма согласованности (внутренняя, внешняя, обе) охватывается данным механизмом?

2) Обеспечивает ли она слабую или сильную защиту целостности данных? Устойчива ли она к нарушениям при проектировании, к случайным изменениям, к обоим вариантам? Обеспечивает ли она восстановление данных?

3) Защищает ли она атомарность операций, или же она обеспечивает гарантию (в том числе) того, что операция будет выполнена?

Приложение В
(справочное)
Схема возможностей обеспечения целостности

<table>
<tr><td colspan="3" rowspan="3">Схема средств защиты</td><td rowspan="3">Элемент</td><td colspan="3">Объект: инициатор, верификатор, целостность - ДТС</td></tr>
<tr><td colspan="3">Функция</td></tr>
<tr><td colspan="3">Информационный объект: данные с защитой целостности</td></tr>
<tr><td colspan="3">Цель сервиса</td><td colspan="3">Защищать данные от неправомочных модификации/удаления/создания/вставки/воспроизведения</td></tr>
<tr><td rowspan="4">Деятельность</td><td rowspan="2"></td><td>Объект</td><td colspan="4">Разрешение защиты домена (SDA)</td></tr>
<tr><td>Функция</td><td colspan="4"></td></tr>
<tr><td colspan="2">Деятельность, связанная с управлением</td><td colspan="4">- установка информации управления;
- составление списка информации управления;
- модификация информации управления
- блокировка информации управления;
- удаление информации управления;
- разблокировка информации управления</td></tr>
<tr><td rowspan="2"></td><td>Объект</td><td>инициатор</td><td>верификатор</td><td>целостность - ДТС</td></tr>
<tr><td colspan="2">Функция</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Деятельность, связанная с работой</td><td>- Данные, подвергнутые защитному преобразованию
Метка ACL
Контрольная сумма
Контрольный признак
Электронная подпись</td><td>- Аудит целостности
Метка ACL
Контрольная сумма
Контрольный признак
Электронная подпись
- Обратное защитное преобразование (восстановление данных)
Контрольный признак
Электронная подпись</td><td>- Бумага
ACL (список управления доступом)
Контрольный признак
Контрольная сумма
Сертификат</td></tr>
<tr><td rowspan="3">Информация</td><td></td><td>Управляемый SDA элемент данных ввода/вывода</td><td colspan="4">- идентификаторы (инициатор, верификатор, целостность - ДТС) ;
- криптографические ключи;
- изменяющееся во времени значение</td></tr>
<tr><td></td><td>Используемый тип информации</td><td colspan="4">- информация для защитного преобразования целостности (SII);
- информация для обнаружения изменений в целостности (MDII);
- информация для обратного защитного преобразования целостности (UII)</td></tr>
<tr><td></td><td>Информация управления</td><td colspan="4">- период времени;
- размещение;
- маршрутизация;
- системный статус</td></tr>
</table>

Рис. В.1. Схема возможностей обеспечения целостности

В данном приложении используются следующие понятия:

В.1 Объекты целостности

Целостность в открытых системах включает некоторые базовые объекты:

– инициатор;

– верификатор;

– доверенная третья сторона для обеспечения целостности.

В.1.1 Инициатор

Объект, который формирует данные с защитой целостности посредством их защитного преобразования или передачи, или же сохранения.

В.1.2. Верификатор

Объект, который получает или отыскивает данные, переданные от инициатора, контролирует их после проверки правильности на предмет обнаружения нарушений целостности, и при необходимости, восстанавливает их значения.

В.1.3 Доверенная третья сторона для обеспечения целостности

Объект, который распределяет SII или MDI и/или выполняет имеющие отношение к целостности операции от имени инициатора или верификатора.

Приложение
(справочное)
Библиография

[1] Рекомендации ITU-T X.224 (1993) Протокол для обеспечения транспортных средств для ВОС (OSI) в режиме соединения.

[2] Рекомендации МККТТ X.800 (1991) Архитектура защиты информации для взаимодействия открытых систем для приложений МККТТ.

[3] CLARK, David and WILSON, David: Сравнение политики защиты коммерческих и военных вычислительных средств. Сборник Симпозиума IEEE за 1987 по Защите и Секретности.

[4] Специальная публикация NIST 500-160: Сообщение о приглашении на симпозиум по политикам обеспечения целостности в компьютерных информационных системах (WIPCIS); изданное Stuart W.Katzke and Zella G.Ruthberg.

[5] Специальная публикация NIST 500-168: Сообщение о приглашении на симпозиум по целостности данных, изданное Zella G. Ruthberg and William T.Polk.

[6] ИСО/МЭК 9979:1999 Информационная технология. Методы защиты данных. Процедуры для регистрации криптографических алгоритмов.

[7] ИСО/МЭК 8073:1997 Информационная технология. Протокол обеспечения сетевых сервисов в режиме наличия соединения.

[8] ИСО/МЭК 10736:1995 Информационная технология. Связь и информационный обмен между системами. Протокол защиты транспортного уровня.

[9] ИСО/МЭК 11577:1995 Информационная технология. Взаимодействие открытых систем. Протокол защиты сетевого уровня.

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.

Для заметок

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