ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
4-бөлім
Істен шықпау негіздері

Информационная технология
ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ
Основы безопасности для открытых систем
Часть 4
Основы неотказуемости

ҚР СТ ИСО/МЭК 10181-4-2008

(ИСО/МЭК 10181-4:1996 «Ақпараттық технологиялар. Ашық жүйелердің өзара әрекеті. Ашық жүйелер үшін қауіпсіздік негіздері. Істен шықпау 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
4-бөлім
Істен шықпау негіздері

ҚР СТ ИСО/МЭК 10181-4-2008
(ИСО/МЭК 10181-4:1996 «Ақпараттық технологиялар. Ашық жүйелердің өзара әрекеті. Ашық жүйелер үшін қауіпсіздік негіздері. Істен шықпау негіздері», IDT)

Ресми басылым

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

Астана

Кіріспе

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасының Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**

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

3 Осы стандарт Қазақстан Республикасының экономикасының қажеттіліктерін айқындайтын қосымша талаптар мәтін бойынша көлбеу қаріппен белгіленіп ИСО/МЭК 10181-4:1997 «Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелердің қауіпсіздік негіздері. Істен шықпау негіздері» («Information technology. Open Systems Interconnection. Security frameworks for open systems. Non-repudiation framework»), IDT, халықаралық стандартына балама.

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

“Ақпараттық технология. Қауіпсіздікті қамтамасыз ету тәсілдері мен құралдары. Ашық жүйенің өзара әрекеті. Ашық жүйе қауіпсіздігінің негіздері” деп жалпы аталатын ҚР СТ ИСО/МЭК 10181-ші осы стандарты мынадай бөлімдерден тұрады:

– 1 бөлім. Шолу

– 2 бөлім. Сәйкестендіру негіздері.

– 3 бөлім. Еркін басқарудың негіздері

– 4 бөлім. Істен шықпаудың негіздері

– 5 бөлім. Құпиялық негіздері

– 6 бөлім. Бүтіндік негіздері

– 7 бөлім. Қауіпсіздік жағдайлары мен жедел хабарламаларды есепке алу негіздері

ҚР СТ ИСО/МЭК 10181 *А-Е қосымшалары* анықтамалық болып табылады.

Істен шықпауды қамтамасыз етудің сервисін тағайындау дегеніміз – оқиға немесе іс-әрекеттің болғаны мен болмағаны жайлы даулы жайларды шешу үшін жария болған оқиға немесе іс-әрекетке қатысты бұлтартпас айғақтарды жинау, қамтамасыз ету, оларды қол жетерліктей ету және нақтылау болып табылады.

Істен шықпауды қамтамасыз ету сервисі әртүрлі контекстер мен жайларда қолданылуы мүмкін. Олар, сондай-ақ, мәліметтер дайындауда, мәліметтерді сақтауда және мәліметтер беруде қолданылуы мүмкін. Істен шықпауды қамтамасыз ету процестері куәлік заттардың жасақталуын көздейді; бұл оқиғаның немесе іс-әрекеттің болғанын дәлелдеу мүмкін еместей етіп, одан бас тартқан жағдайда, кейбір оқиғалар немесе іс-әрекеттердің шын мәнінде болғанының фактісін дәлелдеу үшін қолданылады.

Ашық жүйенің өзара әрекеттесуінің АЖӘ (ВОС) (*ГОСТ ИСО 7498-2 қараңыз*) базалық эталондық моделінде істен шықпауды қамтамасыз етудің мынадай екі типі бар:

– түпнұсқадан істен шықпауды қамтамасыз ету – деректерді жіберу фактісін жіберушінің жалған мойындамауын жоққа шығаруда қолданылады;

– жеткізуден істен шықпауды қамтамасыз ету – деректерді қабылдау фактісін алушының жалған мойындамауын жоққа шығаруда қолданылады.

Ашық жүйенің өзара әрекеттесуінің (АЖӘ - ВОС) базалық эталондық моделінің хаттамаларын пайдаланушы қосымшаларға істен шықпауды қамтамасыз ету сервисінің басқа да түрлері - қосымшалардың нақтылы кластарына арналған спецификалық түрлері қажет болуы мүмкін. Мысалы, MHS (*ИСО/МЭК 10021-2*) беру сервисі үшін талқылаудан істен шықпауды

анықтайды; ал ЭОД (EDI, Рек. МСЭ-Т Х, 435 қараңыз) қайтару және беріп жіберу сервистері үшін істен шықпауды анықтайды.

Осы құжаттағы қаралған тұжырымдамалар негізі АЖӘ - (ВОС) ның базалық эталондық моделінің коммуникацияларымен шектеліп қалмайды, алайда оларды одан әрі пайдалану үшін мәліметтерді дайындау және сақтау сияқты қолданысқа ие болып, кең таралуы мүмкін.

ҚР СТ ИСО/МЭК 10181-нің осы бөлімі істен шықпауды қамтамасыз ету сервистерінің жалпы негіздерін былайша анықтайды:

– істен шықпауды қамтамасыз ету сервистерінің *ГОСТ ИСО 7498 және МККТТ Х.800-де* баяндалған түсініктерін кеңейтеді және олардың ашық жүйеде қалай қолданылатынын түсіндіреді.

– осыған ұқсас сервистердің нұсқаларын қарастырады;

– аталған сервистер мен қорғаныстың басқа да сервистерінің өзара байланыстарын түсіндіреді.

Істен шықпауды қамтамасыз ету үшін мыналар қажет болуы мүмкін:

– соттар: бұлардың міндетіне оқиғаны немесе іс-әрекетті жоққа шығару нәтижесінде туындайтын даулы жағдайларда шешімдер шығару кіреді;

– сенім білдірілген үшінші жақ: бұлар куәларды айғақтау үшін қолданылатын мәліметтердің түпнұсқалығына және бүтіндігіне кепілдік береді.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
4-бөлім
Істен шықпау негіздері

Енгізілген күні 2008.07.01

1. Қолданылу саласы

Осы стандарт ашық жүйелер ортасында қауіпсіздік сервистерін қолдану міндеттерін шешуге арналған қауіпсіздік негіздерін белгілейді. “Ашық жүйе” термині дерекқорды, жүйеленіп бөлінген қосымшаларды, ашық жүйелердің (АЖБ) талдануы мен өзара әрекеттесуін білдіреді. Қауіпсіздіктің негізгі ережелермен жүйе құрудың әдістемесіне және олардың тетіктеріне еш қатысы жоқ.

Қауіпсіздіктің негізгі ережелері қауіпсіздіктің спецификалық сервистерін алу үшін қолданылатын мәліметтер элементтерін де, сол сияқты әрекет нәтижелерін де (бірақ хаттама элементтерін емес) қамтиды.

Қауіпсіздіктің бұл сервистері өзара әрекеттесуші жүйе негіздерінде де, сондай-ақ жүйе аралық мәліметтер алысуда да, жүйелер басқаратын мәліметтерге де қолданыла алады.

Осы стандарт:

– істен шықпаудың негізгі түсінігін;

– істен шықпауды қамтамасыз етудің жалпы сервисін;

– істен шықпау сервисін қамтамасыз етудің мүмкін тетіктерін;

– істен шықпауды қамтамасыз ету сервистері мен тетіктері үшін басқарудың жалпы талаптарын белгілейді.

Кез-келген басқа да қорғаныс сервисі тәрізді істен шықпауды қамтамасыз ету нақтылы жағдай үшін контекстегі берілген қауіпсіздік саясатында ғана жүзеге асуы мүмкін. Қауіпсіздік саясатын айқындау осы стандарт шеңберінен тыс.

Осы стандарттың қолдану аясы хаттамалар құрамындағы алмасу деталдарының спецификасын қамтымайды; ал бұл хаттамалардың орындалуы істен шықпауды қамтамасыз ету үшін өте қажет. Сондай-ақ стандарт істен шықпауды қамтамасыз етудің сервистерін жүзеге асыруда қолданылуы мүмкін нақтылы тетіктерді сипаттамайды және қауіпсіздікті басқарудағы сервистер мен хаттамаларды қамтамасыз етуді бүге-шігесіне дейін баяндамайды.

Осы құжатта көрсетілген кейбір іс-шаралар қорғаныстың криптографиялық тәсілдерінің көмегімен жүзеге асырады. Берілген негіздер

нақтылы криптографиялық немесе басқа да алгоритмде, не нақтылы криптографиялық тәсілдерді (яғни симметриялық яки ассиметриялық) пайдалануға тәуелді емес, алайда істен шықпауды қамтамасыз ету тетіктерінің кейбір кластары нақтылы алгоритмнің қасиетіне тәуелді болуы мүмкін. *Ақпаратты криптографиялық қорғаудың нақты құралдарын таңдау және қолдану Қазақстан Республикасының заңнамасымен регламенттеледі.* Анығында, тәжірибеде әртүрлі көптеген алгоритмдер қолданылады. Криптографиялық жағынан қорғаныстағы мәліметтерді пайдаланғысы келетін екі мән бір ғана криптографиялық алгоритмді қолдау керек.

Осы стандарт стандарттардың әртүрлі типтерінде қолданылуы мүмкін:

1) Істен шықпау түсінігі енгізілген стандарттар.

2) Істен шықпауды қамтамасыз етуді қоса алғандағы абстракты сервистерді айқындайтын стандарттар.

3) Істен шықпауды қамтамасыз етудің қолданылуын айқындайтын стандарттар.

4) Істен шықпауды қамтамасыз ету құралдарын ашық жүйе архитектурасында айқындайтын стандарттар.

5) Істен шықпауды қамтамасыз етудің тетіктерін айқындайтын стандарттар.

Жоғарыда жіктелген стандарттардың нұсқаларына берілген негіздерді былай пайдалануға болады:

– 1), 2), 3), 4) немесе 5) стандарт типтерін берілген негіздердің терминологиясында қолдануға болады;

– 2), 3), 4) немесе 5) стандарт типтерін 7-бөлімде көрсетілген құралдарда қолдануға болады;

– 5) стандарт типтері 8-бөлімде көрсетілген тетіктер кластарына негіз бола алады.

2. Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ ИСО/МЭК 10181-1-2008 Ақпараттық технология. қауіпсіздікті қамтамасыз ету тәсілдері мен құралдары. Ашық жүйенің өзара әрекеті. Ашық жүйе қауіпсіздігінің негіздері. 1 бөлім. Шолу.

ГОСТ ИСО 7498-2-2002 Ақпараттық технология. Ашық жүйенің өзара әрекеті. Базалық эталондық модель. 2 бөлім. Ақпарат қорғанысының архитектурасы.

3. Терминдер мен анықтамалар

Осы стандартта *ҚР СТ ИСО/МЭК 10181-1-2008*, ГОСТ ИСО 7498-2, [1] бойынша терминдер, сондай-ақ сәйкес анықтамаларымен мынадай терминдер қолданылды:

3.1 Куәгерліктің беделін түсіру (compromised evidence): Бір кездегі қанағаттанарлық куәгерлік бұдан былай сенім білдірілген үшінші жақтың (СБҮЖ) немесе соттың сеніміне ие бола алмайды.

3.2 Қарсы қолтаңба (counter-signature): мәліметтер блогына енген, алайда басқа мәнге ие сандық қолтаңба (мысалы, СБҮЖ -СБҮЖ).

3.3 Куәлік (evidence): Даулы жағдайларды шешу үшін қолданылатын мәліметтер; ол жеке өзі немесе басқа бір мәліметпен қоса қолданылуы мүмкін.

3.4 Куәлік жасаушы (evidence generator): Істен шықпау куәлігін жасаушы мән.

Ескертпе – Бұл мән куәлік сұраушы жақ, түпнұсқа, қабылдаушы немесе бірігіп қимылдаушы бірнеше тараптар болуы мүмкін (мысалы, қол қоюшы және онымен бірге қол қойған жақ).

3.5 Куәгерлік субьектісі (evidence subjekt): іс-әрекетке немесе оқиғаға қатыстылығы куәлікпен дәлелденетін мән.

3.6 Куәгерлікті пайдаланушы (evidence user): Куәгерлікті пайдаланушы мән.

3.7 Куәгерлік верификаторы (evidence verifier): Куәгерлікті тексеруші мән.

3.8 Хабарламаны сәйкестендіру коды (message autentication code): Криптографиялық тексеруден өткен мағына; ол мәліметтер бүтіндігін және мәліметтердің түпнұсқалығын сәйкестендіреді, яғни түпнұсқа дәлдігін тексереді.

3.9 Істен шықпауды қамтамасыз ету сервисін сұраушы тарап (non-repudiation service requester): Нақтылы іс-әрекет немесе оқиға үшін куәлік жасауды талап ететін мән.

3.10 Нотариус (notary): Мәліметтер мінездемесінің дәлдігіне кейіннен кепіл бола алатын, мәліметтерді тіркеуші сенім білдірілген үшінші жақ.

3.11 Түпнұсқа (originator): Түпнұсқаның контексте берілуінің мәні; істен шықпауды қамтамасыз етудің субьектісі ретінде әрекет кезінде мағлұматтар жасайды.

3.12 Алушы (recipient): Алушының контексте берілуінің мәні; істен шықпауды қамтамасыз етудің субьектісі ретінде әрекет кезіндегі мағлұматтарды қабылдап алады.

Ескертпе - істен шықпаудың логикалық моделінде басқа да мәндер қаралуы мүмкін. Мысалы, қожайын алғашқы хабарды жасаушы мән ретінде қарастырылса, ал хабар беруші агент – хабарды жеткізуші мән; бұл берілген контекстегі мәндер түпнұсқа және қабылдап алушы ретінде сипатталады.

4. Қысқартулар

Осы стандартта мынадай қысқартулар пайдаланылады:

4.1 Ашық жүйенің өзара байланысы; АЖБ (ВОС) (Open System Interaction OSI).

4.2 Куәландырушы орталық; КО (КО) (Certificate Authority; CA).

4.3 Сенім білдірілген үшінші жақ; СБҮЖ (СБҮЖ) (Trusted Third Party; TTP).

4.4 Хабарларды басқару жүйесі; ХБЖ (СУС) MHS (Message Handling System).

4.5 Электронды мәліметтер алмасулар; ЭМА (ОЭД) (Elektronic Data Interchange; EDI).

4.6 Кері қайтарылған сертификаттар тізімі; КҚСТ CRL (Certificate Revocation List).

5. Істен шықпау туралы жалпы мәліметтер

5.1. Істен шықпаудың негізгі түсініктері

Істен шықпауды қамтамасыз ету сервисі дегеніміз куәгерлік жасау, оны растау және тіркеу, сондай-ақ даулы жағдайды шешу үшін куәгерлік мағлұматтарын қайтадан айғақтау әрі оны онан әрі іздестіру. Қосымша куәгерлік тіркелмесе даулы жағдайды шешу мүмкін емес.

Осы беріліп отырған тараудағы істен шықпауды қамтамасыз ету сервисі нақтылы оқиға немесе әрекет куәгерлігінің қамтамасыз етілуі. Істен шықпауды қамтамасыз ету сервисі оқиға немесе іс-әрекетке қатысушылар тарапынан талап етілуі мүмкін. Істен шықпауды қамтамасыз ету сервисімен қорғалған әрекетке, мысалы, мыналарды жатқызуға болады:

– хабарламаны X.400 хаттамасы бойынша жөнелту;

– мәліметтер базасын жазбалармен толықтыру;

– қашықтан орындауға сұрау жасау.

Түпнұсқадан істен шықпауды қамтамасыз ету үшін түпнұсқаны айғақтап, мәліметтің бүтіндігін растау керек. Жеткізуден істен шықпауды қамтамасыз ету үшін қабылдап алушыны айғақтап, мәлімет бүтіндігін растау керек. Кейбір жағдайларда контекстке байланысты істен шықпау куәгерлігі талап етілуі мүмкін (мысалы, күні, уақыты, түпнұсқаны алушының тұрғылықты жері). Бас тарту әрекеті орын алған жағдайда сервис мынадай құралдарды ұстанады:

– куәгерліктің жасалуы;

– куәгерліктің тіркелуі;

– жасалған куәгерліктің айғақталуы;

– куәгерлікті іздеу және қайтадан айғақтау.

Тараптар арасындағы даулы жағдайлар тек қана куәгерлікті алға тартумен ғана шешіле алады. Алайда, даулы мәселенің, даулы оқиғаның немесе іс-әрекеттің болған яки болмағанын куәгерлікті бағалай отырып және оны нақтылайтын соттардың шешуін талап ететін жағдайлар болады. Сот шешімі дауласушы тараптар сот билігін мойындаған кезде ғана тиімді бола алады.

Алға тартылған куәгерлікті соттың қабылдауы үшін, әдетте, оны бір немесе бірнеше сенім білдірілген үшінші жақ куәландыруы қажет. Соттың өзі де куәгерлікке нүкте қоюшы адам ретінде сенім білдірілген үшінші жақ бола алады. Істен шықпауды қамтамасыз ету механизмі сенім білдірілген үшінші жақ пен куәгерлік формаларының көптеген типтерін пайдаланады.

5.2. Сенім білдірілген үшінші жақтың рөлі

Істен шықпауды қамтамасыз ету сервисі бір немесе бірнеше сенім білдірілген үшінші жақты іске қосуы мүмкін. Сервисті қажет еткен сайын істен шықпауды қамтамасыз етудің салғырт өтуін қолдайтын сенім білдірілген үшінші жақ – тәуелсіз сенім білдірілген үшінші жақ деп аталады. Куәгерліктің жасалуына немесе куәгерліктің айғақталуына белсенді түрде қатысушы сенім білдірілген үшінші жақ жедел сенім білдірілген үшінші жақ деп аталады. Жедел сенім білдірілген үшінші жақ, егер ол барлық өзара іс-қимыл байланысында дәнекер ретінде көрінсе, онда ол жапсарлас сенім білдірілген үшінші жақ деп аталады.

Сенім білдірілген үшінші жақ куәгерлікті жинауда, тіркеуге алуда, сондай-ақ куәгерліктің бірдейлілігін айғақтау үшін қажет болуы мүмкін.

Әртүрлі рөлдегі бірнеше сенім білдірілген үшінші жақ қажет болуы мүмкін (мысалы, нотариустың қызметі, мониторинг жасаушы, кілт сертификаттаушы, қол қоюды ұйымдастырушылар, қолды айғақтаушы және жеткізуші ұйым қызметтері. Сенім білдірілген үшінші жақтың біреуі осы аталған рөлдердің біреуін немесе бірнешеуін атқаруына болады.

Куәгерліктің жасалуы кезінде сенім білдірілген үшінші жақ істен шықпауды қамтамасыз ету сервисінен куәгерлік жасауды сұрап отырған жақпен бірлесе жұмыс істейді.

Куәгерлікті тіркеу кезінде сенім білдірілген үшінші жақ куәгерлікті жазып алады, ол кейіннен куәгерлікті пайдаланушыда немесе соттың қолында болуы мүмкін.

Уақытты белгілеу кезінде сенім білдірілген үшінші жаққа уақытты белгілеу сұралған кездегі куәгерлікті жасақтау сеніп тапсырылады.

Мониторинг кезінде сенім білдірілген үшінші жақ іс-әрекеттің немесе оқиғаның ізін бақылап отырады және оған болған жағдайды куәландыруды қамтамасыз ету сеніп тапсырылады.

Кілттерді сертификаттау кезінде сенім білдірілген үшінші жақ істен шықпауды қамтамасыз етуге қажет ашық кілттің дұрыстығын куәлендіру

үшін куәгерлікті жасаушыға қатысты істен шықпаудың сертификаты ретінде әрекет етеді.

Кілттерді таратуда сенім білдірілген үшінші жақ куәгерлікті жасаушыларға немесе куәгерлік верификаторларына кілттер ретінде әрекет етеді. Сол сияқты ол көбінесе симметриялы әдістер қолданылған кезде кілттерді қолдануды шектей де алады.

Қол қоюды ұйымдастыру кезінде сенім білдірілген үшінші жаққа куәгерлік субъектісі атынан сандық қолтаңба түрінде куәгерлік ұсынуға сенім білдіріледі.

Куәгерлікті айғақтау кезінде сенім білдірілген үшінші жақ мәннің сұрау салуы бойынша куәгерлікті тексереді.

Қойылған қолдарды растау кезінде куәгерлікті пайдаланушы сенім білдірілген үшінші жаққа сандық қолтаңба формасындағы куәгерлікті тексеруді сеніп тапсырады.

Ескертпе - қол қоюды ұйымдастыру куәгерлікті жасауда жиі кездесетін жағдай. Қойылған қолды растау куәгерлікті айғақтауда жиі кездесетін жағдай.

Нотариус рөліндегі сенім білдірілген үшінші жақ екі немесе одан да көп мәндер арасындағы және бұрын тіркелген сенім білдірілген үшінші жақ арасындағы мәліметтердің қасиетіне кепілдік береді (мысалы, олардың сақталуына, түпнұсқаға, уақытына немесе олардың қызметіне).

Жеткізуші ұйым ретінде сенім білдірілген үшінші жақ белгіленген мәліметті алушымен бірлесе әрекет етеді және мәліметті алушыға жеткізуге тырысады. Мұнан соң ол мәліметтердің жеткізілгенін, мәліметтердің жеткізілмегенін, немесе жеткізу әрекетінің қолданылғанын, бірақ алуды растау болмағанын растайтын куәгерлік ұсынады. Соңғы жағдайда куәгерлікті пайдаланушы белгіленген алушының мәліметтерді алған-алмағанын анықтай алмайды.

5.3. Істен шықпауды қамтамасыз ету сатылары

Істен шықпауды қамтамасыз ету төрт сатыда жүргізіледі:

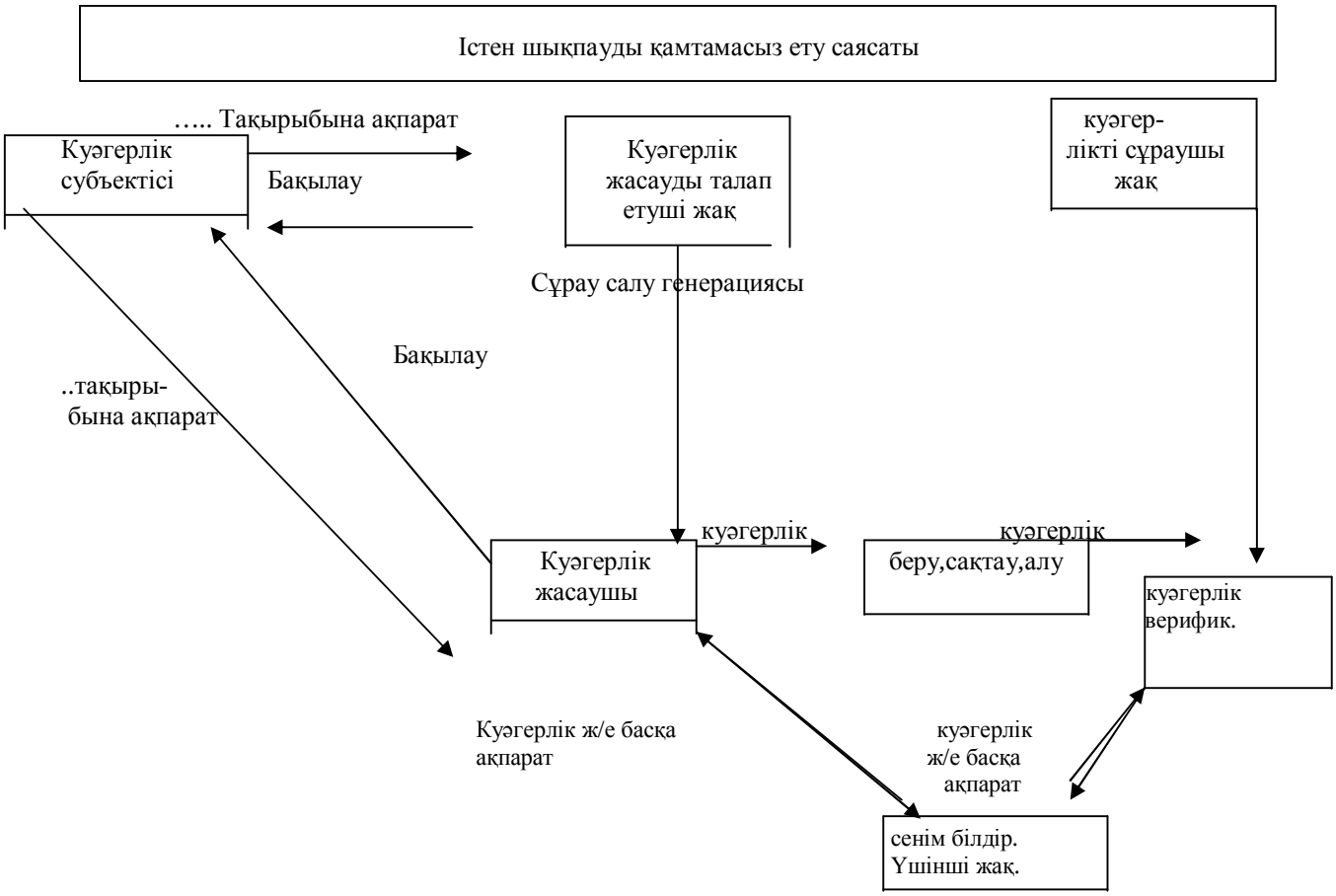
– Куәгерліктің жасалуы;

– Куәгерліктің берілуі, сақталуы және алынуы;

– Куәгерліктің айғақталуы;

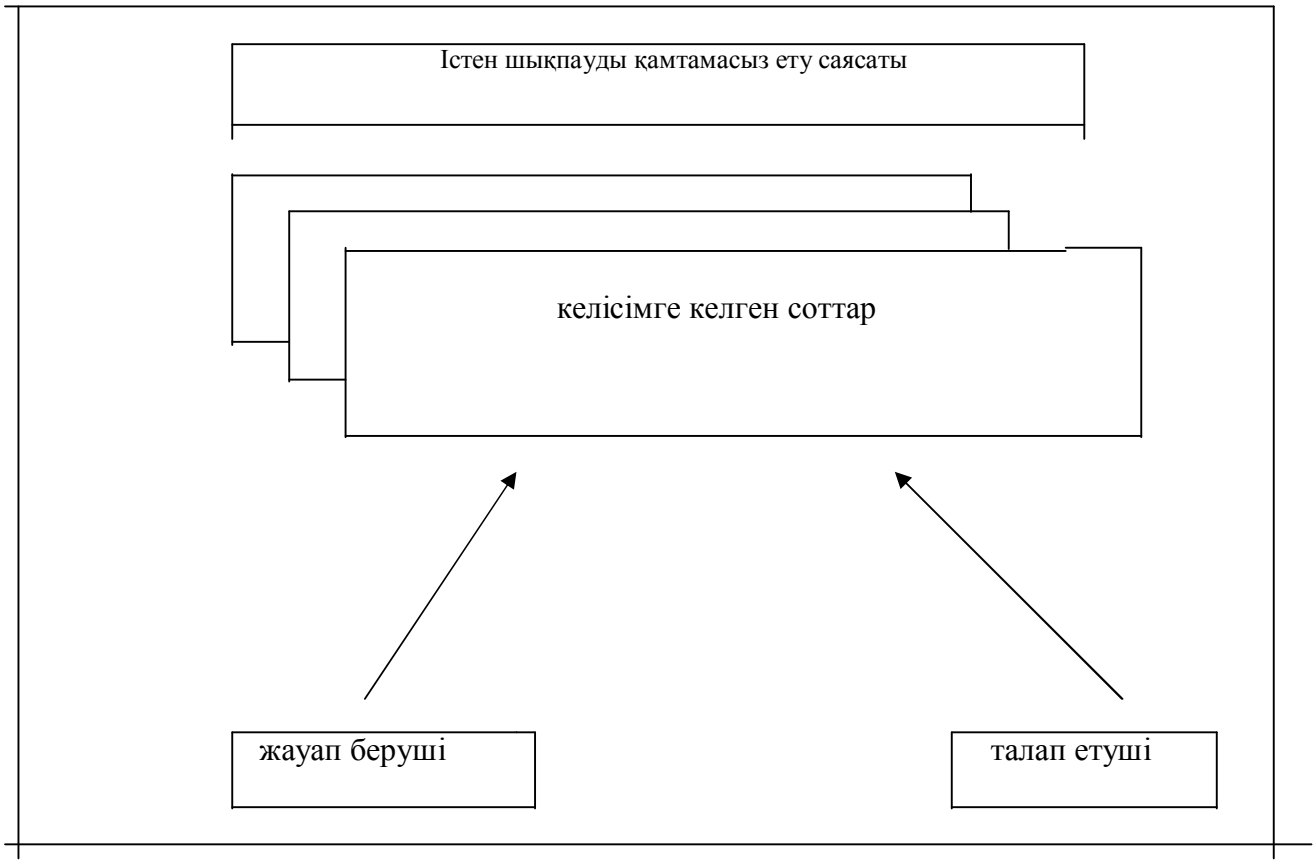
– Даулы жағдайдың шешілуі;

1-суретте алғашқы үш саты көрсетілген; 2-суретте төртінші саты көрсетілген.



Ескертпе - берілген схема көрнекілік мақсатында, ол айқындаушы бола алмайды.

1 сурет – Мәліметтерді жасау, беру, сақтау/алу және айғақтау сатыларына қатысушы мәндер



Ескертпе – берілген схема көрнекілік мақсатында, ол айқындаушы бола алмайды.

2 сурет – Істен шықпауды қамтамасыз ету процесіндегі даулы жағдайдың шешілу сатысы

5.3.1 Куәгерлікті жасау

Куәгерліктің жасалу сатысында куәгерлікті сұратқан тарап куәгерлікті жасаушыдан оқиға немесе іс-әрекеттің куәгерлігінің жасалуын талап етеді.

Оқиға немесе іс-әрекетке қатысы бар деп танылған мән куәгерліктің субъектісі деп аталады. Бұл топтар әртүрлі топтастырылуы мүмкін. Куәгерлік субъектісі мен куәгерлік жасаушы, куәгерлік субъектісі, куәгерліктің жасалуын талап еткен тарап және куәгерлік жасаушы бір мәнге ие болуы мүмкін; немесе куәгерліктің жасалуын талап етуші тарап пен сенім білдірілген үшінші жақ; Куәгерліктің жасалуын талап етуші жақ, куәгерлік жасаушы және сенім білдірілген үшінші жақ. Істен шықпауды қамтамасыз ету сервисінің типтеріне қарай куәгерлікті куәгерлік субъектісі, сенім білдірілген үшінші жақ сервисімен бірлесе отырып немесе бір ғана сенім білдірілген үшінші жақпен бірге жасауы мүмкін.

Ескертпе – істен шықпауды қамтамасыз ету сервисінің контексіне сәйкес келетін типтік куәгерлік қатысушы мәндердің идентификаторларын, мәліметтерін, сондай-ақ уақыты мен күнін де қамтиды. Жеткізілу режимі (мысалы АЖБ -ВОС-тың эталонды моделінің базалық коммуникациясы, мәліметтер базасының сақталуы және одан мәліметтердің алынуы), қатысушы мәндердің тұрғылықты жері, ерекшеленген идентификатор және мәлімет жасаушының “иесі” сияқты қосымша ақпараттар да қосылуы мүмкін.

5.3.2 Куәгерліктің берілуі, сақталуы және алынуы

Осы беріліп отырған сатыда куәгерлік өзара мәндер арасында беріледі немесе сақталу орнына беріледі.

5.3.3 Куәгерліктің расталуы

Куәгерліктің бұл сатысында куәгерлікті пайдаланушының сұрауы бойынша куәгерлік верификациясы арқылы тексеріледі. Даулы жағдай туа қалған жағдайда ұсынылған куәгерлік шын мәнінде жеткілікті болатынына куәгерлікті пайдаланушының көзін жеткізу үшін осы саты қажет. Ақпарат ұсынылған кезде куәгерлікті растау үшін сенім білдірілген үшінші жақтың сервисі қосымша қатысуы мүмкін. Куәгерлікті пайдаланушы мен куәгерлік верификаторы бір ғана мәнге ие болуы мүмкін.

5.3.4 Даулы жағдайдың шешілуі

Даулы жағдайдың шешілуі сатысында тараптар арасындағы даулардың шешілуіне соттар жауапты. Дауласушы тараптар кейде талап етуші және жауап беруші деп аталады. Даулы жағдайдың шешілу сатылары 2 - суретте көрсетілген.

Сот даулы жағдайды шешу барысында дауласушы тараптардан және/немесе сенім білдірілген үшінші жақтан куәгерлік жинайды. Соттың даулы мәселелерді шешу үшін қолданатын процесі осы стандарттың таралу аймағынан тысқары болады.

Бұл саты әрдайым міндетті емес. Егер барлық мүдделі тараптар оқиға немесе іс-әрекет болды (немесе болмады) деп өзара келіссе, онда ешқандай да даулы ситуация туындамайды. Онан әрі, тіпті пайда болған даулы жағдайдың өзін тараптар сотты қатыстырмай-ақ шешуі мүмкін. Мысалы, дауға қатысушы тараптардың бірі адал болып, бірақ қателескен болса, онда оны қарсы жақ түсінуі мүмкін: ол үшін оған басқа тараптың куәгерлігі тағылуы керек.

Істен шықпауды қамтамасыз ету сервисін сұраған сайын бұл саты қажет болмауы да мүмкін, ол үшін істен шықпауды қамтамасыз етудің барлық тетіктері даулы жағдайдың шешілу сатысын қолдауы қажет. Яғни, олар даулы ситуация туындаған жағдайда оның шешілуін қамтамасыз етуге тиіс.

5.4. Істен шықпауды қамтамасыз ету сервисінің кейбір типтері

Істен шықпауды қамтамасыз ету сервисінің көптеген типтері бар. Көбінесе істен шықпауды қамтамасыз ету сервисінің мәліметтерді берумен байланысты түрлері жиі қолданылады. Ақпарат жіберуде кем дегенде екі мән қатысады, олардың бірі жіберуші де, екіншісі қабылдап алушы. Бұл жағдайға қатысты мынадай потенциалды даулы жағдайлар туындайды:

Мұндай шабуылды білген кезде мүмкіндігінше фактінің қасақана алмастырылғаны жөнінде кеңінен жария ету қажет, бірақ куәгерлікті пайдаланушылардың бәріне қасақана алмастырылған кілттің көмегімен тексеруге болатын ақпаратты жеткізу мүмкін бола бермейді.

Қандай куәгерліктің қасақана алмастыруды ескерткенге дейін тексерілгенін тексерілген куәгерліктің тіркеу журналын жүргізе алатын куәгерлікті тексеру ұйымдарының көмегімен (мысалы, қол қоюды тексеру ұйымы арқылы) анықтау қажет. Мұндай тәсілмен қандай куәлік ескертпеге дейін, қайсысы ескертпеден кейін тексерілгенін білуге болады.

Егер тексеру кілті ашық кілт болған болса, онда оның қасақана алмастырылғаны аян болысымен-ақ дереу басқасымен ауыстыру қажет.

– жіберушінің оқиғаға қатысы жоқ екендігін айғақтау барысында кездесетін даулы жағдайлар, мысалы, күдікті жіберушінің алушы немесе белгісіз бұзушының хабарды ұрлап алды деп шағымдануы;

– алушының оқиғаға қатысы жоқ екендігін айғақтау барысында кездесетін даулы жағдайлар, мысалы, күдікті алушы хабарды жібермеген немесе жіберу барысында жоғалған, немесе белгісіз бұзушы алды деп шағымдануы;

Хабарды жіберу барысында туындайтын даулы жағдайлар түрлері бойынша істен шықпауды қамтамасыз ету сервисін (шешуге көмектесетін) жіктеуге болады.

Жіберушінің алушыға хабар жіберілуі мына төмендегі жеке оқиғалар ізімен қарастырылады:

– жіберушінің жіберу агентіне хабар жіберуі;

– жіберу агенттері арасында хабар жіберілуі (бірнеше жіберу агенттері болатын болса);

– жіберу агентінен алушыға хабар жіберілуі.

Осы оқиғалардың әрқайсысына байланысты істен шықпауды қамтамасыз ету сервистерінің қарастырып отырған оқиға куәлігін көрсететін бірнеше типтері бар. Сол себепті істен шықпауды қамтамасыз етудің қосымша типтері:

– жіберілген хабардың істен шықпауын қамтамасыз ету агентінің хабарды алып жіберу кезінде жалған бас тартуынан қорғау үшін (немесе жіберушіден, немесе өзге жіберуші агенттен);

– тасымалданған хабардың істен шықпауын қамтамасыз ету – фактіні жіберуде агенттің жалған бас тартуынан қорғау үшін (немесе алушыға, немесе өзге жіберуші агентке).

Ескертпе – хабардың жіберілуі мен тасымалдануы хабардың мәніне жауапкершілікке немесе хаттың мағынасындағы ақпаратты ұғынуына кепілдік бермейді.

5.5 АЖБ үлгілері бойынша істен шықпаудың куәланған мысалдары

Қолданылған сервистер бойынша істен шықпауды қамтамасыз ету төмендегі әрекеттер мен оқиғалардың әрқайсысы куәліктің белгілі бір типтерін талап етеді.

5.5.1 Істен шықпау көздерінің қамтамасыз етілуі

Куәлік мына құрамбірліктерді қамтуы тиіс (қол қоюға болатын немесе нотариалды түрде расталған):

– жіберушінің айырмалық идентификаторы;

– жіберілген мәліметтер немесе олардың сандық белгісі.

Куәлік сонымен қатар мына компоненттерді қамти алады:

– алушының айырмалық идентификаторы;

– жіберілген мәліметтердің мерзімі мен уақыты.

5.5.2 Жеткізілген нәрсенің істен шықпауының қамтамасыз етілуі

Куәлік мына құрамбірліктерді қамтуы тиіс (қол қоюға болатын немесе нотариалды расталған):

– жіберушінің айырмалық идентификаторы;

– жіберілген мәліметтер немесе олардың сандық белгісі.

Куәлік сонымен қатар мына құрамбірліктерді қамти алады:

– алушының айырмалық идентификаторы;

– жіберілген мәліметтердің мерзімі мен уақыты.

Куәлік сонымен қатар жеткізуші органын пайдалану барысында мына құрамдарды қамти алады (қол қоюға болатын немесе нотариалды расталған):

– жеткізуші органының айырмалық идентификаторы;

– жеткізуші органының бірінші рет жіберу әрекетінің мерзімі мен уақыты;

– алушының алуға дайындық сигналын қабылдауының мерзімі мен уақыты;

– жіберуші органының жіберуді орындау мерзімі мен уақыты;

– жіберу органының жіберуді орындай алмаған жағдайдағы мерзімі мен уақыты;

– жіберудің мүмкін емес болған жағдайдағы кездесетін себептер (мысалы, байланыс каналының үзілуі);

– қанағаттандырылған хабар жіберу процесіндегі талап етілген өңдеу белгісі.

6 Істен шықпауды қамтамасыз ету саясаты

Істен шықпауды қамтамасыз ету саясатына мыналар кіреді:

1. Куәліктің құрылу ережесі, мысалы, істен шықпауды қамтамасыз ету куәлігінің құрылуы үшін әрекеттер тобының спецификациясы; куәлік құрудағы әрекеттердің СБҮЖ спецификациясы; СБҮЖ-бен орындалудағы рөлдер; куәлік құрудың мәнін қамтитын іс-шаралар.

2. Куәлікті растаудың ережесі, мысалы, куәлікті қанағаттандыра алатын СБҮЖ спецификациясы мен әрбір куәлік нысанын СБҮЖ үшін екендігі мойындалады.

3. Куәлікті сақтау ережесі, мысалы, сақталудағы куәліктің сақтығын қамтамасыз етудегі қолданылған тәсілдер.

4. Куәлікті пайдаланудың ережесі, мысалы, куәлікті пайдаланудағы міндеттердің спецификациясы

Ескертпе – істен шықпауды қамтамасыз етудің кейбір тетіктерінде куәлікті қолданудың рұқсат етілмеуінің алдын алу қиындықтары болуы мүмкін.

5. Сот шешімдерін қабылдау ережесі, мысалы, даулы жағдайларды шеше алатын төрешілердің келісілген спецификациясы

Бұл әрбір ережелер топтамасы жеке орган арқылы анықталады. Мысалы, куәлікті құру ережесі жүйе иесі арқылы анықталады, ал, сот шешімдерін қабылдау ережесі ел заңымен анықталады.

Егер саясаттың әртүрлі бөліктері сәйкес келмеген уақытта, істен шықпауды қамтамасыз ету сервисі дұрыс жұмыс жасамауы мүмкін, мысалы даулы жағдайды шешу барысында шын мәнінде болған оқиғаны теріске шығарып мойындамау.

Төреші даулы жағдайларды шешу барысында істен шықпауды қамтамасыз ету саясатын қолдануы мүмкін. Мысалы, төреші істен шықпауды қамтамасыз ету саясаты мен куәліктің сәйкес келуін қарастыруы мүмкін.

Қауіпсіздік саясатының қалыптасуы айқын немесе белгісіз түрде анықталып жүзеге асырылады. Істен шықпауды қамтамасыз ету саясатының айқын тапсырмасы (мысалы, кәдімгі тілдегі құжаттарда) саясаттың түрлі бөліктері арасындағы даулы мәселелерді анықтаумен қатар, төреші шешіміне де көмектесе алады.

Істен шықпауды қамтамасыз ету саясаты сонымен қатар, куәліктің компреметациялық жағдайымен немесе компреметацияның жағдайымен

немесе куәлікті құрудағы пайдаланылған кілттердің жойылуымен байланыста болуы мүмкін.

Істен шықпауды қамтамасыз ету саясаты тәуелсіз қауіпсіздіктер немесе жоғары сатыдағы қауіпсіздіктер деп өзара қауіпсіздіктер арасындағы келісімнің нәтижесі болып табылады.

7 Ақпарат және істен шықпауды қамтамасыз ету құралдары

7.1 Ақпарат

Даулы мәселелерді шешуде пайдалануға арналған ақпарат осы құжатта куәлік деп аталады. Куәлік куәлікті пайдаланушының өзімен немесе сенімді үшінші жақ иесімен сақталады. Сандық қолтаңба, қорғалған конверт пен қауіпсіздік маркері куәліктің нақты формалары ретінде саналады. Сандық қолтаңбалар ашық кілт технологияларымен, қорғалған конверттер мен қауіпсіздік маркерлері құпия кілттердің технологиясымен пайдаланылады. Куәлікке жататын мысал ретінде мына ақпараттар қамтылуы мүмкін:

– істен шықпауды қамтамасыз ету саясатының идентификаторы;

– жіберушінің айырмалық идентификаторы;

– алушының айырмалық идентификаторы;

– сақтандырылған конверттегі сандық қолтаңбасы;

– куәлікті құрушының айырмалық идентификаторы;

– куәлік құрудағы сұралатын екі жақтың айырмалық идентификаторы;

– хабарлама немесе хабарламаның сандық қолтаңбасы;

Ескертпе – егер хабарламаның орнына оның сандық қолтаңбасы қолданылса, қолтаңбаны алу үшін оны анықтайтын тәсіл қажет.

– хабарлама идентификаторы;

– қауіпсіздік маркерін растау үшін құпия кілттің нышаны болуы қажет;

– сандық қолтаңбаны растау үшін нақты ашық кілттің белгісі болуы қажет (мысалы, КО айырмалық идентификаторы және сертификаттың реттік саны);

– СБҮЖ уақытын таңбалайтын, нотариустың айырмалық идентификаторы;

– куәліктің бірегей идентификаторы;

– куәлікті тіркеудің немесе орналастырудың уақыты мен мерзімі;

– сандық қолтаңба мен қауіпсіздік маркерінің жасалуының уақыты мен мерзімі.

7. 2 Істен шықпауды қамтамасыз ету құралдары

Бұл бөлім істен шықпауды қамтамасыз етуді құру, жіберу, куәлікті растау немесе СБҮЖ куәлігін орнату сияқты түрлі тәсілдерін пайдалануды анықтайды.

7.2.1 Басқарумен байланысты тәсілдер

Істен шықпаудың қамтамасыз етілуін басқару тәсілдері болып табылатын ақпаратты бөлу, пароль немесе кілт (кілтпен басқарумен бірге) т.б. істен шықпауды қамтамасыз ету үшін қажетті тәсілдер болып саналады. Аталған нұсқалар арқылы істен шықпауды қамтамасыз ету үшін қарастыруға арналған өзара мәндер мен басқа да мәндерді байланыстырудың кейбір хаттамаларын қолдана алады. Істен шықпаудың қамтамасыз етілуін басқару процесі сонымен қатар, куәлікті алуда пайдаланылатын кілттердің жойылуын қамтиды.

Істен шықпаудың қамтамасыз етілуін басқару тәсілдері пайдаланушыға істен шықпауды қамтамасыз ету үшін ақпаратты алуға, өзгертуге, жоюға мүмкіндік береді. Жалпы айтқанда, бұл тәсілдер:

– ақпаратты басқару тәсілдерін орнату;

– ақпаратты басқару тәсілдерін өзгерту;

– ақпаратты басқару тәсілдерін жою;

– ақпаратты басқару тәсілдерін аудару амалдарын жүзеге асырады.

Істен шықпауды қамтамасыз ету сервисін қолдау – басқарумен байланысты келесі әрекеттерге әкеп соғады:

– тіркеу журналындағы оқиғаларды тіркеу;

– даулы жағдайларда қабылданған шешім қорытындысын тіркеу;

– оқиғаның жекеленген хабарландыруы;

– оқиғаның жойылған хабарламасы.

Әрбір оқиғаға байланысты қабылданған нақты әрекеттер істен шықпаудың қамтамасыз етілуінің саясатына байланысты болады.

7.2.2 Жұмыспен байланысты тәсілдер

7.2.2.1 Куәлікті құру тәсілдері

Бұл тәсіл куәлікті құруға арналған. Куәлік еш кедергісіз (СБҮЖ-тің көмегінсіз) бір немесе бірнеше СБҮЖ арқылы куәлік субъектісі құрыла алады.

Куәлікті құру тәсілдерінің керекті мәліметтері:

– істен шықпауды қамтамасыз ету саясаты;

– куәлік субъектісінің айырмалық идентификаторы;

– істен шықпауды қамтамасыз ету сервисіне қарайтын мәннің айырмалық идентификаторы;

– мәліметтер немесе сандық қолтаңба;

– сандық қолтаңба, қауіпсіздік маркері немесе басқа куәлік жасауға арналған СБҮЖ-дің айырмалық идентификаторы.

– Куәлікті құру тәсілдерінің керекті мәліметтері:

– куәлік (мысалы, сандық қолтаңба мен қауіпсіздік маркері);

– сандық қолтаңба, қауіпсіздік маркері немесе басқа куәлік құрудағы СБҮЖ-тің айырмалық идентификаторы.

7.2.2.2 Уақыт белгісін құру тәсілдері

Бұл тәсілдер уақыт дәлдігін құру үшін арналған:

Уақытты анықтауды құру үшін арналған керекті мәліметтер:

– уақыт дәлдігін сұрайтын мәннің айырмалық идентификаторы;

– уақыт таңбасын жүзеге асыру үшін СБҮЖ-тің айырмалық идентификаторы;

– мәліметтер (мысалы, қол қойылған хат, түбіршек), немесе сандық қолтаңба, немесе мәліметтердің сандық көшірмесі.

Уақытты таңбалаудағы керекті мәліметтер:

– екінші жақтың қойылған қолтаңбасы, үшінші адамның сенімі арқылы;

– қарсы жақтың қолтаңбасын белгілеу үшін әдісті немесе криптографиялық алгоритмді таңбалау (мәліметтердің немесе сандық қолтаңбаның пайданылғаны туралы да көрсетіледі);

– уақытты таңбалау сервисінің айырмалық идентификаторы;

– уақыт таңбасын құру үшін мерзімі мен уақытына сұраныс алу;

– қарсы жақтың қойылған қолтаңбасының уақыты мен мерзімі;

– уақыт таңбасы мен мәліметтердің сандық қолтаңбасы қойылған хат.

7.2.2.3 Нотариалды түрде расталған куәлікті жасау тәсілдері

Бұл тәсіл СБҮЖ-де куәлікті орналастыру үшін пайдаланылады.

Бұл тәсілдердің керекті мәліметтері:

– кәулікті жасауда сұралатын екі жақтың айырмалық таңбалары;

– куәлік (мысалы, сандық қолтаңба немесе қауіпсіздік маркері);

– куәлікті жасаушының айырмалық идентификаторы;

– істен шықпауды қамтамасыз ету саясатының айырмалық идентификаторы.

Керекті мәліметтер мыналардан тұрады:

– куәліктің тіркеу нөмірі;

– куәлікті тіркеудің уақыты мен мерзімі.

7.2.2.4 Куәлікті растау тәсілдері

Бұл тәсіл куәлікті растау үшін пайдаланылады.

Бұл тәсілдердің қажетті мәліметтері:

– куәлік;

– куәлік субъектісінің айырмалық идентификаторы;

– куәлікті пайдаланушының айырмалық идентификаторы;

– куәлікті тексеру үшін қолданылатын кілт идентификаторы;

– куәлікті таңбалау белгісі (істен шықпауды қамтамасыз ету саясатының қоданылған куәлігін бағалау үшін және оның сәйкестігін анықтау үшін;

Керекті мәліметтер:

– тексерудің нәтижесі (дұрыс немесе дұрыс емес);

– куәлік субъектісінің айырмалық идентификаторы;

– куәлікті жасаушының айырмалық идентификаторы;

– куәлікті тексеруді талап ететін мәннің айырмалық идентификаторы;

– сандық қолтаңба мен қауіпсіздік маркерін тексеретін СБҮЖ айыру идентификаторы;

– мәліметтер немесе олардың сандық көшірмесі.

7.2.2.5 Куәлік жасау тәсілдерін СБҮЖ құрылғысының көмегімен жіберу

Мәліметті немесе түбіршекті жіберудің орнына жіберуші мен алушының арасына мәліметтер СБҮЖ арқылы жіберілуі мүмкін, сондықтан да істен шықпау куәлігі осы СБҮЖ арқылы жіберілуі мүмкін. Бұл тәсіл сонымен қатар, алынған мәліметтерді мойындамау үшін байланыс каналының үзілуі туралы жалған ақпарат беру кезінде пайдаланылады.

СБҮЖ құрылғысының бұл тәсілін пайдалану үшін қажетті өлшемдер:

– мәліметтер;

– алушының айырмалық идентификаторы;

– Бұдан басқа да өлшемдер берілуі мүмкін:

– мәліметтердің сандық қолтаңбасы;

– жіберушінің айырмалық идентификаторы;

– сандық қолтаңба;

– СБҮЖ құрылғысының айырмалық идентификаторы;

– Істен шықпауды қамтамасыз ету саясаты.

– СБҮЖ-тің мәліметтері деп саналатын көрсеткіштер:

– үшінші жақтың сенімді адамының айырмалық идентификаторы;

– алушының айырмалық идентификаторы;

– куәліктің тіркелу нөмірі;

– тіркелудің уақыты мен мерзімі;

– мәліметтер немесе олардың сандық қолтаңбасы.

8 Істен шықпауды қамтамасыз ету тетіктері

Істен шықпауды қамтамасыз ету сервисі сандық қолтаңба, шифрлеу, түпнұсқа екендігін анықтау механизмдері, басқа сервистердің уақыт пен мерзімді таңбалауда қолдауы сияқты тетіктердің көмегімен жүзеге

асырылады. Істен шықпауды қамтамасыз ету үшін криптографиялық алгоритмдердің симметриялық және ассиметриялық түрлері пайдаланылады. Істен шықпауды қамтамасыз ету сервисі қауіпсіздік талаптарына сәйкес тетіктер мен сервистер комбинациясын пайдалана алады.

Бұл бөлім істен шықпауды қамтамасыз ету сервисін пайдалану тетіктерін және тетікке төнген қауіптерді суреттейді.

8.1 СБҮЖ қауіпсіздік маркерінің көмегімен істен шықпауды қамтамасыз ету (қорғалған конверт)

Бұл істен шықпау куәлігінің механизмі қауіпсіздік маркері мен СБҮЖ-ға ғана әйгілі бекітілген құпия кілттен тұрады. Сенімді үшінші жақ куәгердің сұранысы бойынша куәлікті пайдаланушы мен төреші үшін СБҮЖ-тің тексеруі нәтижесінде қауіпсіздік маркері құрады. Бұл жағдайда СБҮЖ куәлік жасаушы және куәлік верификаторы есебінде саналады.

Куәлікті құруды талап ететін жақ сенімді үшінші жаққа мәліметтерді немесе оның көшірмесін қауіпсіздік маркерін генерациялау сұранысымен бірге жібереді. Сұраныстың бүтіндігі қорғалуы тиіс (мысалы, бітеу арқылы) сонымен қатар, сұраныстың құпиялығы қорғалуы тиіс (мысалы, шифрлеу арқылы). Бүтіндікті сақтайтын қауіпсіздік маркерлері - қорғаныс конверттері деп аталады.

Қауіпсіздік маркерін пайдаланудағы керекті мәліметтер:

– тәсілді белгілеу немесе криптографиялық алгоритмдерді қауіпсіздік маркерінің бүтіндігін қамтамасыз ету үшін қолданылады;

– тәсілді белгілеу немесе криптографиялық алгоритмдерді қауіпсіздік маркерінің құпиялылығын қамтамасыз ету үшін қолданылады;

– куәлік субъектісінің айыру идентификаторы;

– куәлікті құруда сұралатын екі жақтың айыру идентификаторы;

– істен шықпауды қамтамасыз ету кезінде қолданылатын саясат;

– оқиға немесе әрекет уақыты мен мерзімі;

– оқиға мен әрекетті суреттейтін мәліметтер.

– Керекті мәліметтер мыналардан тұрады:

– қауіпсіздік маркері

– қауіпсіздік маркерін құрудың уақыты мен мерзімі.

8.2 Істен шықпауды қамтамасыз ету үшін қауіпсіздік маркері мен модульдерді бөгде нәрсенің араласуынан қорғау барысында пайдалану

Бұл істен шықпау тетіктерінің куәлігі бөгде нәрселердің араласуынан қорғалған криптографиялық модульдердің ішінде сақталған бекітілген құпия кілттен тұрады. Оны тек куәлік құрушы мен куәлік верификаторы

және төреші ғана пайдалана алады. Бөгде нәрсенің араласуынан қорғалған модульдер құпия кілт арқылы жасалатын операция түрлерінен шектейді және модульден тыс кілт мағынасын ашудан қорғайды.

Куәлік құрушы модулін құпия кілтті бекітілген маркер құруда пайдалануға рұқсат етіледі. Ал, куәлік верификаторы мен төреші ие болған модульдер арқылы тек маркерді тексеруге ғана рұқсат етіледі. Барлық қатысушы жақтар модульді құпия кілт бөгде нәрсенің араласуынан қорғау мақсатында дұрыс орнатылды деп есептелуі тиіс, өйткені, бір құпиялы кілт тек бір мәнмен ғана қолданылады алады. Ал, басқа мәндер арқылы кілт тек куәлікті тексеру мақсатында ғана қолданыла алады.

Куәлікті қолдануда даулы жағдайлар туылған кезде пайдаланушы бекітілген маркерді төрешіге көрсете алады және де оны тек куәлікті құрушы модульдің көмегімен ғана іске асатынын, ал осы кілттің мазмұнын құрайтын басқа модульдердің қауіпсіздік маркерін құруға мүмкіндігі жоқ.

8.3 Сандық қолтаңбаны пайдалану арқылы істен шықпаудың қамтамасыз етілуі

Бұл схемада істен шықпау куәлігі мәліметтер құрылымынан тұрады. Қолтаңбаны жасау барысында қол қою кілті пайдаланылады, ал тексеру кезінде – тексеру кілті пайдаланылады.

Қауіпсіздік саясатына байланысты уақыт туралы ақпараттың қажеттігі туындайды. Ол уақытты белгілеу органының қызметін атқаратын СБҮЖ-дің немесе мәнді қамтамасыз ететін сандық қолтаңбаның құрамына енеді. Егер уақыт белгісі СБҮЖ-ге жіберілмеген жағдайда басқа мәндер оған сенуге тиісті емес. Егер төрешіге даулы жағдайды шешу үшін уақыт белгісі немесе мәтіндік ақпарат қажет болса, бұл ақпарат сенімді көздерден алынуы тиіс (мысалы, сенімді үшінші жақтан).

Сандық қолтаңба қолтаңба құрушының қызметін атқаратын куәліктің субъектісі немесе СБҮЖ арқылы жасалады.

Куәлік субъектісі арқылы жасалған сандық қолтаңба тікелей сандық қолтаңба деп аталады. СБҮЖ-дің арқылы жасалған куәлік субъектісінің сандық қолтаңба тетігі жанама сандық қолтаңба деп аталады.

Егер қолтаңбаны тексеруге арналған сертификат кері шақырылса, онда даулы жағдайларды шешу үшін бір ғана сандық қолтаңба жеткіліксіз болып саналады. Осындай жағдайларды шешу үшін төрешіге сандық қолтаңбаны жасау кезінде сертификаттың істеп тұрғанын көрсететін ал, одан кейін сертификаттардың күші жойылғаны туралы куәлікті қосымша көрсету қажет (мысалы, кері шақырылған сертификаттар тізімі, CRL). Бірақ та егер жабық кілттің иесі әдейі қасақана уақытты дұрыс көрсетпесе немесе қастық ойлаушы қол қоюға арналған жабық кілтті қасақана пайдаланатын болса бұл схема мұндай даулы жағдайларды шеше алмайды. Мұндай даулы жағдайларды шешу үшін қосымша уақытша сенімді үлгі-нұсқаны немесе

уақытты таңбалау қызметін уақытша атқарушы СБҮЖ-дің қолын пайдалану керек (Д қосымшасын қараңыз).

Куәлік верификаторы тексеру процесіне қажетті ақпаратты алу үшін каталогтар сервисін пайдалануы мүмкін (қауіпсіздік сертификаты сияқты). Куәлік верификаторы куәлік құрушының ашық кілтін иеленуі керек. Бұл кілт қауіпсіздік сертификатының сақтау каталогында сақталады. Бірнеше сертификаттың қажеттігі туындау мүмкін. Сертификаттың жұмыс істейтініне көз жеткізу үшін кері шақырылған пайдаланыла алатын сертификаттардың тізімін сұрау керек. Аталған әрекеттерді әрбір сертификаты бар куәландыратын орталықтарға арнайы жасау қажет ([2]-ні қараңыз).

Куәлікті пайдаланушы қолын растау үшін қолтаңбаны тексеру қызметін атқарушы СБҮЖ-тің көмегіне жүгіне алады. Бұл сенімді үшінші жақ хабарламаның түпнұсқасының (хабарламаның сандық көшірмесі, егер қолданылатын болса) немесе сандық қолтаңбасының сәйкестігін тексереді.

Бұл жағдайда СБҮЖ қызметі куәлікті пайдаланушыны қолтаңбаны тексеру процесінің қиындықтарынан босату үшін және болашақтағы сұраныстардың реакциясын оңтайландыру үшін алдыңғы сұраныстың нәтижесін сақтауды қамтамасыз ету қажет. Бұл үшін СБҮЖ каталогпен өзара байланысты қажет етеді. Қолтаңбаны тексеруші қызметін атқарушы СБҮЖ ашық кілтті немесе бір КО-ны сақтайды деп жорамалданады. Сенімді үшінші жақ сонымен қатар бұрыннан бар әртүрлі куәландыратын орталықтардың сенім қарым-қатынасын ескеруі мүмкін

8.4 Уақытты таңбалау арқылы істен шықпауды қамтамасыз ету

Егер уақытша сенімді үлгі-нұсқа қажет болған жағдайда, егер сандық қолтаңба мен қауіпсіздік маркерін жасайтын мәнге берілген сағатқа сенуге болмайтын болса, уақытты таңбалауды қамтамасыз ететін сенімді үшінші жақтың көмегін пайдалану керек. Уақытты таңбалау кілт қолтаңбасының атына кір келтіруге дейінгі хабарламаның қол қойылу ақиқатын анықтау үшін және бұл хабарламаның алаяқтық емес екендігін айқындау үшін пайдаланылады. Уақытты таңбалау қызметін атқару барысында сенімді үшінші жақ хабарламаның алған уақытын айқындау үшін сандық қолтаңба мен қауіпсіздік маркерін қамтамасыз етеді. Уақытты таңбалау куәлікті жасаушы арқылы, істен шықпауды қамтамасыз ету сервисінің көмегіне жүгінген жақ арқылы, куәлікті пайдаланушы арқылы, куәлік верификаторы арқылы сұралуы мүмкін.

Уақытты таңбалау уақыт, мерзім және пломба немесе сандық қолтаңбаны мәліметтерге қосады. Уақытты таңбалау уақыт белгісін сұрайтын мәннің аутентификациясын керек етпейді. Куәлік верификаторы қауіпсіздік саясатының тапсырылуымен уақыт белгісінің диапазоны жететін аумақ шеңберінде тұрған тұрмағанын анықтау қажет.

Қолтаңба жасау процесі мен маркер құру процесімен уақытты таңбалаумен біріге алады. Егер сандық қолтаңба жасаушы мәннің, сенімді де берік сағаты болған жағдайда қарсы қолтаңба қажет болмайды.

8.5 Қосылған сенімді үшінші жақты пайдалану арқылы істен шықпауды қамтамасыз ету

Сенімді үшінші жақтың тәсілдері нақты оқиғалар мен әрекеттерге арналып сұралады немесе ашық көрсетілмейді. Құрамалы СБҮЖ істен шықпауды қамтамасыз ететін сервистің барлық бірлескен әрекеттерінде жүзеге асырушы ретінде әрекет етеді, сонымен қатар, куәлікті пайдаланушыға куәліктерді көрсете алады.

Қалай болған жағдайда да, құрамалы СБҮЖ мәліметтерді жіберумен қатар, оқиға мен әрекетті қадағалап отырады.

Алдында кездескен даулы жағдайларды шешу үшін жазбаларды сақтау сенімді үшінші жаққа сеніп тапсырылады. Мәліметтердің немесе олардың сандық көшірмелерінің сенімді үшінші жақта сақталуы куәлік ретінде қызмет етуі мүмкін.

8.6 Нотариусты пайдалану арқылы істен шықпаудың қамтамасыз етілуі

АЖБ моделіндегі мәліметтердің екі немесе одан көп мәндер арасында берілетін тұтастық, қайнар көз, уақыт, міндет сияқты қасиеттері нотариалды түрде растау механизмімен кепілдікке алынады. Қатысушы мәндер қажетті ақпараттарды нотариусқа сеніп сақтайды. Алдыда кездескен даулы жағдайларды шешу үшін жазбаларды сақтау куәгерліктің көмегімен кепіл болып қамтамасыз етіледі. Нотариустың сервисін қолдау барысында сандық қолтаңба, шифрлеу, бүтіндіктің бақылау тетіктері сәйкестіріп пайдаланылады.

Куәлікті құрудың қызметін атқарушы нотариус мәліметтердің қасиеттеріне кепілдік бере отырып куәлікті тіркейді. Сонымен қатар, куәлікті идентификациялауда тіркеу номері пайдаланылады.

Куәлікті тексеру қызметін атқарушы нотариус куәліктің әрекет етуін растайды.

8.7 Істен шықпауды қамтамасыз ету процесіндегі қауіп-қатерлер

Істен шықпауды қамтамасыз ету механизмінің бірде-бірі қауіп-қатерлерден мүлде ада деп айтылмайды. Егер СБҮЖ ұйғарымнан тыс өзін басқаша ұстайтын болса, СБҮЖ-ті қосатын тетіктер қауіпті болуы мүмкін. Мұндай жағдай кенеттен істен шығу болған кезде немесе сырт жақтан болған шабуыл нәтижесінде болуы мүмкін. Бұл қауіп-қатерлер маңызды болса да осы стандартта талқыланбайды. Істен шықпауды қамтамасыз ету тетіктері СБҮЖ-тің дұрыс жұмыс жасамауынан және де СБҮЖ-тің

оңайлықпен хаттаманы істен шығаруы деп бөлінеді. Тетіктер таңдауда жіберілетін қауіп-қатерді айқындау арқылы қауіп-қатердің қайсысы болуы ықтимал екендігін, ал кейбір қауіп-қатердің маңызды зардаптарға әкеп соғатынын бағалау арқылы айқындау қажет. Төменде болуы ықтимал қауіп-қатерлердің мысалдары туралы және оған қарсы әрекеттер туралы талқыланады.

8.7.1 Кілттерге зиян келтіру

8.7.1.1 Мәнге жататын кілт жасаудың зиян шегуі

Кілтті рұқсатсыз пайдалану кезінде және оның заңды иегер арқылы айғақталуы барысында мынадай қауіптің пайда болуы мүмкін: бұзушы куәлікті құру үшін кілтті рұқсатсыз пайдалануы мүмкін, және ол куәлікті пайдаланушылар үшін әрекет етуші деп табады. Істен шықпауды қамтамасыз ету механизмінің куәлікті құру кілтін дұрыс пайдаланбағандықтан болған қандай да бір зақым дер кезінде қайта іске қосыла алмайды. Бірақ та куәлікті құру органының көмегімен жоғалған заттардың деңгейін анықтай алады (мысалы, қолтаңбаны жасау органы арқылы), сонымен қатар, құрылған куәліктердің қай уақытта және қай кезде құрылғандығы туралы мәліметтерді тіркеу журналынан тауып алуға мүмкіндік береді. Кілтке жасалған қастандық туралы мүмкіндік болғанынша барлық куәлік алушыларға хабарландырулар жіберілу керек, бірақ та кейбір жағдайда куәлікті пайдаланушылардың рұқсатсыз кілттің көмегімен құрушылардан сақтанып отыру керек.

Кілтті рұқсатсыз пайдалану заңды иесі арқылы анықталады, онда жағдайда құру кілтінің күші міндетті түрде жойылуы қажет. Егер кілт жабық кілт болатын болса, сәйкес ашық кілттің сертификатын шақыру керек. Бұл [2]-де анықталған шақырылған сертификаттар тізімі арқылы жүзеге асуы мүмкін. Бірақ бұл жеткіліксіз болып табылады, өйткені кілтпен қастандық жасау әрекеттерін тоқтата алмайды. Куәлікті құру СБҮЖ-бен және куәлік субъектімен бірігіп жұмыс істеуді талап ете отырып істен шықпауды қамтамасыз ету механизмін пайдалану арқылы бұл қатерге қарсы тұра алады. Мысалы, жанама сандық қолтаңбаны немесе уақытты таңбалау органының қарсы қолын пайдалану арқылы бұл қауіп түрінен сақталынады. Бұл соңғы жағдайда егер уақыт таңбалау органының қойылған қолы дұрыс болған болса істен шықпауды қамтамасыз ету саясаты куәліктің әрекет етуін анықтайды (Д қосымшасын қараңыз).

Тура осындай тәсілмен кілттің заңсыз пайдалануын қарастыруға болады. Егер істен шықпауды қамтамасыз ету саясаты куәлік субъектісінің кілттің заңсыз пайдаланылғаны мен оның әшкере болған уақыт арасында өз кілтінің қастандық жасалғанына жауап бермейтін болса, куәлік субъектісі кілтінің заңсыз пайдаланғанын дәлелдеп, болған оқиға мен әрекеттерден бас тартуы тиіс. Кілтті басқа біреудің пайдаланғаны туралы хабарлауына

дейінгі кешіктірілген уақытты мүмкіндігінше анықтау бұл қауіпке қарсы тұруға көмектеседі. Егер куәлік иесінің кілтті басқа біреудің заңсыз пайдаланылғаны туралы берілген уақыт ішінде хабарлай алмаған болса, онда куәлік иесі кілтпен қастандық жасалған барлық зардаптарға жауапты болады. Куәліктің верификаторы әрбір куәлікті қабылдау кезінде кілтпен қастандықтың жасалғаны туралы хабарлауды қаншалықты кешіктірілгені туралы көз жеткізіп отыруы тиіс.

8.7.1.2 Кілтті құруды басқа біреудің қолдануы

СБҮЖ арқылы кілттің зиян шегуі табылған жағдайда, бұл кілттің күші жойылуы тиіс. Егер кілт жабық кілт болатын болса, сәйкес ашық кілттің сертификатын шақыру керек. Бұл [2]-де анықталған шақырылған сертификаттар тізімі арқылы жүзеге асуы мүмкін. Бұрындары жасалған куәліктің рұқсатсыз пайдаланылған (мүмкін) кілтпен жұмыс істеуі кезінде өз кілтінің әрбір пайдаланылуын СБҮЖ тіркеу журналына тіркеп отыруы тиіс. Егер СБҮЖ-дің кілті рұқсатсыз пайдаланылған уақытта даулы жағдайды шешу үшін тіркеу журналын пайдалануға болады.

8.7.1.3 Мәнді тексеру кілтінің алмастырылуы

Куәлікті пайдаланушы мен верификаторды қолдарындағы жалған куәліктің дұрыстығына сендіру қаупі кездеседі. Бірақ та сот шешімін талап ететін даулы жағдай туған кезде куәліктің жалғандығы айқындалады. Яғни, мұндай жағдайда куәлікті пайдаланушы жауапкершіліктен босатылады, өйткені ол өзінің куәлігінің дұрыс екендігіне сенімді болғандықтан әрекеттер жасауы мүмкін, бірақ сот дауды оның пайдасына шешпейді. Бұл қауіпке қарсы тұра алатын тәсілдер мәннің дұрыстығын - тексеру кілтінің дұрыстығымен сәйкестігін анықтау үшін күшті іс-шараларды пайдаланады. Алмастыру болған жағдайда жалған тексеру кілті ауыстыру әшкере болған сәтте жойылуы тиіс.

8.7.1.4 СБҮЖ тексеру кілтінің алмастырылуы

Егер СБҮЖ-дің пайдалануындағы тікелей тексеру куәлігінің тексеру кілті ашық кілт болған жағдайда, төрешіге тексеру үшін берілетін кілттерді берудің бір тәсілінің көмегімен СБҮЖ-тдің жалған куәлікті алып алданып қалуы (мысалы, қағаз құжаттар, сертификаттар тізбегі). Бұған нақты мысал ретінде қастандық ойлаушының төрешіге тәуелді ашық кілттің көшірмесін алмастыруы дәлел бола алады.

Бұндай жағдайды анықтаған жағдайда алмастыру фактісі туралы барынша кең хабарлануы керек, бірақ алмастырылған кілт көмегімен тексеріле алатын куәгерлікті барлық пайдаланушыларға бұл ақпаратты жеткізу мүмкін болмайды. Жоғалған немесе рұқсатсыз пайдаланылған криптографиялық кілт орасан қастандықтың нәтижесінде мәліметтерді тіркеу үшін рұқсат етілген уақыт таңбалау сервисінің уақытша терезесіне

орналасады. Осы тәсілмен қай куәлік ескерткенге дейін бе, болмаса кейін тексерілгенін байқауға болады.

Егер тексеру кілті куәлікті пайдаланушылар сертификаттарды тікелей тексеру үшін пайдаланылатын ашық кілт болып табылатын болса, онда ол оның алмастырылуы белгілі болған сәттен бастап алмастырылуы керек,

8.7.2 Куәгерліктің беделінің түсуі

Бір кездегі қанағаттанарлық куәгерлік біраз уақыттан соң керексіз болуы мүмкін. Мұндай ақпарат беделі түскен ақпарат деп аталады.

8.7.2.1 Рұқсатсыз өзгеріс немесе куәгерліктің бұзылуы

Мұндай жағдайда іс-әрекет немесе оқиға болып өткен, бірақ оқиғаның болмағанын көздейтін тараптар сақтаулы куәгерлікті өзгертуге немесе бұзуға қол жеткізеді. Бұдан соң бұл тараптар шын мәнінде болып өткен оқиғаны жемісті түрде жоққа шығара алады. Мұндай қауіпке қарсы тұруға болады; ол үшін куәгерлікті өзгертуден немесе бұзудан сақтайтын қорғаныс тетіктерін қолдануға болады (мысалы, резервтегі көшірмелердің сақталуы). Сенім білдірілген үшінші жақты пайдалану бұл қауіптен сақтануды күшейте түседі, себебі сенім білдірілген үшінші жақпен қамтамасыз етілген сақтау құралдары куәгерлікті пайдаланудың сақтау құралдарына қарағанда жақсырақ қорғалған.

8.7.2.3 Куәгерліктің бұзылуы немесе жоққа шығарылуы

Бұл қауіп сенім білдірілген үшінші жақта сақталған куәгерліктің бұзылуынан тұрады. Куәгерліктің бұзылуы немесе жоққа шығарылуы сенім білдірілген үшінші жақ абай болмаған жағдайда және тиісті резерв схемасын қамтамасыз етпеген жағдайда туындауы мүмкін. Мұндай қауіптен істен шықпауды қамтамасыз етудің мынадай тетіктерін пайдалану жолымен ғана құтылуға болады: яғни, даулы жағдайларды шешу үшін қажетті барлық куәгерліктер куәгерлікті пайдаланушыда сақталған болса ғана қауіп сейіледі. Мұндай жағдайда куәгерлікті пайдаланушы сенім білдірілген үшінші жақтың арам пиғылы болған кезде де немесе абайламай қалған жағдайда да куәгерліктің бұзылмайтынына кепілдік бере алады.

8.7.3. Куәгерліктің жалғандығы

8.7.3.1 Куәгерліктің өз ішіндегі жалғандығы

Мұндай сәтте даулы оқиға орын алмауы мүмкін, бірақ қаскөйлер жүйеге өз ішінен кіреді де, оқиға болды деп жалған куәгерлік жасайды. Бұл нотариустың көмегімен жүзеге асуы мүмкін. Сақтаулы куәгерлікті жалғандықтан қорғау үшін немесе өз ішінен өзгертуден қорғау үшін криптографиялық тетіктер қолданылады.

8.7.3.2 Куәгерліктің жалған расталуы

Куәгерлікті тексеру үшін қолданылатын сенім білдірілген үшінші жақтың механизмінде мынадай қауіп бар: сенім білдірілген үшінші жақ

куәгерліктің дұрыстығын хабарлайды, бірақ шындығында олай емес. Даулы ситуация туындаған жағдайда куәгерлікті пайдаланушы сотты даулы жағдайдың болғанына сендіре алмайды. Мұндай қауіпке сенім білдірілген үшінші жақтың көмегінсіз-ақ, куәгерлікті куәгерлік верификаторына тікелей тексертіп, ұрынбауға болады.

8.7.3.3 Куәгерліктің жалғандығын сенім білдірілген үшінші жақтың жасауы

Сенім білдірілген үшінші жақ болмаған оқиға куәлігін болды деп жалған куәгерлік жасау қаупі бар. Егер сот сенім білдірілген үшінші жаққа сенетін болса, онда ол жалған куәгерлікті қабылдауы мүмкін, осының нәтижесінде ол алданып, қате шешім қабылдауға мәжбүр. Мұндай қауіптің алдын алу үшін сенім білдірілген үшінші жақ жалған куәгерлік жасай алмайтындай немесе кепілдік беретіндей, қолданыстағы сенім білдірілген үшінші жақ сенімділікке ие болатындай, әрі олардың сайланбалы болуын көздейтін істен шықпауды қамтамасыз етудің тетіктері қолданылады. Мұндай жағдайда мәннің сенімділігін бұлтартпас куәгерлікпен қамтамасыз ету қиын.

9 Басқа қызмет түрлерімен және қорғаныс тетіктерімен өзара әрекеті

Бұл жерде істен шықпауды қамтамасыз ету үшін қорғаныстың басқа да сервистері қолданылуы мүмкін екендігі айтылып отыр. Мұнда істен шықпаудың қорғаныстың басқа сервистері үшін қолданылуы қарастырылмаған.

9.1 Сәйкестендіру

Сенім білдірілген үшінші жақпен бірлесе отырып, мәнге өзінің түпнұсқалығын сәйкестендіру сервисі арқылы дәлелдеу қажет болуы мүмкін. Мәлімет қай наркөзінің сәйкестендіру сервисінің көмегімен кепілдікке ие болған алмасулар талап етілуі мүмкін. Мысалы, сенім білдірілген үшінші жақты қол қоюды ұйымдастыруда пайдаланған кезде куәгерлік субъектісінің қол қояр кездегі түпнұсқалығын тексеру талап етілетін шығар.

9.2 Қол жеткізуді басқару

Қол жеткізуді басқару сервисі сенім білдірілген үшінші жақтағы сақтаулы ақпарат немесе сервис, сенім білдірілген үшінші жақ беретін ақпарат тек қана авторлардың ризалығына ие мәндер үшін ғана ашық болуы мүмкін.

9.3. Құпиялылық

Құпиялылық сервисі мәліметтерді рұқсатсыз ашудан қорғау үшін (кейбір жағдайларда сенім білдірілген үшінші жақ орындаған мәліметтердің рұқсатсыз ашылуы мүмкін), сондай-ақ куәгерліктің рұқсатсыз ашылуын қорғау үшін қажет.

9.4 Бүтіндік

Бүтіндікті қамтамасыз ету сервисі куәгерліктің бүтіндігін қамтамасыз ету үшін қажет.

Мәліметтер бүтіндігі сондай-ақ түпнұсқадан істен шықпауды қамтамасыз еткенде немесе жеткізуден істен шықпауды қамтамасыз еткенде қажет; түпнұсқа мен алушының арасындағы мәліметтерді өзгертпей, сақтау үшін қажет.

9.5 Қауіпсіздік оқиғаларын есепке алу

Куәгерлікті пайдаланушы қауіпсіздік оқиғаларын тізімдеу қызметін келешекте туындауы мүмкін даулы жағдайлар кезінде қолданылатын куәгерлікті сақтау үшін пайдалана алады.

Нотариус немесе жапсырма сенім білдірілген үшінші жақ қауіпсіздік оқиғаларын тізімдеу қызметін түпнұсқаның, тағайындаулардың және хабарлардың мерзімін жазып алу үшін пайдалана алады.

9.6 Кілтті басқару

Кілтпен басқару сервисі куәгерлікті жасауда және куәгерлікті тексеруде қолданылатын кілттерді қамтамасыз ету үшін қолданылуы мүмкін. Кілтпен басқару сервисі куәгерлікті тексеру кілттерін, тіпті сәйкес кілттің өзі жарамсыз немесе ашылмай қалған кезде де кілтпен қамтамасыз ету үшін талап етілуі мүмкін.

А қосымшасы
(анықтамалық)

Істен шықпауды ашық жүйелер байланысының (АЖБ-тың) базалық эталон үлгісі шеңберінде қамтамасыз ету

А.1 Түпнұсқадан істен шықпауды қамтамасыз ету

Түпнұсқадан істен шықпауды қамтамасыз ету сервисі алушыға мәліметтер куәлігін ұсынады, бұлар жіберушінің мәліметтерді немесе олардағы ақпараттарды жібергендігінен бас тартуына жол беретін кез-келген теріс әрекетінен қорғайды. Бұған қол жеткізуге болады, егер куәгерлік жасаушы (әдетте мәлімет жіберуші, кейде сенім білдірілген үшін жақ болуы да мүмкін) куәгерлік верификаторына (көбінесе мәлімет алушы, алушының атынан әрекет етуші тарап болуы да мүмкін) мәліметтерді жіберушінің жібергенін куәландыра алса.

Қол қою тетіктерін қолданған кезде куәгерлік мәліметтердің сандық қолтаңбасы немесе мәліметтердің сандық таңбасы түрінде болады. Түпнұсқадан істен шықпауды қамтамасыз ету айғақталған куәгерліктің күні бұрын келісілген схемасына байланысты. Ол мынадай сатылардан тұрады:

1) Істен шықпауды қамтамасыз ету сервисін сұратқан тарап куәлік жасайды немесе оны сенім білдірілген үшінші жақтан алады, әрі бұл куәгерлікті мәліметтерге қосады.

2) Куәгерлікті пайдаланушы куәгерлікке еркін қол жеткізеді.

3) Даулы ситуация жағдайында куәгерлікті пайдаланушы мәліметтер мен куәгерлікті ұсынады; сот мәліметтерді куәгерлікпен салыстырады.

А.2 Жеткізуден істен шықпауды қамтамасыз ету

Жеткізуден істен шықпауды қамтамасыз ету сервисі куәгерліктің мәліметтерін жіберушіге қажет; бұл мәліметтер алушының мәліметтерді алмадым деп жалтаруынан қорғайды. Егер куәгерлік жасаушы (әдетте мәліметтер алушы, кейде сенім білдірілген үшінші жақ болуы да мүмкін) куәгерлік верификаторына (көбінесе мәліметтерді жіберушіге немесе сенім білдірілген үшінші жаққа) мәліметтердің жеткізілгеніне куәлік жасаса бұған қол жеткізуге болады.

Бұл сервис алушыдан куәландырылған түбіртек (квитанция) мәліметі қайтарылған кезде ғана мүмкін болады. Түбіртек (квитанция) алушының сандық қолтаңба түріндегі хабардың түпнұсқасын алғаны жөніндегі куәгерлігі болуы қажет (немесе хабар түпнұсқасының сандық таңбасы) және алған уақыты көрсетілуі керек.

Қол қою тетіктерін пайдаланған кезде куәгерлік ретінде қол қойылған түбіртектің (квитанцияның) болуы міндетті.

Жеткізу ұйымының қызметін атқаратын сенім білдірілген үшінші жақтың қатыстылығына қарай бұл сервистің екі нұсқасын қарастыруға болады.

Б қосымшасы
(анықтамалық)
Істен шықпаудың қамтамасыз ету тәсілдерінің құрылымы

<table>
<tr><td colspan="2" rowspan="3">Қауіпсіздік тәсілдерінің құрылымы</td><td>Элемент</td><td colspan="3">Мәні: куәлік субъектісі, куәлікті құрушы, куәлік верификаторы, СБҮЖ-дің істен шықпауды қамтамасыз етуі, төреші</td></tr>
<tr><td colspan="3">Ақпараттық объектісі: куәлік</td></tr>
<tr><td colspan="3">Мән қызметі: жинау, қолдау, қолайлы ету, айқын куәлікті растау</td></tr>
<tr><td rowspan="6">ӘРЕКЕТТЕР</td><td>Мәні</td><td colspan="4">СБҮЖ, қауіпсіздік органы</td></tr>
<tr><td>Қызметі</td><td colspan="4">(анықталмаған)</td></tr>
<tr><td>Басқарумен байланысты әрекеттер</td><td colspan="4">- орнатылу,
- өзгертілу,
- өшірілу,
- аударылу</td></tr>
<tr><td>Мәні</td><td>Куәлік құрушы</td><td>Куәлік верификаторы</td><td>СБҮЖ-дің істен шықпауды қамтамасыз етуі</td><td>Төреші</td></tr>
<tr><td>Қызметі</td><td>(анықталмаған)</td><td>(анықталмаған)</td><td>(анықталмаған)</td><td>(анықталмаған)</td></tr>
<tr><td>Басқарумен байланысты әрекеттер</td><td>- куәлік құру;
- нотариалды расталған куәлікті құру</td><td>- куәлік құру;
- нотариалды расталған куәлік құру.</td><td>- уақыт маркерін құру
- СБҮЖ-тің көмегімен жіберу</td><td>(анықталмаған)</td></tr>
<tr><td rowspan="3">АҚПАРАТТАР</td><td>SDA басқаруындағы деректердің енгізу және шығару элементтері</td><td colspan="4">- басқару ақпараты, мысалы, пароль немесе кілттер;
- ақпараттар түрі;
- істен шықпауды қамтамасыз ету саясаты.</td></tr>
<tr><td>Операциялар да қолданылатын ақпарат түрлері</td><td colspan="4">- куәлік;
- сандық қолтаңба;
- қауіпсіздік маркері;
- қауіпсіздік сертификаты;
- уақыт маркері.</td></tr>
<tr><td>Басқару ақпараты</td><td colspan="4">Тіркеу журналына сот оқиғалары мен шешімдерін тіркеу;
мән аралығындағы тіркеу</td></tr>
</table>

В қосымшасы
(анықтамалық)

Сақтау және қайта жөнелту жүйелерінде істен шықпауды қамтамасыз ету

Сақтау мен жіберу жүйесіндегі хат – жіберуші мен алушының арасындағы жіберу агенттері деп аталатын бір немесе бірнеше дәнекерші арқылы жіберіліп отырады. Хатты жіберудегі осы жүйелерге сәйкес.

Хатты жіберудегі осы жүйелер жіберуші мен алушының арасындағы байланысты ғана емес, жіберуші мен жіберу агентінің арасындағы байланысты, жіберу агенті мен алушының арасындағы байланысты, және де агенттер арасындағы байланысты да қамтиды. Істен шықпауды қамтамасыз ету сервисі хабарлама жіберудің әр деңгейінде пайдаланылады.

Түпнегіздің істен шықпауын қамтамасыз ету сервисі хабарламаның мазмұны мен хабарламаның жіберілуінің жалғандығынан сақталады. Бұл сервисті беріліп отырған куәлікті алушы немесе жіберу агенті пайдалана алады.

Жеткізудің істен шықпауын қамтамасыз ету сервисі хабарламаның мазмұны мен хабарламаның жіберілуінің жалғандығынан сақталады. Бұл сервисті беріліп отырған куәлікті жіберуші немесе жіберу агенті пайдалана алады.

Жіберудің істен шықпауын қамтамасыз ету сервисі хабарламаны алу мен жіберуде фактіні жіберу агентінің (жіберушіден немесе басқа жіберу агенттерінен). Бұл сервисті беріліп отырған куәлікті алушы немесе жіберу агенті пайдалана алады.

Тасымалдаудың істен шықпауын қамтамасыз ету сервисі хабарламаны алу мен жіберуде фактіні жіберу агентінің (жіберушіден немесе басқа жіберу агенттерінен). Бұл сервисті беріліп отырған куәлікті алушы немесе жіберу агенті пайдалана алады.

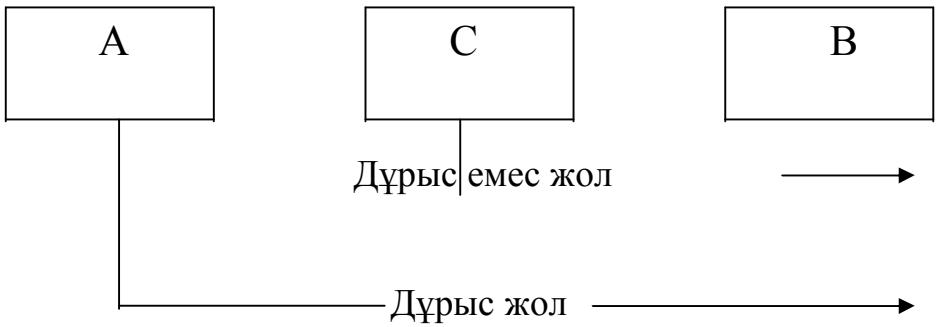
Табыстаудың істен шықпауын қамтамасыз ету сервисі хабарлама үшін алынған жауапкершілік жалған жоққа шығарудан қорғау үшін қолданылады. Егер хабарламаның жеткізілуінде бірнеше табыстау агенттері қатысса, бұл сервис қолданылады. Хабарламаны бірінші қабылдаған табыстау агенті екінші табыстау агентіне жібереді; екінші табыстау агенті біріншісіне осы хабарламаны қабылдағаны жауапкершілігіне куәлік береді. Егер табыстау агенттерінің саны екіден асса, аталмыш сервис екінші және үшінші агенттердің арасында қолданылуы мүмкін.

Сервис атауы	**Қорғайды**	**Қолданылады**
Істен шықпаудың түпнегізі	Түпнегізден	Түпнегізден, жіберу агентінен
Істен шықпаудың жіберілуі	Жіберу агентінен	Жіберушіден
Істен шықпаудың тасымалдануы	Жіберу агентінен	Жіберушіден
Істен шықпаудың берілуі	Жіберу агентінен	Жіберу агентінен
Істен шықпаудың жеткізілуі	Алушыдан	Жіберушіден, жіберу агентінен

Г Қосымшасы
(анықтамалық)
Істен шықпауды қамтамасыздандыру сервисінде қалпына келтіру

Қауіпсіздікті қалпына келтіру қалыпты жағдайларда болуға тиіс емес жағдайлармен байланысты. Алайда шынайы өмірде компьютерлік қауіпсіздікке қатерлі жағдай төнуі әбден мүмкін және бұндай жағдайға күні бұрын дайындалған абзал. Көбінесе істен шықпауды қамтамасыз етудің көптеген тетіктері криптографиялық кілттер мен құпиялылыққа тәуелді, ал бұлар олардың қорғанысы үшін қажет. Криптографиялық кілттердің жоғалуы мен олардың ашылуы қалпына келтіру жоспарында көрініс табуы керек, және бұл тиісті сәтте дереу орындалуы керек.

Істен шықпауды қамтамасыз ету сервисі үшін жабық криптографиялық кілттерді пайдаланған кезде төмендегідей ситуация туындауы мүмкін:



А тарапынан беделі түскен жабық кілтті қолданып, С тарапынан қол қойылған мәліметтер В адал қатысушыға берілуі мүмкін. Кей кезде В тарапынан әрекет (немесе әрекетсіздік) әсерінен А тарабын тауып алып, іс-әрекетін ақтау тәрізді қол қойылған хабар беруге себеп табылуы мүмкін. А тарабы жабық кілттің жоғалуы туралы хабарлауда ашық хабарламаға сүйенеді. Істі соттар қараған кезде А тарабына жауапты жағы ашық хабарлама мен жалған хабардың арасындағы уақыт айырмашылығы негізінде айқындалуы мүмкін. Егер хабар кілттің беделінің жоғалғаны туралы хабар кеш берілсе, онда А тарабы кінәлі деп танылуы мүмкін. С тарабы одан бұрынырақ хабар таратса, қауіптің алдын алу шаралары қолға алынбаса, онда А тарабы жауапты болады.

Мұндай жағдайдан шығу үшін хабарға қай уақытта қол қойылғаны аса маңызды. С тарабының хабарға қойған уақытына сенбестік білдірілсе, дереу сенім білдірілген үшінші жаққа хабарласып, хабардың заңды тіркелуін талап ету керек.

Істен шықпауды қамтамасыз ету сервистерінің жіктелген қосымша типтері (жеткізуден және көшіруден істен шықпау) модульдің әртүрлі деңгейдегі жүйесіне талдау жасау арқылы қамтамасыз етіледі, сондай-ақ бас тартпауды қамтамасыз ету сервисінің іргелі типтерінің тетіктерін пайдалану да тиімді. Мысалы, көшіріп жеткізуден істен шықпау хабарларды бөлшектеп жіберудің көмегі арқылы қамтамасыз етілсе, олардың бір бөлшегі жеткізілу туралы түбіртек (квитанция) болып табылады.

Д қосымшасы
(анықтамалық)
Каталогпен жұмыс жасау

Сандық қолтаңба ашық кілттің көмегі арқылы тексеріледі. Егер ашық кілт каталогта орналасқан пайдаланушы сертификатында болатын болса, КО-ның ашық кілті белгілі болған жағдайда кілттің дұрыстығын тексеруге болады.

Сертификатты шығарған куәландыратын орталық (КО) сертификатты дайындаудан кейін өзінің ашық кілтін өзгертуі мүмкін. "Ескі" ашық кілттің дұрыстығын тексеру үшін түрлі тәсілдер керек. Әдетте тек КО-ның ашық кілті ғана жалғыз белгілі кілт болғандықтан, осы ашық кілтпен ескі ашық кілтті байланыстыру қажеттігі туындайды. Алушыға КО кілтінің өзгерілгені беймәлім болғандықтан "ескі" сертификаттарды тексеру тәсілін қамтамасыз ету түрлі куәландыратын орталықтардың міндетіне жүктеледі. Бұл екі түрлі тәсілмен іске асады:

– сертификаттың көмегімен әрбір ескі КО ашық кілтін жаңа ашық КО кілтімен;

– сертификаттың көмегімен әрбір ескі КО ашық кілтін келесі ашық КО кілтімен;

Бірінші жағдайда ескі КО ашық кілтінің әрекеті тікелей тексеруге болатын бірегей сертификат шығаруда куәландыратын орталықтар қолданған жабық кілтке сәйкес келуі тиіс.

Соңғы жағдайда сертификаттар тізбегін КО ескі ашық кілтінің әрекетінің әр қадамын тексеру үшін жинақтау қажет. Бұл мынадай тәсіл арқылы орындалады: алдымен хабарламаның уақыты мен мерзіміне сәйкес келетін әрекет уақытын көрсететін сертификат тұрады, содан кейін бұрынғы КО ашық кілтінің мазмұнын табуға көмектесетін уақыт әрекеті тұрады.

Ескертпе - КО ескі ашық кілтін рұқсатсыз пайдалану мүмкін болған жағдайда бірінші тәсіл қолайлы болып табылады. Өйткені, екінші тәсілде ескі КО ашық кілтіне дейін созылған сертификаттар тізбегі үзіледі, соның салдарынан ескі КО ашық кілті жарамсыз болып қалады.

Жұмыс істеуге тиіс сертификаттар үшін басқа КО-дан немесе олардың қолданушыларынан кері шақырылған сертификаттарды КО сертификаттар тізімі каталогында қарамайды. Сол себепті, көпшілік кілттің уақытша жарамды екенін дәлелдеу үшін куәлік пайдаланушысы мен СБҮЖ-тің барлық керекті мәліметтерді мүмкіндік болып тұрған уақытта жинауы қажет (кері шақырылған сертификаттар тізімін қосқан кезде, бос болса да).

Кері шақырылған сертификаттар тізімі КО-дан шыққан уақытын көрсетеді. Және де даулы жағдайларды шешуге көмектесетін басқа мерзімді – пайдаланушы өзінің кілтін рұқсатсыз пайдаланылғандығы туралы бейхабар болған уақытты көрсетеді. Пайдаланушының бұл уақытқа дейінгі барлық қолтаңбалары жарамды деп саналады. Бұл уақыттың көрсетілмеуі себепті ең жаманы қауіпсіздік сертификатының әрекет ету уақыты кезінде жасалған әрекеттер жарамсыз деп саналады. Коммерциялық ортада пайдаланушы үшін хабарлама жазу үшін пайдаланылған кілт жоғалған жағдайда да бұл қолтаңбалардың жарамды деп есептелуі маңызды болуы мүмкін. Кері шақырылған сертификаттар тізімінде уақыттың болуы міндетті емес, егер бұл сертификаттың кілті істен шықпауды қамтамасыз ету сервисінде қолданылуы үшін қажет болуы мүмкін.

Сенімді қарым-қатынас уақыт өткен сайын өзгеріп отырады. Мысалы, төреші бүгін КО-ға сенім артса, ертең де оған сенім артуы міндетті емес. Даулы жағдайлардың өз пайдасына шешілу шешілмеуін білу мақсатында Бұл сенім түрі пайдаланушыға

ыңғайлы әрі оңтайлы болуы қажет. Әкімшілік мойындаған сенім қарым-қатынасының типтері көрсетілуі тиіс. Бұл сенім тапсырмалары келесі сенім тәсілдерінің көмегімен модельденеді:

– куәландырылған орталықтар толықтай сенімді және олардың әрбіреуіне ашық кілттің мағынасы айқын;

– куәландырылған орталықтарға КО сертификаты мен пайдаланушылық сертификаттарын шығару сеніп тапсырылған;

– куәландырылған орталықтарға тек пайдаланушылық сертификаттарын шығару сеніп тапсырылған (КО сертификатына басқа).

Бұл ақпаратты барлық куәлік тұтынушыларына жеңіл түсінікті ету. Ол әрекет ету уақытын қамтитын қауіпсіздік сертификатының үлгісімен жасалуы мүмкін. Қауіпсіздік саясатының екі түрлі формасы анықталды: төреші қадағалайтын қауіпсіздік саясатының сертификаты және тұтынушы жауап беретін қауіпсіздік саясатының сертификаттары.

Қосымша
(анықтамалық)

Библиография

[1] ИСО/МЭК 7498-1-1994 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Базалық эталондық үлгі. 1-бөлім. Базалық үлгі.

[2] ИСО/МЭК 9594-8: 1995 Ақпараттық технологиялар. Ашық жүйелердің бір-бірімен әрекеті. Анықтамалық. 8 бөлім. Сәйкестендіру негіздері

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: мәліметтерді өңдеу, ақпараттық алмасу, жүйелер байланысы, ашық жүйенің өзара әрекеттесуі, коммуникациялық іс-шаралар, хабарлар қорғанысы, қауіпсіздік әдістері

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ

Основы безопасности для открытых систем
Часть 4
Основы неотказуемости

СТ РК ИСО/МЭК 10181-4-2008

(ИСО/МЭК 10181-4:1997 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы неоказуемости», 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 10181-4:1997 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы неоказуемости» («Information technology. Open Systems Interconnection. Security frameworks for open systems. Non-repudiation 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

СТ РК ИСО/МЭК 10181-2008 под общим наименованием «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.

Приложения настоящего стандарта являются справочными.

Назначение сервисов обеспечения неотказуемости состоит в том, чтобы собирать, обеспечивать, делать доступными и подтверждать неопровержимые свидетельства, касающиеся объявленного события или действия, для решения спорных ситуаций о возникновении или отсутствии события или действия. Сервисы обеспечения неотказуемости могут использоваться в различных контекстах и ситуациях. Они могут использоваться при создании данных, хранении данных или передачи данных. Процессы обеспечения неотказуемости предполагают формирование свидетельства, которое может быть использовано для доказательства факта того, что некоторое событие или действие имело место, и поэтому впоследствии отречься от того, что действие или событие имело место будет невозможно.

В среде базовой эталонной модели ВОС (см. ГОСТ ИСО 7498-2-2002) существуют следующие два основных типа сервисов обеспечения неотказуемости:

– обеспечение неотказуемости источника, которое используется для опровержения ложного отрицания отправителем факта отправки данных или их содержимого;

– обеспечение неотказуемости доставки, которое используется для опровержения ложного отрицания получателем факта получения данных или их содержимого (т.е. информации, представляемой данными).

Приложениям, использующим протоколы базовой эталонной модели ВОС, могут потребоваться другие типы сервисов обеспечения неотказуемости, специфические для конкретных классов приложений.

Например, MHS – система управления сообщениями (ИСО/МЭК 10021-2:2003) определяет неотказуемость для сервиса подачи на рассмотрение, а

ЭОД – электронный обмен данными (EDI, см. Рек. МСЭ-Т Х.435) определяет неотказуемость для сервисов возвращения и передачи.

Концепции рассматриваемых в настоящем документе основ не ограничиваются коммуникациями базовой эталонной модели ВОС, но могут интерпретироваться шире, включая такое применение как создание и хранение данных для последующего использования.

Настоящий стандарт определяет общие основы для предоставления сервисов обеспечения неотказуемости, которые:

– расширяют понятия сервисов обеспечения неотказуемости, описанные в Рек. МККТТ Х.800 и ГОСТ ИСО 7498-2-2002, и описывают, как они могут быть использованы в Открытых системах;

– описывают варианты предоставления подобных сервисов;

– объясняют связи данных сервисов с другими сервисами защиты.

Для сервисов обеспечения неотказуемости могут потребоваться:

– судья, в задачи которого входит решение спорных ситуаций, возникающих в результате отрицания событий или действий;

– доверенные третьи стороны, гарантирующие подлинность и целостность данных, используемых для подтверждения свидетельства.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ ОСНОВЫ БЕЗОПАСНОСТИ ДЛЯ ОТКРЫТЫХ СИСТЕМ Часть 4 Основы неотказуемости

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт устанавливает основы безопасности, предназначенные для решения задачи применения сервисов безопасности в среде открытых систем. Под термином "Открытые системы" понимаются такие области, как базы данных, распределенные приложения, открытая распределенная обработка 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 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:

– основные понятия неотказуемости;

– общие сервисы обеспечения неотказуемости;

– возможные механизмы обеспечения сервисов неотказуемости;

– общие требования управления для сервисов и механизмов обеспечения неотказуемости.

Как и для любого другого сервиса защиты, неотказуемость может быть обеспечена только в контексте заданной политики безопасности для конкретного приложения. Определение политики безопасности выходит за рамки настоящего стандарта.

Настоящий стандарт не включает спецификации деталей обменов, входящих в состав протоколов, выполнение которых необходимо для обеспечения неотказуемости. Также стандарт не описывает подробно конкретные механизмы, которые могут быть использованы для реализации сервисов обеспечения неотказуемости, и не содержит подробностей обеспечения сервисов и протоколов управления безопасностью.

Некоторые из процедур, описанных в данном документе, реализуют защиту с помощью криптографических методов. Данные основы не зависят от

использования конкретного криптографического или иного алгоритма либо от конкретных криптографических методов (т.е. симметричных или асимметричных), хотя некоторые классы механизмов обеспечения неотказуемости могут зависеть от свойств конкретного алгоритма. *Выбор и применение конкретных средств криптографической защиты информации регламентируется законодательством Республики Казахстан*. На практике будет использоваться множество различных алгоритмов. Две сущности, желающие воспользоваться криптографически защищенными данными, должны поддерживать один и тот же криптографический алгоритм.

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

1) Стандарты, в которые входит понятие неотказуемости.

2) Стандарты, которые определяют абстрактные сервисы, включающие обеспечение неотказуемости.

3) Стандарты, которые определяют использование сервисов обеспечения неотказуемости.

4) Стандарты, которые определяют средства обеспечения неотказуемости в архитектуре открытых систем.

5) Стандарты, которые определяют механизмы обеспечения неотказуемости.

Перечисленные варианты стандартов могут использовать настоящий стандарт следующим образом:

– стандарты типа 1), 2), 3), 4) или 5) могут использовать терминологию данного стандарта;

– стандарты типа 2), 3), 4) или 5) могут использовать средства, определенные в разделе 7;

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

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

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

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 применены термины по *СТ РК ИСО/МЭК 10181-1-2008*, ГОСТ ИСО 7498-2, [1], а также следующие термины с соответствующими определениями:

3.1 Скомпрометированное свидетельство (compromised evidence) - свидетельство, которое когда-то было удовлетворительно, но больше не пользуется доверием доверенной третьей стороны или судьи.

3.2 Встречная подпись (counter-signature) - цифровая подпись, прилагаемая к блоку данных, который уже был подписан другой сущностью (например, ДТС).

3.3 Свидетельство (evidence) - информация, которая либо сама, либо при использовании вместе с другой информацией может быть использована для разрешения спорных ситуаций.

3.4 Создатель свидетельства (evidence generator) - сущность, создающая свидетельство неотказуемости.

Примечание. Данная сущность может быть стороной, запрашивающей свидетельство, источником, получателем или несколькими сторонами, действующими совместно (например, подписавшая сторона и сторона, подписавшая вместе с ней).

3.5 Субъект свидетельства (evidence subject) - сущность, участие которой в действии или событии устанавливается свидетельством.

3.6 Пользователь свидетельства (evidence user) - сущность, использующая свидетельство.

3.7 Верификатор свидетельства (evidence verifier) - сущность, проверяющая свидетельство.

3.8 Код аутентификации сообщения (message authentication code) - криптографическое контрольное значение, используемое для обеспечения аутентификации источника данных и целостности данных.

3.9 Сторона, запрашивающая сервис обеспечения неотказуемости (non-repudiation service requester) - сущность, требующая создания свидетельства для конкретного действия или события.

3.10 Нотариус (notary) - доверенная третья сторона, регистрирующая данные, чтобы впоследствии можно было гарантировать предоставление точности характеристик данных.

3.11 Источник (originator) – в контексте передачи данных сущность, которая создает данные в действии, являющаяся объектом сервиса обеспечения неотказуемости.

3.12 Получатель (recipient) - в контексте передачи данных сущность, которая получает данные в действии, являющаяся объектом сервиса обеспечения неотказуемости.

Примечание. В логической модели неотказуемости могут быть рассмотрены и другие сущности. Например, владелец представляет собой сущность, которая создает первоначальное сообщение, а агент передачи - сущность, которая передает сообщение; в данном контексте сущности представляются как источники и получатели.

4 Сокращения

В настоящем стандарте используются следующие сокращения:

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

4.2 УЦ (Certificate Authority; CA) - удостоверяющий центр;

4.3 ДТС (Trusted Third Party; TTP) - доверенная третья сторона;

4.4 СУС (Message Handling System; MHS) - система управления сообщениями;

4.5 ЭОД (Electronic Data Interchange; EDI) - электронный обмен данными;

4.6 СОС (Certificate Revocation List; CRL) - список отозванных сертификатов.

5 Общие сведения о неотказуемости

5.1 Основные понятия неотказуемости

Сервис обеспечения неотказуемости включает создание, подтверждение и регистрацию свидетельства, а также последующий поиск и повторное подтверждение данного свидетельства для разрешения спорных ситуаций. Разрешение спорных ситуаций не представляется возможным при отсутствии предварительной регистрации свидетельства.

Назначением сервиса обеспечения неотказуемости, описанного в данных основах, является обеспечение свидетельства для конкретного события или действия. Сервисы обеспечения неотказуемости могут быть затребованы сущностями, отличными от участвующих в событии или действии. Примерами действий, которые могут быть защищены сервисом обеспечения неотказуемости, являются:

– отправка сообщения по протоколу X.400;

– добавление записи в базу данных;

– запрос на дистанционное выполнение.

Для обеспечения неотказуемости источника необходимо подтвердить идентичность источника и целостность данных. Для обеспечения неотказуемости доставки должны быть подтверждены идентичность получателя и целостность данных. В некоторых случаях может также потребоваться свидетельство неотказуемости, связанное с контекстом (например, для даты, времени, местонахождения источника/получателя).

Сервис предоставляет следующие средства, которые могут использоваться в случае попыток отказа от действий, имевших место:

– создание свидетельства;

– регистрация свидетельства;

– подтверждение созданного свидетельства;

– поиск и повторное подтверждение свидетельства.

Спорные ситуации между сторонами могут разрешаться непосредственно путем предъявления свидетельства. Однако, может потребоваться, чтобы спорная ситуация была разрешена судьей, который оценивает свидетельство и определяет, произошло ли спорное событие или действие. Судебное решение может быть эффективным только в том случае, когда спорящие стороны признают власть судьи. Чтобы представленное свидетельство было признано судьей, обычно оно должно быть заверено одной или несколькими доверенными третьими сторонами. Судья и сам может быть доверенной третьей стороной, заверившей свидетельство. Механизмы обеспечения неотказуемости используют множество типов доверенных третьих сторон и форм свидетельства.

5.2 Роли доверенной третьей стороны

Сервис обеспечения неотказуемости может задействовать одну или несколько доверенных третьих сторон.

Доверенные третьи стороны, которые поддерживают обеспечение неотказуемости без активного участия в каждом обращении к сервису, называются независимыми доверенными третьими сторонами. Доверенная третья сторона, активно участвующая в создании или подтверждении свидетельства, называется оперативной ДТС. Оперативная ДТС, выступающая в качестве посредника во всех взаимодействиях, называется встроенной ДТС.

Доверенная третья сторона может потребоваться для регистрации и/или сбора свидетельств, а также для подтверждения адекватности свидетельств. Может быть несколько доверенных третьих сторон, выступающих в различных ролях (например, выполняющих функции нотариуса, маркирования времени, мониторинга, сертификации ключей, создания подписи, подтверждения подписи и органа доставки). Одна доверенная третья сторона может выступать в одной или нескольких из этих ролей.

При создании свидетельства ДТС сотрудничает со стороной, запрашивающей создание свидетельства у сервиса обеспечения неотказуемости.

При регистрации свидетельства ДТС записывает свидетельство, которое может быть впоследствии извлечено пользователем свидетельства или судьей.

При маркировании времени ДТС доверяется сформировать свидетельство, содержащее время получения запроса маркирования времени.

При мониторинге ДТС отслеживает действие или событие, и ей доверяется обеспечивать свидетельство того, что было обнаружено.

При сертификации ключей ДТС предоставляет сертификаты неотказуемости, связанные с создателем свидетельства для подтверждения действительности открытого ключа, используемого в целях обеспечения неотказуемости.

При распределении ключей ДТС предоставляет ключи создателям свидетельств и/или верификаторам свидетельств. Она также может ограничить использование ключей, в частности, при использовании симметричных методов.

При создании подписи ДТС доверяется предоставить свидетельство в форме цифровой подписи от имени субъекта свидетельства.

При подтверждении свидетельства ДТС по запросу сущности проверяет свидетельство.

При подтверждении подписи пользователь свидетельства доверяет ДТС проверить свидетельство в форме цифровой подписи.

Примечание. Создание подписи является частным случаем создания свидетельства. Подтверждение подписи является частным случаем подтверждения свидетельства.

В роли нотариуса ДТС гарантирует свойства данных (например, их целостность, источник, время или назначение), передаваемых между двумя или более сущностями и ранее зарегистрированных ДТС.

В роли органа доставки ДТС взаимодействует с намеченным получателем данных и пытается доставить данные получателю. Затем она предоставляет свидетельство того, что данные были доставлены, что данные не были доставлены, или что попытка доставки была предпринята, но подтверждение получения не было. В последнем случае пользователь свидетельства не может определить, были ли данные получены намеченным получателем.

5.3 Стадии обеспечения неотказуемости

Обеспечение неотказуемости производится в четыре стадии:

– создание свидетельства;

– передача, хранение и извлечение свидетельства;

– подтверждение свидетельства;

– разрешение спорной ситуации.

На рисунке 1 показаны первые три стадии; на рисунке 2 показана четвертая стадия.

Рисунок 1. Сущности, участвующие в стадиях создания, передачи, хранения/извлечения и подтверждения свидетельства

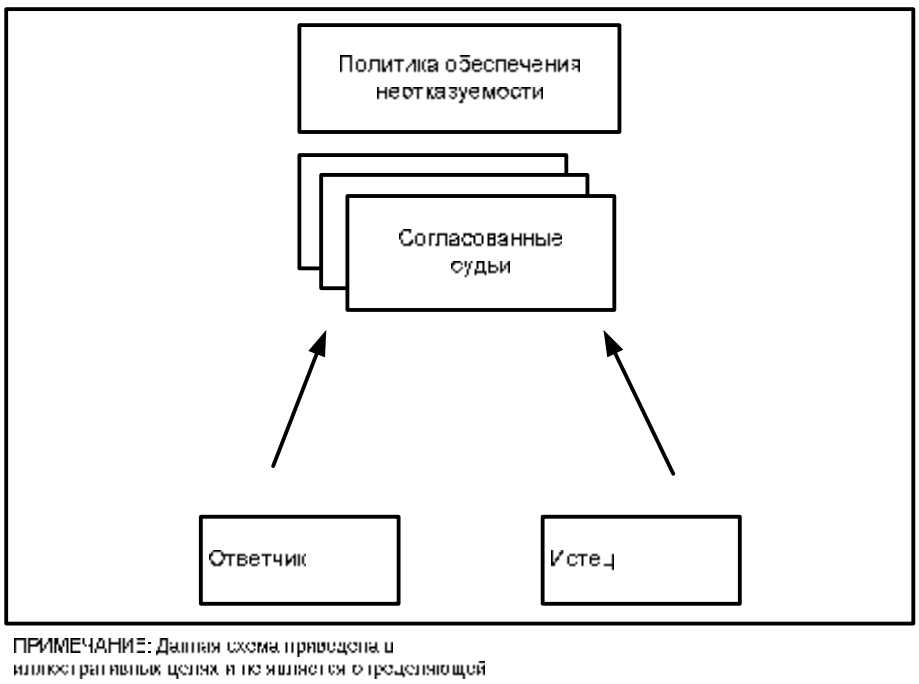


Рисунок 2. Стадия разрешения спорной ситуации в процессе обеспечения неотказуемости

5.3.1 Создание свидетельства

На стадии создания свидетельства сторона, запросившая это, требует, чтобы создатель свидетельств создал свидетельство осуществления события или действия. Сущность, чье участие в действии или событии устанавливается свидетельством, называется субъектом свидетельства. Возможно различное группирование этих сущностей: одной сущностью могут быть субъект свидетельства и создатель свидетельства, а также субъект свидетельства, сторона, запросившая создание свидетельства, и создатель свидетельства; или сторона, требующая создания свидетельства, и доверенная третья сторона; или создатель свидетельства и доверенная третья сторона; сторона, требующая создания свидетельства, создатель свидетельства и доверенная третья сторона. В зависимости от типа сервиса обеспечения неотказуемости свидетельство может создаваться субъектом свидетельства, возможно совместно с сервисами доверенной третьей стороны, или одной доверенной третьей стороной.

Примечание. В зависимости от контекста сервиса обеспечения неотказуемости соответствующее типовое свидетельство будет включать идентификаторы участвующих сущностей, данные, а также время и дату. Возможно также добавление в него дополнительной информации, такой, как режим передачи (например, коммуникации базовой эталонной модели ВОС, сохранение в базе данных и извлечение из нее), местонахождение участвующих сущностей, отличительный идентификатор и "владелец"/ создатель данных.

5.3.2 Передача, хранение и извлечение свидетельства

На данной стадии свидетельство передается между сущностями, или из места хранения, или в место хранения.

5.3.3 Подтверждение свидетельства

На этой стадии свидетельство проверяется верификатором свидетельства по запросу пользователя свидетельства. Данная стадия предназначена для того, чтобы пользователь свидетельства убедился, что представленное свидетельство действительно будет достаточным в случае возникновения спорной ситуации. В предоставлении информации для подтверждения свидетельства могут дополнительно участвовать сервисы доверенной третьей стороны. Пользователь свидетельства и верификатор свидетельства могут быть одной и той же сущностью.

5.3.4 Разрешение спорной ситуации

На стадии разрешении спорной ситуации за разрешение споров между сторонами несет ответственность судья. Спорящие стороны иногда называются истцом и ответчиком. Стадия разрешения спорной ситуации показана на рис. 2.

Когда судья разрешает спорную ситуацию, он собирает свидетельства от спорящих сторон и/или доверенных третьих сторон. Процесс, используе-

мый судьей для разрешения спорных ситуаций, находится вне области распространения настоящего стандарта.

Эта стадия не всегда является обязательной. Если все заинтересованные стороны соглашаются в том, что событие или действие произошло (либо соглашаются, что оно не произошло), то никаких спорных ситуаций не возникает. Далее, даже возникшая спорная ситуация может быть разрешена сторонами непосредственно без привлечения судьи. Например, если одна из сторон, участвующих в споре, является честной, но ошибается, то эта сторона может понять, что она ошибается после того, как ей будет предъявлено свидетельство другой стороны.

Хотя эта стадия не всегда обязательна для каждого обращения к сервису обеспечения неотказуемости, все механизмы обеспечения неотказуемости должны поддерживать стадию разрешения спорных ситуаций. То есть, они должны обеспечивать разрешение спорных ситуаций при их возникновении.

5.4 Некоторые типы сервисов обеспечения неотказуемости

Существует множество типов сервисов обеспечения неотказуемости. Наиболее часто используются сервисы обеспечения неотказуемости, связанные с передачей данных.

В передаче сообщения участвуют, по крайней мере, две сущности, а именно отправитель и получатель. Потенциальные спорные ситуации, касающиеся данного события, включают:

– спорные ситуации, в которых оспаривается участие отправителя в событии, например, подозреваемый отправитель заявляет, что сообщение было похищено либо получателем, либо замаскированным взломщиком;

– спорные ситуации, в которых оспаривается участие получателя в событии, например, подозреваемый получатель заявляет, что сообщение либо не отправлялось, либо было потеряно при передаче, либо было получено замаскированным взломщиком.

Для передачи сообщений сервисы обеспечения неотказуемости можно классифицировать по видам спорных ситуаций, которые данные сервисы помогают разрешать.

Передача сообщений от отправителя получателю может рассматриваться как последовательность следующих отдельных событий:

– передача сообщения от отправителя агенту передачи;

– передача сообщения между агентами передачи (если участвует несколько агентов передачи);

– передача сообщения от агента передачи получателю.

Для каждого из этих событий существуют типы сервисов обеспечения неотказуемости, представляющие свидетельство по рассматриваемому собы-

тию. Соответственно, определяются следующие дополнительные типы сервисов обеспечения неотказуемости:

– обеспечение неотказуемости отправки производится для защиты от ложного отрицания агентом передачи факта получения сообщения (либо от отправителя, либо от другого агента передачи) для передачи;

– обеспечение неотказуемости транспортировки производится для защиты от ложного отрицания агентом передачи факта передачи сообщения (либо получателю, либо другому агенту передачи).

Примечание. Обеспечение неотказуемости отправки и транспортировки сообщения не гарантируют того, что сущность несет ответственность за сообщение или, что она поняла информацию, содержащуюся в сообщении.

5.5 Примеры свидетельств неотказуемости по модели ВОС

В зависимости от используемых сервисов обеспечения неотказуемости требуются конкретные типы свидетельств для каждого из перечисленных ниже событий и действий.

5.5.1 Обеспечение неотказуемости источника

Свидетельство должно включать следующие компоненты (которые могут быть подписаны или нотариально заверены):

– отличительный идентификатор отправителя;

– отправленные данные или их цифровой отпечаток.

Свидетельство может также включать следующие компоненты:

– отличительный идентификатор получателя;

– дата и время отправки данных.

5.5.2 Обеспечение неотказуемости доставки

Свидетельство должно включать следующие компоненты (которые могут быть подписаны или нотариально заверены):

– отличительный идентификатор получателя;

– полученные данные или их цифровой отпечаток.

Свидетельство может также включать следующие компоненты:

– отличительный идентификатор отправителя;

– дата и время получения данных.

При использовании органа доставки свидетельство может также включать следующие компоненты (которые могут быть подписаны или нотариально заверены):

– отличительный идентификатор органа доставки;

– дата и время первой попытки доставки, предпринятой органом доставки;

– дата и время приема от получателя сигнала готовности к получению;

– дата и время выполнения доставки органом доставки;

– дата и время, когда орган доставки не смог выполнить доставку;

– возможная причина невозможности доставки (например, разрыв канала связи);

– указание требований обработки, удовлетворенных в процессе доставки сообщения.

6 Политики обеспечения неотказуемости

Политики обеспечения неотказуемости могут включать:

– Правила создания свидетельства, например, спецификации классов действий, для которых должно быть создано свидетельство неотказуемости; спецификации ДТС, задействованных при создании свидетельства; роли, выполняемые этими ДТС; процедуры, которым должны следовать сущности при создании свидетельства.

– Правила подтверждения свидетельства, например, спецификации ДТС, чьи свидетельства являются удовлетворительными, и формы свидетельств для каждой ДТС, которые будут признаваться.

– Правила хранения свидетельства, например, средства, используемые для обеспечения целостности хранящегося свидетельства.

– Правила использования свидетельства, например, спецификация задач, для которых может быть использовано свидетельство.

Примечание. В некоторых механизмах обеспечения неотказуемости может быть затруднительно предотвратить неразрешенное использование свидетельства.

– Правила принятия судебных решений, например, спецификация согласованного судьи (судей), который может разрешать спорные ситуации.

Каждый из этих наборов правил может определяться отдельным органом. Например, правила создания свидетельства могут определяться владельцем системы, а правила принятия судебных решений могут определяться законами страны, в которой система используется.

Если различные части политики несовместимы, то сервис обеспечения неотказуемости, возможно, не будет работать правильно, например, позволяя на стадии разрешения спорной ситуации успешно отрицать событие, которое в действительности произошло.

Политика обеспечения неотказуемости сама может быть использована судьей при разрешении спорной ситуации. Например, судья может обратиться к политике обеспечения неотказуемости, определяя, выполнялось ли создание свидетельства в соответствии с данной политикой.

Политики безопасности могут быть сформулированы явным образом или могут неявно определяться реализациями. Явное задание политики обеспечения неотказуемости (например, в документах на естественном языке) может помочь обнаружить конфликты между различными частями политики, а также может помочь судье.

Политики обеспечения неотказуемости также связаны со случаями компрометации свидетельства, либо со случаями компрометации или аннулирования ключей, использованных для создания свидетельства.

Политики обеспечения неотказуемости для взаимодействия между доменами безопасности могут быть результатом соглашений между независимыми доменами безопасности или могут быть установлены вышестоящим доменом безопасности.

7 Информация и средства обеспечения неотказуемости

7.1 Информация

Информация, которая может быть использована для разрешения спорной ситуации, именуется в настоящем документе свидетельством. Свидетельство может храниться либо пользователем свидетельства локально, либо доверенной третьей стороной. Конкретными формами свидетельства являются цифровые подписи, защищенные конверты и маркеры безопасности. Цифровые подписи используются вместе с технологией открытых ключей, а защищенные конверты и маркеры безопасности используются с технологией секретных ключей. Примерами информации, которая может быть отнесена к свидетельству, являются:

– идентификатор политики обеспечения неотказуемости;

– отличительный идентификатор отправителя;

– отличительный идентификатор получателя;

– цифровая подпись защищенного конверта;

– отличительный идентификатор создателя свидетельства;

– отличительный идентификатор стороны, запрашивающей создание свидетельства;

– сообщение или цифровой отпечаток сообщения;

Примечание. Если вместо сообщения используется его цифровой отпечаток, необходим признак, определяющий метод, используемый для получения отпечатка.

– идентификатор сообщения;

– признак секретного ключа, необходимого для подтверждения маркера безопасности;

– обозначение конкретного открытого ключа, необходимого для подтверждения цифровой подписи (например, отличительный идентификатор УЦ и порядковый номер сертификата);

– отличительный идентификатор нотариуса, ДТС, маркирующей время, встроенной ДТС и т. п.;

– уникальный идентификатор свидетельства;

– дата и время размещения или регистрации свидетельства;

– дата и время создания цифровой подписи или маркера безопасности.

7.2 Средства обеспечения неотказуемости

Настоящий раздел определяет ряд средств обеспечения неотказуемости, которые могут быть использованы для создания, отправки и подтверждения свидетельства или для размещения свидетельства у ДТС.

7.2.1 Средства, связанные с управлением

Средства управления обеспечением неотказуемости включают средства распределения информации, паролей или ключей (включая управление ключами) среди сущностей, необходимых для обеспечения неотказуемости. Перечисленные варианты средств могут ориентироваться на использование некоторого протокола между связывающимися сущностями и другими сущностями, обеспечивающими сервисы обеспечения неотказуемости. Управление процессами обеспечения неотказуемости может также включать аннулирование ключей, используемых для получения свидетельства.

Средства управления обеспечением неотказуемости позволяют пользователю получать, изменять и удалять информацию, необходимую для обеспечения неотказуемости. В общих чертах данными средствами являются:

– средства установки информации управления;

– средства изменения информации управления;

– средства удаления информации управления;

– средства перечисления информации управления.

Для поддержки сервисов обеспечения неотказуемости могут потребоваться следующие действия, связанные с управлением:

– регистрация события в журнале учета событий;

– регистрация результатов разрешения спорной ситуации;

– локальное уведомление о событии;

– удаленное уведомление о событии.

Конкретное действие, предпринимаемое для каждого события, зависит от действующей политики безопасности.

7.2.2 Средства, связанные с работой

7.2.2.1 Средство создания свидетельства.

Данное средство предназначено для создания свидетельства. Свидетельство может создаваться непосредственно субъектом свидетельства (без привлечения ДТС), одной или несколькими ДТС, выступающими от имени субъекта свидетельства, или совместно субъектом свидетельства и одной или несколькими ДТС.

Возможными входными данными для средства создания свидетельства могут являться:

– политика обеспечения неотказуемости;

– отличительный идентификатор субъекта свидетельства;

– отличительный идентификатор сущности, обращающейся к сервису обеспечения неотказуемости;

– данные или их цифровой отпечаток;

– отличительный идентификатор ДТС, которая будет использована для создания цифровой подписи, маркера безопасности или другого свидетельства.

Возможными выходными данными средства создания свидетельства могут являться:

– свидетельство (например, цифровая подпись или маркер безопасности);

– отличительный идентификатор ДТС, создавшей цифровую подпись, маркер безопасности или другое свидетельство.

7.2.2.2 Средство создания метки времени.

Данное средство предназначено для создания меток времени.

Возможными входными данными средства создания метки времени могут являться:

– отличительный идентификатор сущности, запрашивающей метку времени;

– отличительный идентификатор ДТС, осуществляющей маркировку времени;

– данные (например, подписанное сообщение, квитанция), или цифровая подпись, или цифровой отпечаток данных.

Возможными выходными данными средства создания метки времени являются:

– встречная подпись, созданная доверенной третьей стороной;

– обозначение метода и/или криптографического алгоритма, используемого для создания встречной подписи (которое, к тому же, показывает, использовались ли данные или их цифровой отпечаток);

– отличительный идентификатор сервиса маркирования времени;

– дату и время получения запроса на создание метки времени;

– дату и время создания встречной подписи;

– подписанное сообщение, включающее метку времени и цифровой отпечаток входных данных.

7.2.2.3 Средство создания нотариально заверенного свидетельства.

Данное средство используется для размещения свидетельства у ДТС.

Возможными входными данными средства являются:

– отличительный идентификатор стороны, запрашивающей создание свидетельства;

– свидетельство (например, цифровую подпись или маркер безопасности);

– отличительный идентификатор создателя свидетельства;

– отличительный идентификатор политики обеспечения неотказуемости.

Возможные выходные данные включают:

– регистрационный номер свидетельства;

– дату и время регистрации свидетельства.

7.2.2.4 Средство подтверждения свидетельства.

Данное средство используется для подтверждения свидетельства.

Возможными входными данными средства являются:

– свидетельство;

– отличительный идентификатор субъекта свидетельства;

– отличительный идентификатор пользователя свидетельства;

– идентификатор ключа, используемого для проверки свидетельства;

– признак назначения свидетельства (позволяющий оценить, соответствует ли свидетельство данному использованию для данной политики обеспечения неотказуемости).

Возможными выходными данными являются:

– результат проверки (т.е. правильно или неправильно);

– отличительный идентификатор субъекта свидетельства;

– отличительный идентификатор создателя свидетельства;

– отличительный идентификатор сущности, требующей проверки свидетельства;

– отличительный идентификатор ДТС, проверяющей цифровую подпись или маркер безопасности;

– данные или их цифровой отпечаток.

7.2.2.5 Средство создания свидетельства передачи с помощью встроенной ДТС.

Вместо передачи данных и/или квитанций непосредственно между отправителем и получателем данные могут быть переданы через ДТС, так что свидетельство неотказуемости может быть представлено этой ДТС. Данное средство также может быть использовано в случае наличия подозрений в том, что получатель заявил о сбое канала связи, чтобы отрицать доставку данных.

Для использования данного средства встроенной ДТС должны быть предоставлены следующие параметры:

– данные;

– отличительный идентификатор получателя.

Кроме того, могут быть предоставлены следующие параметры:

– цифровой отпечаток данных;

– отличительный идентификатор отправителя;

– цифровая подпись;

– отличительный идентификатор встроенной ДТС;

– политика обеспечения неотказуемости.

Возможными выходными данными, предоставляемыми ДТС, являются:

– отличительный идентификатор встроенной доверенной третьей стороны;

– отличительный идентификатор получателя;

– регистрационный номер свидетельства;

– дата и время регистрации;

– данные или их цифровой отпечаток.

8 Механизмы обеспечения неотказуемости

Сервис обеспечения неотказуемости может быть реализован с помощью механизмов, подобных цифровым подписям, шифрованию, механизмам подтверждения подлинности и целостности данных, при поддержке со стороны других сервисов, подобных маркированию времени. Для обеспечения неотказуемости могут быть использованы как симметричные, так и асимметричные криптографические алгоритмы. Сервис обеспечения неотказуемости может использовать комбинацию этих механизмов и сервисов, удовлетворяющих требованиям безопасности рассматриваемого приложения.

Данный раздел описывает механизмы, которые могут быть использованы для обеспечения сервиса обеспечения неотказуемости, а также некоторые из угроз для этих механизмов.

8.1 Обеспечения неотказуемости с помощью маркера безопасности ДТС (защищенного конверта)

В данном механизме свидетельство неотказуемости состоит из маркера безопасности, опломбированного с помощью секретного ключа, известного только ДТС. Доверенная третья сторона по запросу создания свидетельства от соответствующей стороны создает маркер безопасности, который может быть впоследствии проверен данной ДТС для пользователя свидетельства или судьи. В этом случае ДТС является создателем свидетельства и верификатором свидетельства.

Сторона, требующая создания свидетельства, передает доверенной третьей стороне данные или их цифровой отпечаток вместе с запросом о генерации маркера безопасности. Целостность этого запроса должна быть защищена (например, с помощью пломбы), может быть защищена также и конфиденциальность данного запроса (например, с помощью шифрования). Маркеры безопасности с защитой целостности называются защищенными конвертами.

Возможными входными данными, используемыми при создании маркера безопасности, являются:

– обозначение метода и/или криптографического алгоритма, используемого для обеспечения целостности маркера безопасности;

– обозначение метода и/или криптографического алгоритма, используемого для обеспечения конфиденциальности маркера безопасности;

– отличительный идентификатор субъекта свидетельства;

– отличительный идентификатор стороны, запрашивающей создание свидетельства;

– применяемая политика обеспечения неотказуемости;

– дата и время события или действия;

– данные, описывающие событие или действие.

Возможные выходные данные включают:

– маркер безопасности;

– дату и время создания маркера безопасности.

8.2 Обеспечение неотказуемости с использованием маркеров безопасности и модулей, защищенных от несанкционированного вмешательства

В данном механизме свидетельство неотказуемости состоит из маркера безопасности, опломбированного с помощью секретного ключа, хранящегося внутри криптографических модулей, которые защищены от несанкционированного вмешательства, и которыми обладают создатель свидетельства, верификатор свидетельства и судья. Модули, защищенные от несанкционированного вмешательства, ограничивают набор операций, которые могут быть выполнены с секретным ключом, и защищают значение ключа от раскрытия за пределами модуля.

Модуль создателя свидетельства разрешает использовать секретный ключ для создания опломбированного маркера, а модули, которыми обладают верификатор свидетельства и судья, разрешают только проверку маркера. Все участвующие стороны должны считать, что секретные ключи в модулях, защищенные от несанкционированного вмешательства, были установлены правильно, так что один секретный ключ может использоваться для создания свидетельства только одной сущностью, а другими сущностями этот ключ может использоваться только для проверки свидетельства.

При возникновении спорной ситуации пользователь свидетельства предъявляет опломбированный маркер судье и утверждает, что оно должно было создаваться с помощью модуля создателя свидетельства, а другие модули, содержащие этот же ключ, не способны создавать маркеры безопасности.

8.3 Обеспечение неотказуемости с использованием цифровой подписи

В данной схеме свидетельство неотказуемости состоит из структуры данных, подписанной цифровым образом. При создании подписи используют ключ подписания, а при проверке - ключ проверки.

В зависимости от политики безопасности может потребоваться информация о времени. Она может входить в цифровую подпись, обеспечиваемую сущностью и/или ДТС, выполняющей функции органа маркирования времени. Если метка времени предоставлена не ДТС, другие сущности не обязаны доверять ей. Если судье для разрешения спорной ситуации необходима метка времени и/или контекстная информация, данная информация должна быть получена от доверенных источников (например, от доверенной третьей стороны).

Цифровая подпись может создаваться субъектом свидетельства или ДТС, выполняющей функции создателя подписи.

Цифровая подпись, создаваемая субъектом свидетельства, называется непосредственной цифровой подписью. Механизм цифровой подписи, создаваемой ДТС от имени субъекта свидетельства, называется опосредованной цифровой подписью.

Если сертификат, используемый для проверки подписи, был отозван, то для разрешения спорных ситуаций недостаточно одних цифровых подписей. Для разрешения подобных ситуаций необходимо дополнительно представить судье свидетельство аннулирования сертификатов (например, списки отозванных сертификатов, СОС), показывающее, что на момент создания цифровой подписи сертификат все еще был действующим. Однако эта схема не позволяет разрешать спорные ситуации, если владелец закрытого ключа умышленно использует неправильное время, или если закрытый ключ, используемый для создания подписи, скомпрометирован злоумышленником. Для разрешения подобных спорных ситуаций необходимо дополнительно использовать доверенный временной эталон или встречную подпись ДТС, выполняющей функции маркирования времени (см. приложение Д).

Верификатор свидетельства может использовать сервис каталога для получения информации (такой как сертификаты безопасности), необходимой для процесса проверки. Верификатор свидетельства должен получить открытый ключ создателя свидетельства. Этот ключ может содержаться в сертификате безопасности, хранимом в каталоге. Может потребоваться несколько сертификатов. Чтобы убедиться в том, что сертификат действующий, необходимо также запросить список отозванных сертификатов, которые могут использоваться. Перечисленные действия необходимо выполнить для каждого удостоверяющего центра, задействованного в сертификации (см. [2]).

Для подтверждения подписи пользователь свидетельства может обратиться за помощью к ДТС, выполняющей функции проверки подписи. Данная доверенная третья сторона проверяет соответствие между оригинальным сообщением (или цифровым отпечатком сообщения, если он используется) и цифровой подписью.

В данном случае функция ДТС состоит в том, чтобы освободить пользователя свидетельства от сложностей процесса проверки подписи и обеспечить хранение результатов предыдущих запросов о проверке для оптимизации реакции на будущие запросы о проверке. Для этого ДТС может потребоваться некоторое взаимодействие с каталогом. Предполагается, что ДТС, выполняющая функции проверки подписи, хранит открытый ключ, по крайней мере, одного УЦ. Доверенная третья сторона также может учитывать отношения доверия, существующие между различными удостоверяющими центрами.

8.4 Обеспечение неотказуемости с использованием маркирования времени

Если требуется доверенный временной эталон, но нельзя доверять часам, предоставленным сущностью, создающей цифровую подпись или маркер безопасности, необходимо обратиться к доверенной третьей стороне, обеспечивающей маркирование времени. Маркирование времени может быть использовано для установления факта подписания сообщения до компрометации ключа подписи и, следовательно, того факта, что сообщение не является мошенничеством. При выполнении функции маркирования времени доверенная третья сторона создает цифровую подпись или маркер безопасности, чтобы установить время получения сообщения. Маркирование времени может быть запрошено создателем свидетельства, стороной, обращающейся к сервису обеспечения неотказуемости, пользователем свидетельства или верификатором свидетельства.

Маркирование времени добавляет к данным время, дату и пломбу или цифровую подпись. Маркирование времени не требует аутентификации сущности, запрашивающей метку времени. Верификатор свидетельства должен определить, находятся ли метки времени в пределах допустимого диапазона, задаваемого политикой безопасности.

Маркирование времени может быть объединено с процессом создания подписи или процессом создания маркера. Если у сущности, создающей цифровую подпись, есть надежные и доверенные часы, встречная подпись может не понадобиться.

8.5 Обеспечение неотказуемости с использованием встроенной доверенной третьей стороны

Средства доверенной третьей стороны могут быть запрошены явно для конкретного события или действия, либо они могут быть предоставлены неявно. Встроенная ДТС действует как посредник во всех взаимодействиях, для которых требуется сервис обеспечения неотказуемости, и может представить свидетельство пользователю свидетельства (например, судье). В любом случае, встроенная ДТС может передавать данные и отслеживать событие или действие.

Доверенной третьей стороне доверяется хранение записей для предстоящего разрешения спорных ситуаций. Хранимые доверенной третьей стороной данные или их цифровой отпечаток могут служить свидетельством.

8.6 Обеспечение неотказуемости с использованием нотариуса

В модели ВОС такие свойства данных, передаваемых между двумя или более сущностями, как целостность, источник, время и назначение, гарантируются механизмом нотариального заверения. Участвующие сущности доверяют нотариусу хранить необходимую информацию, требуемую для обеспечения гарантии с помощью свидетельствования, и хранить записи для предстоящего разрешения спорных ситуаций. Для поддержки сервисов нотариуса могут быть соответствующим образом использованы механизмы цифровой подписи, шифрования и контроля целостности.

Выполняя функции создания свидетельства, нотариус регистрирует свидетельство, гарантирующее свойства данных. Кроме того, для идентификации этого свидетельства может использоваться регистрационный номер.

Выполняя функции проверки свидетельства, нотариус подтверждает то, что свидетельство является действующим.

8.7 Угрозы для процессов обеспечения неотказуемости

Ни один механизм обеспечения неотказуемости не является абсолютно неуязвимым по отношению к угрозам. Механизм, включающий ДТС, может стать небезопасным, если ДТС ведет себя иначе, чем предполагается. Это может произойти либо в результате неожиданного сбоя, либо в результате атаки, выполненной извне. Последствия реализации такой угрозы могут быть значительны, но они не обсуждаются в настоящем стандарте. Механизмы обеспечения неотказуемости различаются по следствиям неправильной работы ДТС и по тому, насколько легко на ДТС воздействуют сбои протокола. Для выбора набора механизмов, удерживающих суммарный риск в допустимых пределах, должна быть проведена оценка того, какие угрозы являются наиболее вероятными и какие могут привести к значительным по-

следствиям в конкретной среде. Ниже обсуждаются некоторые примеры подобных угроз вместе с возможными мерами по противодействию им.

8.7.1 Компрометация ключей

8.7.1.1 Компрометация генерации ключа, принадлежащего сущности.

В период между компрометацией ключа и обнаружением этой компрометации законным владельцем ключа существует опасность того, что взломщик может использовать скомпрометированный ключ для создания свидетельства, которое пользователем свидетельства будет считаться действующим. Механизм обеспечения неотказуемости не может противостоять любому повреждению, вызванному подобным неправильным использованием ключа создания свидетельства. Однако возможно определить степень урона с помощью органа создания свидетельства (например, органа создания подписи), который может вести журнал учета созданных свидетельств и, следовательно, делает возможным обнаружить, какое свидетельство было создано и когда оно было создано. Также желательно, как можно шире оповестить о факте злоупотребления ключом, но не всегда возможно довести эту информацию до всех получателей, получивших свидетельство, созданное с помощью скомпрометированного ключа создания свидетельства.

Как только подобная компрометация ключа будет обнаружена законным владельцем ключа, ключ создания необходимо аннулировать. Если ключ создания является закрытым ключом, необходимо отозвать и сертификат соответствующего открытого ключа. Это может быть сделано с помощью сертификатов списков отозванных сертификатов, определенных в [2]. Однако этого недостаточно, так как эти действия не предотвращают злоупотребления ключом. Возможные способы противостояния этой угрозе включают использование механизма обеспечения неотказуемости, в котором создание свидетельства требует сотрудничества ДТС и субъекта свидетельства. Например, использование либо опосредованных цифровых подписей, либо встречных подписей органа маркирования времени может защитить от этой формы угрозы. В последнем случае политика обеспечения неотказуемости определяет, что свидетельство действительно только, если оно правильно подписано органом маркирования времени (см. приложение Д).

Можно также рассмотреть компрометацию ключа. Если политика обеспечения неотказуемости определяет, что субъект свидетельства не несет ответственности за злоупотребление своим ключом между моментом компрометации ключа и моментом обнаружения компрометации, то субъект свидетельства может воспользоваться этим для утверждения, что его ключ был скомпрометирован, и, таким образом, отказаться от действия или события, которое в действительности произошло. Этой угрозе можно противостоять, определив максимальное время задержки, допустимое до объявления о компрометации ключа. При такой политике, если пользователю свидетельства

не удается заявить о компрометации ключа в течение отведенного времени, то субъект свидетельства считается ответственным за все последствия злоупотребления ключами. Верификаторы свидетельства могут затем перед принятием любого свидетельства удостовериться в превышении задержки, допустимой для объявления о компрометации ключа.

8.7.1.2 Компрометация ключа создания.

При обнаружении компрометации ключа ДТС этот ключ должен быть аннулирован. Если ключ создания является закрытым ключом, необходимо отозвать и сертификат соответствующего открытого ключа. Это может быть сделано с помощью сертификатов списков отозванных сертификатов, определенных в [2]. Для работы со свидетельством, созданным ранее с использованием (возможно) скомпрометированного ключа, необходимо, чтобы ДТС регистрировала в журнале учета каждое использование своего ключа. Если ключ ДТС скомпрометирован, тогда для разрешения спорных ситуаций можно использовать журнал учета.

8.7.1.3 Подмена ключа проверки сущности.

Существует угроза, что верификатора/пользователя свидетельства обманом убедили в правильности имеющегося у них свидетельства. Однако при возникновении спорной ситуации, требующей судебного решения, обнаруживается, что свидетельство было недействительным. То есть пользователь свидетельства освобождается от ответственности, так как он действовал честно на основе предположительно правильного свидетельства, но судья решает спор не в его пользу. Возможные способы противостояния данной угрозе включают использование сильных процедур, чтобы убедиться, что правильной сущности соответствует правильный ключ проверки. При возникновении замены неправильный ключ проверки должен быть удален сразу же после обнаружения подмены.

8.7.1.4 Подмена ключа проверки ДТС.

Если ключ проверки является открытым ключом, используемым ДТС для непосредственной проверки свидетельства, то ДТС может быть обманом убеждена принять фальсифицированное свидетельство с помощью подделки любого средства передачи ключа проверки судье (например, бумажные документы, цепочка сертификатов). Конкретным примером этого является случай, когда злоумышленник подменяет копию открытого ключа, принадлежащего судье.

При обнаружении подобной атаки желательно как можно шире оповестить о факте подмены, но нужно заметить, что не всегда возможно довести эту информацию до всех пользователей свидетельства, которое могло проверяться с помощью подмененного ключа. Определить, какое свидетельство проверялось до предупреждения о подмене, можно с помощью органа проверки свидетельства (например, органа проверки подписи), который может вести журнал учета проверенных свидетельств. Таким способом можно уз-

нать, какое свидетельство было проверено до, а какое - после предупреждения.

Если ключ проверки является открытым ключом, используемым пользователями свидетельства для непосредственной проверки сертификатов, то он должен быть заменен, как только его подмена будет обнаружена.

8.7.2 Компрометация свидетельства

Информация, когда-то удовлетворительная в качестве свидетельства, может перестать быть удовлетворительной. Такая информация называется скомпрометированным свидетельством.

8.7.2.1 Неразрешенное изменение или разрушение свидетельства.

В этом случае действие или событие произошло, но стороне, заинтересованной в отрицании события, удается изменить или разрушить хранящееся свидетельство. Затем эта сторона может успешно отрицать событие, которое в действительности произошло. Этой угрозе можно противостоять, используя соответствующие механизмы защиты, чтобы предотвратить изменение или разрушение свидетельства (например, хранение резервных копий). Использование ДТС для хранения свидетельства может улучшить защиту от этой угрозы, так как средства хранения, обеспечиваемые ДТС, могут быть защищены лучше, чем средства хранения пользователя свидетельства.

8.7.2.1 Разрушение или аннулирование свидетельства.

Данная угроза состоит в разрушении свидетельства, хранимого доверенной третьей стороной. Угроза разрушения или аннулирования свидетельства может возникнуть, если ДТС недостаточно осторожна и не обеспечила соответствующую схему резервирования. Данной угрозы можно избежать путем использования такого механизма обеспечения неотказуемости, при котором все свидетельства, необходимые для разрешения спорных ситуаций, хранятся пользователем свидетельства. В этом случае пользователь свидетельства может гарантировать, что свидетельство не будет разрушено даже, если ДТС имеет злой умысел или неосторожна.

8.7.3 Фальсификация свидетельства

8.7.3.1 Фальсификация свидетельства извне.

В этом случае спорное событие не произошло, но злоумышленник проникает в систему извне и создает ложное свидетельство того, что событие произошло. Это может случиться при использовании нотариуса. Для защиты хранящихся свидетельств от подделки или изменения извне могут использоваться криптографические механизмы.

8.7.3.2 Ложное подтверждение свидетельства.

В механизмах, использующих ДТС для проверки свидетельства, существует угроза, что ДТС сообщит пользователю свидетельства о правильности свидетельства, хотя на самом деле это не так. При возникновении спорной

ситуации пользователь свидетельства не сможет убедить судью в том, что спорное событие произошло. Данной угрозы можно избежать путем использования такого механизма обеспечения неотказуемости, в котором верификатор свидетельства может проверить свидетельство непосредственно, не обращаясь к ДТС.

8.7.3.3 Фальсификация свидетельства доверенной третьей стороной.

Существует угроза того, что доверенная третья сторона может подделать свидетельство события, которого не было. Если судья доверяет ДТС, то он может принять фальсифицированное свидетельство и, следовательно, обманом вынужден принять неправильное решение. Для защиты от этой угрозы можно использовать механизм обеспечения неотказуемости, в котором ДТС трудно подделать свидетельство, или гарантирующий, что используемые ДТС заслуживают доверия, а также что они находятся в состоянии, когда им можно доверять. В общем случае, трудно обеспечить неопровержимое свидетельство достоверности сущности.

9 Взаимодействие с другими сервисами и механизмами защиты

В данном разделе описывается использование других сервисов защиты для обеспечения неотказуемости. Здесь не рассматривается использование неотказуемости для поддержки других сервисов защиты.

9.1 Аутентификация

При взаимодействии с доверенной третьей стороной сущностям может потребоваться доказывать свою подлинность с помощью сервиса аутентификации. Может потребоваться, чтобы последующие обмены защищались с помощью сервиса аутентификации источника данных. Например, при использовании ДТС для создания подписи может потребоваться проверить подлинность субъекта свидетельства перед созданием подписи.

9.2 Управление доступом

Сервис управления доступом может использоваться для обеспечения того, чтобы информация, хранящаяся ДТС, или сервис, предоставляемый ДТС, являлись доступными только для авторизованных сущностей.

9.3 Конфиденциальность

Сервисы конфиденциальности могут потребоваться для защиты данных от неразрешенного раскрытия (включая, в некоторых случаях, неразрешенное раскрытие данных, выполненное ДТС или при обращении к ней), а также для защиты от неразрешенного раскрытия свидетельства.

9.4 Целостность

Сервисы обеспечения целостности могут потребоваться для обеспечения целостности свидетельства.

Целостность данных также должна гарантироваться при обеспечении неотказуемости источника или при обеспечении неотказуемости доставки, чтобы данные, передаваемые между источником и получателем, нельзя было изменить, оставаясь необнаруженным.

9.5 Учет событий безопасности

Пользователь свидетельства может использовать функцию регистратора событий безопасности для хранения свидетельства, используемого при возникновении в дальнейшем спорных ситуаций.

Нотариус или встроенная ДТС могут использовать функцию регистратора событий безопасности для записи содержимого, источника, назначения и времени сообщений.

9.6 Управление ключами

Сервис управления ключами может быть использован для предоставления ключей, применяемых при создании свидетельства и при проверке свидетельства. Сервис управления ключами может потребоваться для предоставления ключей проверки свидетельства, даже если соответствующий ключ, используемый для создания свидетельства, стал недействительным или недоступным.

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

А.1 Обеспечение неотказуемости источника

Сервис обеспечения неотказуемости источника предоставляет получателю данных свидетельство, которое защищает от любой попытки отправителя ложно отрицать отправку данных или их содержание. Это может быть достигнуто, если создатель свидетельства (обычно отправитель данных, но может быть и ДТС) доставляет верификатору свидетельства (обычно получателю данных, но возможно и стороне, представляющей получателя) свидетельство того, что данные были посланы отправителем.

При использовании механизма подписи свидетельство является цифровой подписью данных или цифровым отпечатком данных. Обеспечение неотказуемости источника зависит от заранее согласованной схемы подтверждения действительности свидетельства. Оно состоит из следующих стадий:

1) Сторона, запрашивающая сервис обеспечения неотказуемости, создает свидетельство или получает свидетельство от ДТС и добавляет это свидетельство к данным.

2) Свидетельство делается доступным пользователю свидетельства.

3) В случае спорной ситуации пользователь свидетельства представляет данные и свидетельство; судья сравнивает данные со свидетельством.

А.2 Обеспечение неотказуемости доставки

Сервис обеспечения неотказуемости доставки предоставляет отправителю данных свидетельство, которое защищает от любой попытки получателя ложно отрицать получение данных или их содержание. Это может быть достигнуто, если создатель свидетельства (обычно получатель данных, но может быть и ДТС) доставляет верификатору свидетельства (обычно отправителю данных, но возможно и стороне, представляющей отправителя, или ДТС) свидетельство того, что данные были доставлены.

Данный сервис зависит от возвращения получателем данных квитанции со свидетельством. Квитанция должна содержать подтверждение получения в форме цифровой подписи оригинального сообщения (или цифрового отпечатка оригинального сообщения) и время получения.

При использовании механизма подписи в качестве свидетельства необходима подписанная квитанция.

Можно рассматривать два варианта этого сервиса в зависимости от того, участвует или нет в его поддержке ДТС, выполняющая функцию органа доставки.

Приложение Б
(справочное)
Структура средств обеспечения неотказуемости

<table>
<tr><td colspan="2" rowspan="3">Структура средств безопасности</td><td rowspan="2">Элемент</td><td colspan="4">Сущность: субъект свидетельства, создатель свидетельства, верификатор свидетельства, ДТС обеспечения неотказуемости, судья</td></tr>
<tr><td colspan="4">Информационный объект: свидетельство</td></tr>
<tr><td colspan="5">Цель сущности: собирать, поддерживать, делать доступным и подтверждать неопровержимое свидетельство</td></tr>
<tr><td rowspan="7">Действия</td><td>Сущность</td><td colspan="5">ДТС, орган безопасности</td></tr>
<tr><td>Функция</td><td colspan="5">(Не определена)</td></tr>
<tr><td>Действия, связанные с управлением</td><td colspan="5">- установка;
- изменение;
- удаление;
- ведение реестра.</td></tr>
<tr><td>Сущность</td><td>Создатель свидетельства</td><td>Верификатор свидетельства</td><td>ДТС обеспечения неотказуемости</td><td>Судья</td></tr>
<tr><td>Функция</td><td>(Не определена)</td><td>(Не определена)</td><td>(Не определена)</td><td>(Не определена)</td></tr>
<tr><td>Действия, связанные с управлением</td><td>- создание свидетельства;
- создание нотариально заверенного свидетельства.</td><td>- создание свидетельства;
- создание нотариально заверенного свидетельства.</td><td>- создание маркера времени;
- передача с помощью ДТС.</td><td>(Не определена)</td></tr>
<tr><td rowspan="3">Информация</td><td>Элемент данных ввода/вывода, управляемый SDA</td><td colspan="5">- информация управления, например, пароль или ключи;
- тип информации;
- политика обеспечения неотказуемости.</td></tr>
<tr><td>Тип информации, используемой в операции</td><td colspan="5">- свидетельство;
- цифровая подпись;
- маркер безопасности;
- сертификат безопасности;
- маркер времени.</td></tr>
<tr><td>Управляющая информация</td><td colspan="5">Регистрация в журнале учета события и результатов суда;
регистрация отношений между сущностями.</td></tr>
</table>

Приложение В
(справочное)
Обеспечение неотказуемости в системах хранения и пересылки

В системе хранения и пересылки сообщение между его отправителем и получателем передается через одного или нескольких посредников, называемых агентами передачи. В подобных системах передача сообщения затрагивает не только связь между отправителем и получателем, но и связь между отправителем и агентом передачи, связь между агентом передачи и получателем, а также связь между агентами передачи. Сервис обеспечения неотказуемости может использоваться независимо на каждом из этапов передачи сообщения к месту окончательного назначения.

Сервис обеспечения неотказуемости источника защищает от ложного отрицания отправителем факта отправки сообщения или содержания сообщения. Свидетельство, предоставленное данным сервисом, может использоваться либо получателем, либо агентами передачи.

Сервис обеспечения неотказуемости доставки защищает от ложного отрицания получателем факта получения сообщения или содержания сообщения. Свидетельство, предоставленное данным сервисом, может использоваться либо отправителем, либо агентами передачи.

Сервис обеспечения неотказуемости отправки используется для защиты от ложного отрицания агентом передачи факта принятия сообщения для передачи (либо от отправителя, либо от другого агента передачи). Свидетельство, предоставленное данным сервисом, может использоваться отправителем, либо другими агентами передачи.

Сервис обеспечения неотказуемости транспортировки используется для защиты от ложного отрицания агентом передачи факта передачи сообщения для передачи (либо получателю, либо другому агенту передачи). Свидетельство, предоставленное данным сервисом, используется отправителем.

Сервис обеспечения неотказуемости передачи используется для защиты от ложного отрицания агентом передачи принятой ответственности за доставку сообщения. Данный сервис используется, если в доставке сообщения участвует несколько агентов передачи. Когда агент передачи, принявший сообщение первым, передает его второму агенту передачи, второй агент передачи может представить первому свидетельство того, что он принял ответственность за сообщение. Если количество агентов передачи больше двух, данный сервис также может использоваться между вторым и третьим агентом, и т.д.

Порядок использования различных типов сервисов обеспечения неотказуемости приведен в следующей таблице:

Наименование сервиса	Защищает от	Используется
Неотказуемость источника	Источника	Получателем, агентом передачи
Неотказуемость отправки	Агента передачи	Отправителем
Неотказуемость транспортировки	Агента передачи	Отправителем
Неотказуемость передачи	Агента передачи	Агентом передачи
Неотказуемость доставки	Получателя	Отправителем, агентом передачи

Перечисленные дополнительные типы сервисов обеспечения неотказуемости (неотказуемость отправки и транспортировки) могут быть обеспечены с помощью анализа системы на различных уровнях модульности и последующего использования механизмов, обеспечивающих более фундаментальные типы сервисов обеспечения неотказуемости

(неотказуемость источника и неотказуемость доставки). Например, неотказуемость транспортировки может быть обеспечена с помощью разбиения передачи сообщения от отправителя получателю на последовательность обменов сообщениями, одно из которых является квитанцией о доставке, переданной агентом передачи отправителю, и затем, с использованием сервиса неотказуемости отправления, защита этой квитанции.

Приложение Г
(справочное)
Восстановление в сервисе обеспечения неотказуемости

Восстановление безопасности связано с ситуациями, которые не должны возникать в нормальных условиях. Однако реальность компьютерной безопасности состоит в том, что ненормальные условия возникают, и лучше всего заранее подготовиться к подобным случаям.

В частности, многие механизмы обеспечения неотказуемости зависят от криптографических ключей и секретности, необходимой для их защиты. Потеря и раскрытие криптографического ключа должны учитываться планом восстановления, действия по которому могут быть выполнены немедленно.

При использовании закрытых криптографических ключей для сервиса обеспечения неотказуемости может возникнуть следующая ситуация:

Данные, подписанные нечестной стороной (С), использующей скомпрометированный закрытый ключ стороны А, могут быть переданы честному участнику (В). Можно предположить, что в некоторый момент времени у стороны В появится причина в результате действия (или бездействия), связанного с несанкционированным сообщением, найти сторону А и представить подписанное сообщение как оправдание действия. Сторона А будет заявлять о потере соответствующего закрытого ключа и ссылаться на публичное объявление об этом.

При рассмотрении дела судьей ответственность стороны А будет, вероятно, определена в результате сравнения разницы времени между публичным объявлением о компрометации ключа и подписанным несанкционированным сообщением. Сторона А почти наверняка будет признана виновной, если сообщение предшествует объявлению о компрометации ключа. Следовательно, если сторона С сумеет обеспечить более раннюю дату сообщения, то сторона А будет нести ответственность, если не будут предприняты некоторые меры предосторожности, связанные с этим случаем.

Для выхода из подобной ситуации необходимо иметь возможность узнать, когда точно было подписано сообщение. Так как нельзя доверять времени, вставленному в сообщение стороной С, необходимо обратиться к ДТС для официальной регистрации сообщения с помощью:

– копирования сообщения и подписи в соответствующий журнал учета (т.е. с помощью нотариуса);

– применения встречной подписи сообщения, включающей дату и время регистрации, полученные от независимой доверенной стороны (т.е. сервиса маркирования времени).

Следуя этой процедуре, нечестный участник непреднамеренно зарегистрирует действительные дату и время подписи. Судья сможет затем принять решение об ответственности потерпевшей стороны (А) в зависимости от следующего:

– во-первых, от сравнения даты/времени сообщения и даты/времени встречной подписи, которые должны попадать в достаточно небольшое временное окно (например, 24 часа);

– во-вторых, от сравнения даты/времени сообщения и официального уведомления о потере или компрометации ключа.

Таким образом, эффективное злоупотребление потерянным или скомпрометированным криптографическим ключом будет сведено к временному окну, разрешенному сервисом маркирования времени для регистрации данных.

Ответственность стороны А в случае компрометации ключа зависит от действующей политики безопасности. Уязвимости в безопасности не всегда поддаются немедленному обнаружению. Следовательно, если сторона А уведомляет ДТС, как только она узнает о компрометации, сторона С может подделывать сообщения после компрометации закрытого ключа стороны А и до обнаружения стороной А компрометации ключа.

Для разрешения спорных ситуаций могут быть важны два следующих момента времени:

1) Время, когда сторона А сообщила о компрометации. Сторона А будет отказываться от всех сообщений, для которых можно показать, что они подписаны после этого времени (сторона А прекращает использовать закрытый ключ, как только ей становится известно о компрометации).

2) Время, предшествующее по утверждению стороны А компрометации ключа. Сторона А не будет отказываться от сообщений, для которых можно показать, что они были подписаны в это время. Это время может не существовать: сторона А может обнаружить компрометацию, но не знать точно, когда она произошла.

Приложение Д
(справочное)
Взаимодействие с каталогом

Цифровая подпись может проверяться с помощью соответствующего открытого ключа. Если открытый ключ содержится в сертификате пользователя, помещенном в каталог, можно проверить правильность ключа при условии, что известен открытый ключ УЦ.

Так как удостоверяющий центр, издавший сертификат, мог изменить свой открытый ключ с момента подготовки сертификата, требуются средства проверки правильности "старого" открытого ключа. Так как обычно единственным известным ключом является текущий открытый ключ УЦ, существует необходимость связать текущий открытый ключ и устаревшие открытые ключи. Поскольку получателю неизвестно об изменениях ключа УЦ, обеспечение способа проверять "старые" сертификаты входит в обязанности различных удостоверяющих центров. Это может быть реализовано двумя способами:

– с помощью сертификации каждого старого открытого ключа УЦ новым открытым ключом УЦ;

– с помощью сертификации каждого старого открытого ключа УЦ следующим открытым ключом УЦ.

В первом случае действенность старого открытого ключа УЦ, соответствующего закрытому ключу, использованному удостоверяющим центром для издания оригинального сертификата, можно проверить непосредственно.

В последнем случае необходимо суметь собрать цепочку сертификатов, чтобы шаг за шагом проверить действенность старого открытого ключа УЦ. Это выполняется следующим образом: сначала находится сертификат с периодом действия, соответствующим дате/времени подписанного сообщения, а затем рекурсивно находится сертификат с перекрывающимся, но более поздним периодом действия, позволяющий найти значение предыдущего открытого ключа УЦ.

Примечание. Если возможна компрометация старого открытого ключа УЦ, первый метод предпочтителен, потому что при втором методе цепочка сертификатов, протянутая до старого открытого ключа УЦ, будет разорвана и, следовательно, старые открытые ключи УЦ неявно станут недействительными.

Для сертификатов, переставших быть действительными, УЦ не отслеживает в каталоге сертификаты списков отозванных сертификатов других УЦ или их пользователей. Следовательно, чтобы доказать, что данный открытый ключ был действителен в некоторый момент времени, пользователю свидетельства или ДТС придется собирать всю необходимую информацию (включая списки отозванных сертификатов, даже если они пусты), пока она доступна.

Сертификат списка отозванных сертификатов содержит дату, когда он был издан УЦ. Он также может содержать другую дату, которая может помочь разрешить некоторые спорные ситуации, - дату, когда пользователь все еще был убежден, что его ключ не был скомпрометирован. Все подписи, выполненные пользователем до этой даты, будут признаны этим пользователем действительными. При отсутствии этой даты, в самом худшем случае, все подписи, выполненные в течение срока действия сертификата ключа, будут рассматриваться как недействительные. В коммерческой среде для пользователя может быть очень важно, чтобы подписанный документ считался действенным, даже если ключ, использованный для подписания сообщения, был потерян. Хотя в сертификате спи-

ска отозванных сертификатов эта дата необязательна, она может потребоваться, если ключ соответствующего сертификата используется для сервиса обеспечения неотказуемости.

Доверительные отношения со временем могут меняться. Например, судья может доверять УЦ сегодня, но необязательно завтра. Информация о виде доверия должна быть доступной, чтобы пользователь мог узнать, может ли потенциальная спорная ситуация быть решена в его пользу. Должен быть показан тип отношений доверия, признаваемый данным судьей. Эти условия доверия могут моделироваться с помощью следующих выражений доверия:

– удостоверяющий центр является полностью доверенными, и для него известно текущее значение открытого ключа;

– удостоверяющему центру доверено издавать сертификаты УЦ и пользовательские сертификаты;

– удостоверяющему центру доверено издавать только пользовательские сертификаты (но не сертификаты УЦ).

Эту информацию необходимо сделать свободно доступной для пользователя свидетельства. Она может принимать форму сертификата безопасности, включающего срок действия. Определены две формы сертификата политики безопасности: сертификаты политики безопасности, в которых за отслеживание этих сертификатов отвечает судья, и сертификаты политики безопасности, в которых за отслеживание этих сертификатов отвечает получатель.

Приложение
(справочное)
Библиография

[1] ИСО/МЭК 7498-1-1994 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

[2] ИСО/МЭК 9594-8: 1995 Информационная технология. Взаимодействие открытых систем. Справочник. Часть 8. Основы аутентификации.

УДК 681.324:006.354 **МКС 35.040**

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

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