ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚОРҒАУ ӘДІСТЕРІ
Қол жеткізуді басқару бойынша ақпараттық қорғау объектілері

Информационная технология
МЕТОДЫ ЗАЩИТЫ
Объекты информационной защиты по управлению доступом

ҚР СТ ИСО/МЭК 15816-2009

ISO/IEC 15816:2002 Information technology. Security techniques. Security information objects for access control, IDT

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚОРҒАУ ӘДІСТЕРІ
Қол жеткізуді басқару бойынша ақпараттық қорғау объектілері

ҚР СТ ИСО/МЭК 15816-2009

ISO/IEC 15816:2002 Information technology. Security techniques. Security information objects for access control, IDT

Ресми басылым

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

Астана

Алғысөз

1 Техникалық реттеу және метрология комитетінің «Қазақстан стандарттау және сертификаттау институты» республикалық мемлекеттік кәсіпорны және 63 «Байланыс жүйелері, құралдары мен қызметтері» стандарттау жөніндегі техникалық комитеті («Fidelis_2008» жауапкершілігі шектеулі серіктестігі) **ӘЗІРЛЕП ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті Төрағасының 2009 жылғы 27 қазандағы № 534-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт ISO/IEC 15816:2002 Information technology. Security techniques Security information Objects for access control (Ақпараттық технология. Қорғау әдістері. Қол жеткізуді басқару бойынша ақпараттық қорғау объектілері) халықаралық стандартымен бірдей.

Ағылшын тілінен аударылған (en)
Сәйкестік дәрежесі – сәйкес (IDT)

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ **2014 жыл**
ТЕКСЕРУ КЕЗЕҢДІЛІГІ **5 жыл**

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Осы стандартқа өзгерістер туралы ақпарат «Стандарттау бойынша нормативтік құжаттар» сілтемесінде, ал өзгерістер мәтіні – ай сайын жарық көретін «Мемлекеттік стандарттар» ақпараттық нұсқауларда жарияланады. Осы стандарт қайта қаралған (жойылған) немесе ауыстырылған жағдайда тиісті ақпарат «Мемлекеттік стандарт» ақпараттық сілтемесінде жарияланады.

Мазмұны

Кіріспе

Осы қол жеткізуді басқару бойынша ақпараттық қауіпсіздік объектісі (АҚО) жөніндегі стандарт бір функцияның көп реттік және әртүрлі анықтамаларын болдырмау үшін қауіпсіздіктің бір стандартында туындайтын қажеттілікті, объектінің анықтамасын айқындайды. Осы анықтамалардың нақтысы ASN.1 тілінің көмегімен алынған.

Қауіпсіздікті басқару мақсаты ақпаратты қоса алғанда мүлік тиісті жолмен және рентабельдік шеңберде қорғалғанына кепілдік беруден тұрады. Мүдделер мен құқықты құраушы жан-жақтылық меншікті қорғау үшін ұйым өзінің ақпаратын өңдеуді басқаруы тиіс. Маңызды шығын немесе қиындықтар маңызды ақпарат туғызушыға немесе иесіне залалын тигізуі мүмкін, мысалы, егер ол алуға құқығы жоқ адамның қолына тисе (құпиялық бұзылса) немесе егер ол қандай да бір жолмен өзгертілсе (тұтастығы бұзылса). Әрбір ұйым өзінің меншіктік ақпаратын және мүлкін оны сақтаудың, өңдеудің және жеке және жалпы қолжетімді желі бойынша ұйым арасында және ұйым ішінде беру уақытында барлық нысандарды тиісті жолмен қорғауға кепілдік беруі қажет. Ұйымдар олардың мүлкі басқа адамдарда болғанда немесе олармен өңделу кезінде қызмет неғұрлым таралып жүзеге асырылғанда тиісті жолмен қорғалатынына сенімді болуы тиіс.

Қолжетімді басқару бойынша АҚО дамыту мотивациясы ұқсас функциялар үшін жалпы құрылымдарды қолданудан туындайтын қауіпсіздікті басқарудағы өзара іс-әрекеттің икемділігіне және мүмкіндігіне қол жеткізу болып табылады. Қол жеткізуді басқару бойынша құпиялық санатын және баламалық әдістерді стандарттау осы стандартта да қарастырылады.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚОРҒАУ ӘДІСТЕРІ
Қол жеткізуді басқару бойынша ақпараттық қорғау объектілері

Information technology. Security techniques.
Security information objects for access control

Енгізілген күні 2010-07-01

1 Қолданылу саласы

Осы стандарт:

а) қол жеткізуді бақылау бойынша ақпараттық қорғаудың жалпы және арнайы объектілерінің (бұдан әрі – АҚО) теориялық синтаксисін анықтау жөніндегі басшылық принциптерін бекіту;

б) қол жеткізуді басқару бойынша АҚО негіздерін егжей-тегжейлеу;

в) қол жеткізуді басқару бойынша АҚО арнайы ерекшеліктерін егжей-тегжейлеу кезінде қолданылады.

Осы стандарттың қолданылу саласы ASN.1 тілі терминдерінде сипаттамаларды және қосымша семантикалық түсініктерді синтаксистік анықтау арқылы АҚО тек «статиканы» ғана қамтиды.

2 Терминдер, анықтамалар және қысқартулар

Осы стандартта [1] , [2], [3], [4] бойынша терминдер, сондай-ақ тиісті анықтамалары және қысқартулары бар мынадай терминдер қолданылады:

2.1 **АҚО негізгі класы** (generic SIO Class): Бір немесе бірнеше құрауыштар үшін деректер типі анықталмаған АҚО класы.

2.2 **Қауіпсіздік жөніндегі маман** (security authority): Қауіпсіздік жүйесінің іс-әрекеті аймағы шегінде қауіпсіздік саясатын басқаруға жауапты адам.

2.3 **Қауіпсіздік жүйесі іс-әрекетінің аймағы** (security domain): Қауіпсіздіктің жалпы саясатына жататын тұтынушылардың және жүйелердің жиынтығы.

2.4 **Ақпараттық қауіпсіздік объектісі** (security information object): АҚО класының нұсқасы.

2.5 **Ақпараттық қауіпсіздік объектісінің класы** (security information object class): Қауіпсіз пайдалану үшін орындалған ақпараттық объектінің класы.

2.6 **Қауіпсіздік саясатының ақпараттық файлы** (security policy information file): Қауіпсіздік жүйесінің іс-әрекеті аймағы үшін арнайы ақпарат беретін тұжырымдама.

2.7 **АҚО арнайы класы** (specific SIO class): Барлық құрауыштар үшін деректер типі толық анықталған АҚО класы.

2.8 **ASN.1 тілі** (abstract syntax notation one (ASN.1)): Ашық жүйелердің өзара іс-әрекеттері үшін пайдаланылатын деректерді кодтау, беру және кодын алып тастау үшін қызмет ететін деректер құрылымын сипаттауға арналған тіл білмеуді болдырмайтын кодтау әдісін жабдықтау және нақты нотация үшін спецификаға тәуелсіз объектілердің құрылымын сипаттауға арналған ережелердің жиынтығын білдіреді.

Ресми басылым

2.9. **ҚББЕ – қол жеткізуді басқарудың базалық ережесі** (rule based access control (RBAC)).

2.10. **ТТЖХКК – Телеграф және телефон жөніндегі халықаралық кеңес комитет** (consultative Committee for International Telephone and Telegraphy (CCITT)).

3 АҚО негізгі ережесі

3.1 АҚО класын сипаттау

АҚО класы мыналарды қамтиды:

– АҚО класын сәйкестендіруге арналған мән;

– АҚО класындағы әрбір құрауыштағы деректердің бір немесе одан да артық типтердің спецификациясының жиыны;

– АҚО класында тиісті пайдаланылатын семантикаларды жазу.

3.2 АҚО-ның негізгі класына сәйкестік

АҚО-ның негізгі класы бір немесе одан да артық құрауыштардың деректер типі толық анықталмаған АҚО класы болып табылады. АҚО-ның спецификалық класы – барлық құрауыштар үшін деректер типі толық анықталған АҚО класы. АҚО-ның жалпы класы АҚО спецификалық класстарды біріктіруге сәйкес келеді.

3.3 АҚО құрылымы

Әрбір АҚО-ның **с**пецификациясы осы стандартта мынадай бөліктерді қамтиды:

- АҚО сипаты;
- АҚО пайдалануды түсіндіру;
- АҚО құрауыштарын сипаттау.

АҚО құрауыштарын сипаттау ASN.1 тілінің спецификациясын және класы анықталатын объекті сәйкестендіргішті қамтиды.

4 Ақпараттық қорғаныш объектілерінің спецификациясы

Егер АҚО үшін жаңа технологиялық талаптар анықталса, кейінгі әрекеттер жұмыс істеп тұрған спецификацияны қайта пайдалану және мынадай бір талаптардан тұратын әртүрлі спецификацияны таратуды төмендету мүмкіндігі жүзеге асырылған болуы тиіс:

- егер осы стандарт жаңа талаптардан тұратын АҚО анықтаса, осы стандарттың анықтамасы пайдаланылуы тиіс.

- осы стандартта анықталған АҚО құрауыштары, егер олар жаңа талаптардың бір бөлігін қанағаттандыратын болса, жаңа АҚО-ның анықтамасында пайдаланылуы тиіс.

Қол жеткізуді басқаруды қолдау үшін әзірленген АҚР спецификациясы мынадай бөлімдерге енгізілген. Осы бөлімдерде қаралған ақпараттық қорғаныш объектілері үшін ASN.1 тілінің толық анықтамасы модуль ретінде А қосымшасына енгізілген. Бұл модуль 1-суретке сәйкес сәйкестендіріледі.

```
id-SIOsAccessControl-MODULE OBJECT IDENTIFIER ::= {
        joint-iso-itu-t sios(24) specification(0) modules(0) accessControl(0)}
```

1-сурет

4.1 Құпиялылық санаты

4.1.1 Кіріспе

Ұйым мыналарды:

а) жүйеде сақталатын деректер ұсынған қорғаныш деңгейін;

б) деректерге, процестерге немесе ресурстарға қол жетімдік алуға өкілетті адамды;

в) материалдың кез келген дисплейінде немесе баспа үлгісінде көрсетілетін қауіпсіздікті таңбалауды;

г) жүйелер арасында берілетін деректерді маршруттауға және шифрлауға қойылатын талаптарды;

д) санкцияланбаған көшірмелеуге қарсы қорғанышқа арналған талаптарды;

е) деректерді сақтау әдістерін;

ж) пайдаланылатын кодтау алгоритмдерін;

и) субъектілерді авторлау әдістерін;

к) объектіге қолданылатын іс-әрекеттерді тексеру қажеттігін;

л) алушылардың объектіні алудан бас тартуын болдырмауға қойылатын талаптарды;

м) деректердің жасандылығын растау үшін цифрлы қол қоюлардың қажеттілік мәртебесін қамтитын құпиялықтың санатын анықтайтын қауіпсіздік параметрі орнатылған қауіпсіздік саясаты болуға тиіс.

Деректер ақпараттық жүйеден (АЖ) оқылса немесе олар жүйелер арасында электронды әдіспен берілгенде осы деректер тиесілі қауіпсіздік санаттарын көрсету үшін және деректер қандай жолмен қауіпсіздік жоспары жүйесінде өңделуі тиістігін анықтау үшін деректер таңбаланады. Белгі қорғаныш ақпараттан жеке, бірақ логика жағынан оны көрсетуге сәйкестендірілуі мүмкін.

Құпиялық белгісінің тұтастығы және олардың ақпаратқа байланыстылығына кепілдік берілуі тиіс. Бұл ақпараттық жүйелерге және желілерге қорғалған ақпаратқа рұқсат алуды қажет етпей маршруттау және қол жеткізуді басқару тәрізді шешімдердің қауіпсіздігінің тиісті саласын қабылдауға мүмкіндік береді. Құпиялық белгісі ақпараттық жүйедегі деректердің әрбір объектісімен байланысты болуы мүмкін, мысалы, құжаттар, электронды поштадағы хабарлама, көрінетін терезе, деректер базасының жазбасы, директория элементтері және электронды нысандар. Белгілер объектілерді, үй-жайларды сақтау кезінде пайдалану (әсіресе жүйелер арасында) жұмыс істеп тұрған объектілердің ішінен жаңа объекті құратын қосымшаларды қоса алғанда белгі бойынша әрекет ететін қосымшаларды өңдеуге арналған.

Ақпараттық қауіпсіздік іс-әрекетінің әртүрлі аймақтары арасында белгіні қамтыған ақпарат берілгенде әрекет ету аймағы осы деректерді қабылдауды қамтамасыз ету үшін ақпараттық қауіпсіздіктің саясатын келісуге тиіс. Егер ақпараттық қауіпсіздік аймағында белгілерді қабылдау бірге пайдаланылатын деректер саясатымен анықталған белгілерден айырмашылығы болса, онда бірге пайдаланылатын саясат деректерді қандай белгілер жиынына сәйкес беруді анықтауға тиіс.

Белгілер ақпарат қауіпсіздігінің жеткілікті деңгейіне кепілдік бермейді. Қабылданған ақпараттық қауіпсіздік саясатын белгісі бар ақпарат оларды басқару шеңберінде тұрғанда әрбір ұйым қолдануы қажет. Ақпараттық хабарламаны өңдейтін барлық ұйымдар, жекелеген өкілдер, ақпараттық технология жүйелері осы ақпараттың ақпараттық қауіпсіздігі саясатымен таныс деп есептелінеді. Ақпарат алмасатын ұйымдар ақпаратты басқару ақпараттық қауіпсіздіктің келісілген саясатына сәйкес жүзеге асырылатынына сенімді болуы үшін бір бірімен келісім орнатады.

4.1.2 ASN.1 тілінің құпиялылық белгісінің спецификациясы

Құпиялылық белгісі 2-суретте берілгендей мынадай жолмен сәйкестендіріледі.

```
id-ConfidentialityLabel OBJECT IDENTIFIER ::= {
        joint-iso-itu sios(24) specification(0) securityLabels(1) confidentiality(0)}
ConfidentialityLabel ::= SET {
        security-policy-identifier          SecurityPolicyIdentifier OPTIONAL,
        security-classification             INTEGER(0..MAX) OPTIONAL,
```

```
        privacy-mark                    PrivacyMark OPTIONAL,
        security-categories             SecurityCategories OPTIONAL }
(ALL EXCEPT ({-- none; at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

PrivacyMark ::= CHOICE {
  pString                               PrintableString (SIZE(1..ub-privacy-mark-length)),
  utf8String                            UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128 -- as defined in ITU-T Rec. X.411 | ISO/IEC 10021-4

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
        type [0]   SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
        value      [1]   SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type})
}
SECURITY-CATEGORY ::= TYPE-IDENTIFIER

                SecurityCategoriesTable SECURITY-CATEGORY ::=

                        {…}
```

2-сурет

TYPE-IDENTIFIER объектісінің ақпараттық класын кеңейту мысалы Б қосымшасында келтірілген.

4.1.3 Құпиялылық белгілерін байластыру әдістері

4.1.3.1 1-байластыру әдісі

Деректер көшірмесі (D) және құпиялық белгілер көшірмесі (L) деректер жазбасы ретінде қауіпсіздік жүйесінің шекарасы ішінде бірге сақталады. Жүйе құпиялық белгілердің тұтастығын және деректер тұтастығын қорғауға қажетінше мүмкін деп есептелінеді.

Жүйе ұсынған қорғаныш авторланбаған тұтынушы немесе қосымша осы деректерге байланыстырылған деректерді немесе құпиялық белгілерді өзгертпейтіндей болуға тиіс. Байланыстың бұл әдісіне деректерді және құпиялық белгілерді байластыру үшін ешбір шифрланған функция қажет емес.

4.1.3.2 2-байластыру әдісі

Құпия емес цифрлік қолтаңба 3-суретте көрсетілгендей (SigAlg) цифрлік қолтаңбаның алгоритмін пайдаланумен және ашық кілтпен алгоритмнің (X) персоналды кілтін D және L-де анықтады.

S = SigAlg(X,f(D),L)

3-сурет

Цифрлік қолтаңба жазбасында D және L-мен бірге сақталады. Генерирленген цифрлік жазба L -ды D-мен байланыстырады. Бұл анықтамада f - ашық функция, сондықтан f (D) D туралы ақпаратты көрсетпейді.

Осы байланыстылық әдісінде L және S қауіпсіздік жүйесінің шекарасы ішінде сақталуға тиіс. Егер шифрлы қызмет L, D немесе S дұрыс емес мәнінен болған болса, уақтылы еместігі анықталады. Қолды растау кілті ретінде ашық кілт алгоритмін пайдалану арқылы орындалады.

4.1.3.3 3-байластыру әдісі

Хабарлама бара-барлығының құпия емес коды (Message authentification code, MAC)

4-суретте көрсетілгендей (MacAlg) шифрлау алгоритмінің MAC-generation режимін және MAC (K-MAC) алгоритмінің құпия кілтін пайдалану арқылы D және L-да анықтайды.

MAC = MacAlg(K-MAC,f(D),L)

4-сурет

MAC деректер жазбасында D және L-мен бірге сақталады. Құрылған MAC D-ы L-мен байланыстырады. Бұл анықтамада f - ашық функция, сондықтан f (D) D туралы ақпаратты көрсетпейді.

Осы байланыстылық әдісінде L және MAC қауіпсіздік жүйесінің шекарасы ішінде сақталуы тиіс.

Егер шифрлы қызмет L, D немесе MAC дұрыс емес мәнінен болған болса, уақтылы еместігі анықталады. Бұл ұсынылған L және D мәндерін және K-MAC көшірмелерін пайдалана отырып және нәтижесін ұсынылған MAC-пен салыстыра отырып, MAC қатысты есептеу арқылы орындалады.

4.2 Қауіпсіздік саясатының ақпараттық файлы

4.2.1 Кіріспе

Қауіпсіздік саясаты оның ең қарапайым түрінде қауіпсіздік қызметі жұмыстарын қамтамасыз ету үшін критерийлер жиынтығы болып табылады. Қол жеткізуді басқару саясатын есепке ала отырып, қауіпсіздік саясаты бастамашы және мақсаттар арасындағы қол жеткізуді басқару саясатын жүзеге асыру үшін құралдарды анықтайтын қауіпсіздік саясатының көптеген жоғары жүйелік деңгейі болып табылады.

Қол жеткізуді басқару тетігі:

- спецификалық саясат мүмкіндік беретін ақпаратты беруге рұқсат етуге;
- спецификалық саясат айқын рұқсат етпейтін ақпаратты беруге рұқсат етпеуге тиіс.

Қауіпсіздік саясаты қол жеткізуді басқару тетігінің шешімін қабылдау үшін негіз болып табылады. Іс-әрекет аймағы үшін спецификалық қауіпсіздік саясатының ақпараттық файлы арқылы беріледі.

Қауіпсіздік саясатының ақпараттық құралы мыналарды қамтиды:

а) verionInformation – ASN.1 тілінің синтаксисінің нұсқасын және қауіпсіздік саясатының ақпараттық файлының спецификациясының қоса жүретін семантикасын көрсетеді;

б) updateInformation – қауіпсіздік саясатының ақпараттық файлының деректерінің әрекетін көрсетеді;

в) securityPolicyIdData – қауіпсіздік саясатының ақпараттық файлы қолданылатын қауіпсіздік саясатын сәйкестендіреді;

г) privilegeId – қауіпсіздік саясатының ақпараттық файлымен қосылып пайдаланылатын сенімді сертификаттарының қауіпсіздігі санатының жол беретін атрибутта енгізілген синтаксисті сәйкестендіретін объекті идентификаторын (ОИ) көрсетеді. privilegeId деп белігенген синтаксис rbacId деп белгіленгенмен бірігуге тиіс;

д) securityClassifications – жол беретін атрибут жіктеуге құпиялық белгілерді жіктеуді түрлендіреді, сондай-ақ суреттеу эквиваленттілігін қамтамасыз етеді;

е) rbacId – қауіпсіздік саясатының ақпараттық файлымен қосылып пайдаланылатын securityLabel қауіпсіздік санатына енгізілген синтаксисті сәйкестендіретін қол жеткізуді басқару объектісінің идентификаторына негізделген ереже. rbacId деп белгіленген

синтаксис privilegeId деп белгіленгенмен бірігуі тиіс;

ж) securityCategories – жол беретін атрибутта жіктеуге құпиялық белгілерді жіктеуді түрлендіреді, сондай-ақ суреттеу эквиваленттілігін қамтамасыз етеді

и) equivalentPolicies – ҚСАФ-нда барлық эквивалентті саясаттарды біріктіреді;

к) defaultSecurityPolicyIdData – егер деректер құпиялық белгілерінсіз алынатын болса, қолданылатын қауіпсіздік саясатын сәйкестендіреді;

л) extensions – кейіннен сәйкестендірілетін талаптар ретінде қосымша мүмкіндіктерді енгізу тетігін қамтамасыз етеді.

Қауіпсіздік саясатының ақпараттық файлы санкцияланбаған өзгерістерден қорғау мақсатында қол қойылған объекті болып табылады.

4.2.2 ASN.1 тілінің спецификациясы. Қауіпсіздік саясатының ақпараттық файлы

Қауіпсіздік саясатының ақпараттық файлы 5-суретте көрсетілген мынадай синтаксиспен анықталған.

```
SecurityPolicyInformationFile ::= SIGNED {EncodedSPIF}

EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )

SPIF ::= SEQUENCE    {
    versionInformation                      VersionInformationData DEFAULT v1,
    updateInformation                       UpdateInformationData,
    securityPolicyIdData                    ObjectIdData,
    privilegeId                             OBJECT IDENTIFIER,
    rbacId                                  OBJECT IDENTIFIER,
    securityClassifications         [0]     SEQUENCE OF SecurityClassification OPTIONAL,
    securityCategories              [1]     SEQUENCE OF SecurityCategory OPTIONAL,
    equivalentPolicies              [2]     SEQUENCE OF EquivalentPolicy OPTIONAL,
    defaultSecurityPolicyIdData     [3]     ObjectIdData OPTIONAL,
    extensions                      [4]     Extensions OPTIONAL }
```

5-сурет

4.2.2.1 Нұсқау туралы ақпарат

versionInformation өрісі ASN.1 тілі синтаксисінің нұсқасын, сонымен бірге 6-суретте көрсетілген қоса жүретін семантиканы көрсетеді.

```
VersionInformationData:: = INTEGER { v1(0) } (0..MAX)
```

6-сурет

4.2.2.2 Жаңарту туралы ақпарат

UpdateInformationData ҚСАФ-нда деректердің белгілі бір нұсқасына қатысы бар ақпараттың жалғасы болып табылады. sPIFVersionNumber ҚСАФ-нда сәйкестендірілген securityPolicyIdData қауіпсіздік саясаты үшін ҚСАФ ақпаратының әртүрлі нұсқалары арасында дифференцияланады. creationDate ҚСАФ қашан жүргізілгенін көрсетеді. originatorDistinguishedName ҚСАФ қол қойған адамды сәйкестендіреді. keyIdentifier **7-**суретте көрсетілгендей ҚСАФ қол қою үшін пайдаланылатын түйінді сәйкестендіреді.

```
UpdateInformationData ::= SEQUENCE                    {
    sPIFVersionNumber                                 INTEGER (0..MAX),
    creationDate                                      GeneralizedTime,
    originatorDistinguishedName                       Name,
    keyIdentifier                                     OCTET STRING OPTIONAL }
```

7-сурет

4.2.2.3 ID деректері қауіпсіздігінің саясаты

SecurityPolicyIdData ҚСАФ-да қолданылатын қауіпсіздік саясатын сәйкестендіреді. securityPolicyIdData кейіннен objectId и objectIdName болып табылатын ObjectIdData ретінде анықталған. objectId белгілі бір объект тағайындаған объект идентификаторы (ОИ) болып табылады және objectIdName ретінде 8-суретте көрсетілгендей сәйкестендірілетін белгілі бір объект болып табылады.

```
ObjectIdData ::= SEQUENCE {
    objectId                                          OBJECT IDENTIFIER,
    objectIdName                                      ObjectIdName }
ObjectIdName ::= DirectoryString {ubObjectIdNameLength}
```

8-сурет

4.2.2.4 Артықшылық идентификаторы

privilegeId объектісінің идентификаторы ҚСАФ-да бірігуінде пайдаланылатын жол беретін атрибуттың сенімді сертификаттарының қауіпсіздігі санатына енгізілген синтаксисті сәйкестендіреді.

4.2.2.5 Қол жеткізуді басқарудың базалық ережесінің идентификаторы

rbacId объектісінің идентификаторы ҚСАФ-да бірігуінде пайдаланылатын жол беретін securityLabel қауіпсіздігі санатына енгізілген синтаксисті сәйкестендіреді. rbacId деп белгіленген синтаксис privilegeId деп белгіленгенмен сыйымды болуы тиіс.

4.2.2.6 Қауіпсіздікті жіктеу

SecurityClassification жалғасу securityPolicyIdData-да сәйкетендірілген қауіпсіздік саясаты үшін анықталған қауіпсіздікті жіктеудің әр бір мәні үшін ҚСАФ-да болады. Бұл - қосымша элемент.

labelAndCertValue құпиялық белгіде осы жіктеуге арналған мән және биттің орналасқан жерін classList BIT STRING жол беретін атрибутта қауіпсіздіктің осы жіктеуін көрсететін мақсатты санның мәні.

classificationName құпиялық белгілерде жіктеу мәнін таңдайтын немесе қарайтын тұтынушыға көрсететін мәтінді анықтау үшін қосымшаны пайдаланатын осы жіктеуге сәйкестендірілген жол болып табылады.

equivalentClassifications SecurityClassification labelAndCertValue-ға эквивалентті жіктеулер мәндерінің жалғасы болып табылады (securityPolicyIdData басқа қауіпсіздік саясатында анықталған).

hierarchyValue «securitypolicyIdData» деп белгіленген қауіпсіздік саясатында қауіпсіздік жіктеулерінің баспалдағындағы SecurityClassification labelAndCertValue салыстырмалы жағдайын көрсетеді. hierarchyValue қауіпсіздік саясаты шегінде маңызды

болуға тиіс.

markingData деректер объектісіне қоса берілген таңбалау ақпаратын сәйкестендіреді.

markingData жол негізінен қайда көрсетілгенін сәйкестендіретін жолдан және код таңбасынан жасалған. Егер markingPhrase болмаса, онда markingCode, SecurityClassification classificationName жатқызылады.

Қауіпсіздік санаты немесе қауіпсіздік жіктеуі құпиялық белгілеріне енгізу үшін таңдап алынса, егер қоса жүретін ҚСАФ requiredCategory саласы ұсынылса, таңдап алынған мәнмен біріктіруде құпиялық белгілеріне енгізілуге тиісті қауіпсіздік санатын көрсетеді. Егер requiredCategory саласы болмаса, онда таңдап алынған мән қауіпсіздіктің кез келген санына ешбір байланысы жоқ.

Егер OptionalCategoryGroup операциясы onlyOne болып табылса, онда categoryGroup-ға енгізілген қауіпсіздіктің бір (тек бір) санаты құпиялық белгісіне енгізілуге тиіс. Егер OptionalCategoryGroup операциясы onlyOne болып табылса, онда categoryGroup-ға енгізілген қауіпсіздіктің бір немесе одан да астам санаты құпиялық белгісіне енгізілуі тиіс. Егер OptionalCategoryGroup операциясы барлығына бірдей болса, онда categoryGroup-ға енгізілген қауіпсіздіктің барлық санаты құпиялық белгісіне енгізілуге тиіс.

Тұтынушы әрбір мәнді таңдауға тиіс. Егер OptionalCategoryGroups көбейткіші requiredCategories-нде бар болса, онда барлық OptionalCategoryGroups-мен сипатталған талап қанағаттануы тиіс. categoryGroupтің жалғасы OptionalCategoryData болып табылады. optCatDataId объектінің идентификаторы rbacId, privilegeId және SPIF SecurityCategory объектісінің идентификаторларының белгілі бір типімен бірігетін categorydata саласының OptionalCategoryData-нда пайдалану үшін синтаксисті анықтауға тиіс.

Obsolete құрауышы TRUE мәнінде белгіленгенде нақты жіктеулер ескірген болып табылатынын көрсетеді. Мұндай жіктеу деректердің ескі объектілерімен байланысты болуы мүмкін, бірақ ол 9-суретте көрсетілгендей жаңамен байланысты болмауға тиіс.

```
SecurityClassification ::= SEQUENCE   {

      labelAndCertValue
      classificationName
      equivalentClassifications [0]      EquivalentClassifications OPTIONAL,
      hierarchyValue                     INTEGER,
      markingData               [1]      MarkingDataInfo OPTIONAL,
      requiredCategory          [2]      OptionalCategoryGroups OPTIONAL,
      obsolete                           BOOLEAN DEFAULT FALSE      }

LabelAndCertValue ::= INTEGER (0..MAX)
ClassificationName ::= DirectoryString { ubClassificationNameLength }
EquivalentClassifications ::= SEQUENCE SIZE(0..MAX) OF EquivalentClassification

EquivalentClassification ::=          SEQUENCE {
        securityPolicyId              OBJECT IDENTIFIER,
        labelAndCertValue             LabelAndCertValue,
        applied Applied }
Applied ::= INTEGER {
    encrypt (0),
    decrypt (1),
    both    (2) }
(encrypt | decrypt | both)

MarkingDataInfo ::= SEQUENCE SIZE(1..MAX) OF MarkingData
MarkingData ::= SEQUENCE {
    markingPhrase                 MarkingPhrase OPTIONAL,
    markingCodes                  MarkingCodes OPTIONAL }
(ALL EXCEPT ({-- none; at least one component shall be present --}))

MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }
```

```
MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

MarkingCode ::= INTEGER {
        pageTop             (1),
        pageBottom          (2),
        pageTopBottom       (3),
        documentEnd         (4),
        noNameDisplay       (5),
        noMarkingDisplay    (6),
        unused              (7),
        documentStart       (8),
        suppressClassName   (9)   }
OptionalCategoryGroups ::=SEQUENCE SIZE(1..MAX)

OptionalCategoryGroup ::=SEQUENCE {
        operation           Operation,
        categoryGroup       CategoryGroup }
Operation ::= INTEGER {
         onlyOne            (1),
         oneOrMore          (2),
         all                (3)}
  (onlyOne | oneOrMore | all)
CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData
OptionalCategoryData ::= SEQUENCE {
        optCatDataId        OC-DATA.&id({CatData}),
        categorydata        OC-DATA.&Type({CatData}{@optCatDataId }) }
OC-DATA ::= TYPE-IDENTIFIER
CatData OC-DATA ::= { … }
```

9-сурет

4.2.2.7 Қауіпсіздік санаты

SecurityCategory жалғасу securityPolicyIdData-да сәйкестендірілген қауіпсіздік саясаты үшін анықталған қауіпсіздікті жіктеудің әр бір мәні үшін ҚСАФ-да болады. SecurityCategory синтаксисі осы 5.1-де құпиялық белгіде анықталған. privilegeId, rbacId және optCatDataID объектісінің идентификаторы белгілеген синтаксиспен байланысты болуға тиіс, SecurityCategory типіндегі объектінің идентификаторы белгілеген SecurityCategory мәні саласында пайдалануы үшін синтаксис анықталған.

4.2.2.8 Эквивалентті саясат

equivalentPolicies эквивалентті мән ретінде ҚСАФ-да енгізілген мән үшін қауіпсіздіктің барлық саясатының тізбесі болып табылады. securityPolicyId қауіпсіздіктің эквивалентті саясатын сәйкестендіретін объектінің идентификаторы болып табылады. securityPolicyName 10-суретте көрсетілгендей қауіпсіздіктің эквивалентті саясатының қосымша директивті жолы, сәйкестендіруші атауы болып табылады.

```
EquivalentPolicy ::= SEQUENCE {
        securityPolicyId                    OBJECT IDENTIFIER,
        securityPolicyName                  SecurityPolicyName OPTIONAL}

SecurityPolicyName ::= DirectoryString {ubObjectIdNameLength}
```

10-сурет

4.2.2.9 Өкілеттілік бойынша берілген қауіпсіздік саясатының идентификаторы

defaultSecurityPolicyIdDat үшін мән қол жеткізуді басқару функциясын қолдамайтын қосымшалармен өзара іс-әрекеттің мүмкіндігін қолдайды. Объектінің осы идентификаторына құпиялықтың ешбір белгісі пайдаланылмағанда сілтеме жасалады.

Өкілеттілік бойынша қауіпсіздік саясаты жіктеудің қарапайым деңгейіне ие болатынын ескеру қажет. Қорғаныш санатының мәні өкілдік берген қауіпсіздік саясатына алмасатын болса, онда белгіленген мән үшін ҚСАФ SEQUENCE SecurityClassification өкілдік берілген қауіпсіздік саясаты объектісінің policyId идентификаторына орнатылған SEQUENCE equivalentClassification қамтитын болады.

4.2.2.10 Кеңейту

Extension өрісі алдыңғы іске асырылған ҚСАФ-ның өзара әрекеті мүмкіндігін қолдай отырып, қосымша талаптардың сәйкестігіне байланысты ҚСАФ-ын алдағы уақытта кеңейтуге мүмкіндік беретін ақпараттың жалғасы болып табылады. Ол extnId, critical және extnValue құрауыштарынан тұрады. Синтаксис енгізілген [5].

Кеңейту сындарлы немесе сындарлы емес деп белгіленуі мүмкін. ҚСАФ-нда пайдаланылатын жүйе, егер ол сындарлы кеңейтумен байланысқан болса және оны танымаса; бірақ сындарлы емес кеңейтуге қарсылық болса, егер ол танылмаса, ҚСАФ-ның жұмысы тоқтатылуға тиіс. Ескерту сигналы 11-суретте көрсетілгендей пайдаланылуы негізгі контексте болдырмауы мүмкін кез келген сындарлы кеңейтулерді беруі мүмкін.

```
Extensions ::= SEQUENCE OF Extension

Extension ::= SEQUENCE {
        extnId                              EXTENSION.&id ({ExtensionSet}),
        critical                            BOOLEAN DEFAULT FALSE,
        extnValue                           OCTET STRING

                        -- contains a DER encoding of a value of type &ExtnType
                        -- for the extension object identified by extnId -- }
ExtensionSet EXTENSION ::= { … }

EXTENSION ::= CLASS {
      &id                                   OBJECT IDENTIFIER UNIQUE,
      &ExtnType }
WITH SYNTAX { SYNTAX &ExtnType IDENTIFIED BY &id }
```

11-сурет

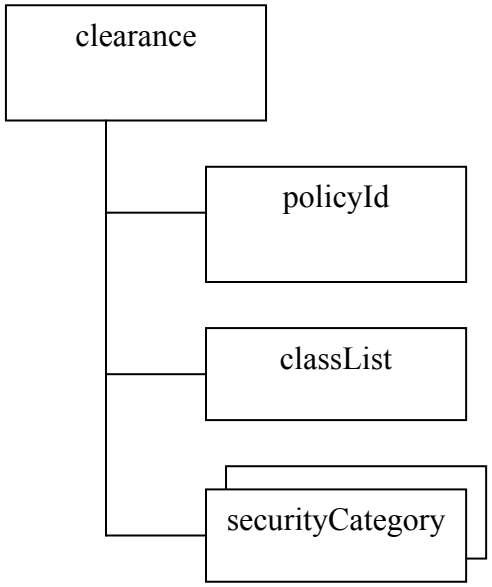
4.3 Жол беретін атрибут

4.3.1 Кіріспе

Жол беретін атрибут белгілі бір тұтынушыға немесе қолданбалы құрауышқа берілген өкілеттілікті анықтау үшін пайдаланылады. Тұтынушыға немесе қолданбалы құрауышқа берілген өкілеттілік ұйым көптеген салалы қауіпсіздік саясаты (немесе саясаттары) болуы мүмкін. Өкілеттілік қауіпсіздікті қамтамасыз ету саясатын қамтуы мүмкін.

Жол беретін атрибут үш құрауыштан тұрады: 12-суретте көрсетілгендей policyId, classList, және қосымша securityCategory.

policyId объектісінің идентификаторы қандай қосымша құрауыштар болуы қажеттігін анықтайды. classList құрауышы [6] анықталған classList-ға сәйкес тұтынушылардың ұсынылған және сатыланған қол жеткізу рұқсатын анықтайды. Класстардың басқа да сатыланған тізімдері басқа ҚАО-не енгізу үшін басқа жерде анықталған немесе қауіпсіздіктің санатына арналған. securityCategory құрауышы белгіленген тұтынушыға биттарда шектейтін және рұқсат ететін санамаланған санаттар да қауіпсіздіктің шектеу және рұқсат ету санаттарының кез келген санын сәйкестендіреді. Осы құрылым 13-суретте келтірілген.



T0733160/d01

12-сурет – Жол беретін атрибуттың құрылымы

T0733170/d02

рұқсат

жалғасы

Policyld	classList	securityCategory (optional)
Қауіпсіздік саясатын анықтайтын объектінің идентификаторы	белгіленбеген (0) жіктелмеген (1) шектелген (2) құпия (3) жасырын (4) айтарлықтай жасырын (5)	Қол жеткізу деңгейі іс-әрекет аймағы бойынша анықталады: -толық қол жеткізу (тек бір адам) -шектелген қол жеткізу (барлық тұтынушылар) -нөмірленген қол жеткізу (мысалы, мемлекеттік қол жеткізу)

13-сурет – Жол беретін атрибут саласы

4.3.2 Жол беретін атрибутты анықтау

Жол беретін атрибут 14-суретте көрсетілгендей анықталады.

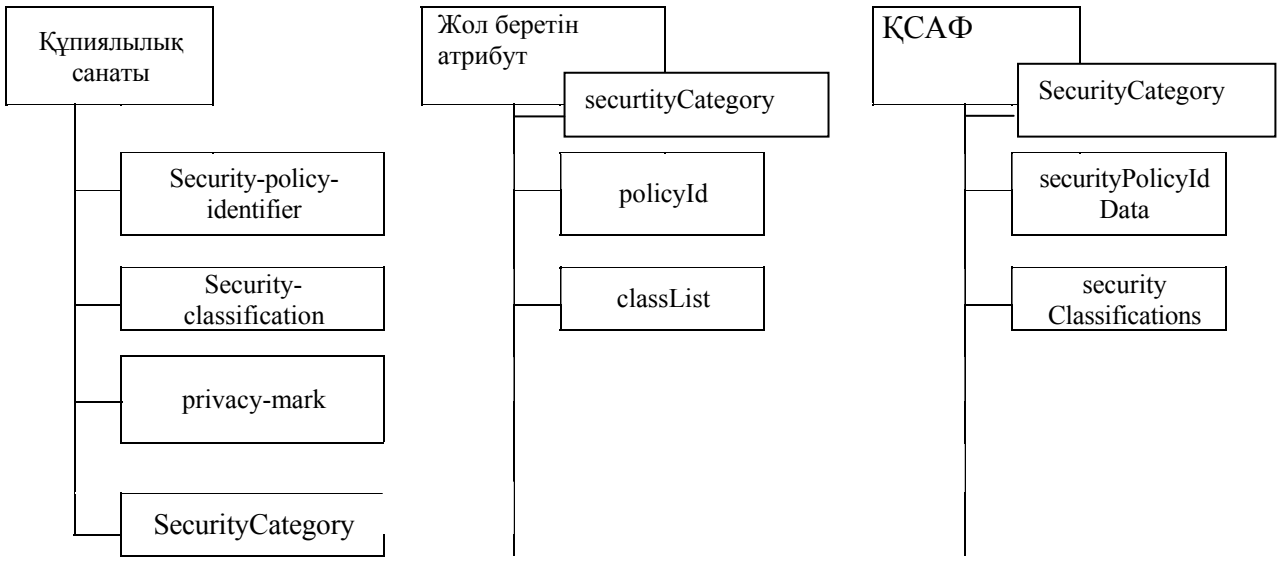
```
clearance ATTRIBUTE ::= { WITH SYNTAX Clearance
        ID                                              id-at-clearance }

id-at-clearance OBJECT IDENTIFIER ::= {
        joint-iso-itu (2) ds (5) attributeType (4) clearance (55) }

Clearance ::= SEQUENCE {
        policyId                                        OBJECT IDENTIFIER,
        classList                                       ClassList       DEFAULT
                                                        {unclassified},
        securityCategories                              SecurityCategories OPTIONAL}

ClassList ::= BIT STRING {
        unmarked                                        (0),
        unclassified                                    (1),
        restricted                                      (2),
        confidential                                    (3),
        secret                                          (4),
        topSecret                                       (5)     }

SecurityCategories ::= SET SIZE(1..MAX) OF SecurityCategory
    -- SecurityCategory is defined in the confidentiality label given in subclause 6.1.2
```

14-сурет

5 Ақпараттық қорғаныш объектісінің өзара әрекеті

5.1 АҚО класының құрылымын салыстыру

Салыстыру үшін 15-суретте ҚСАФ және [6] жол беретін атрибуттың құпиялық белгілерінің құрылымы көрсетілген. Осы құрылымдардағы тең мәнді құрауыштар белгілі бір функционалдық мүмкіндіктерге қол жеткізу үшін қолданбалы бағдарламалық қамтамасыз ету зерттелуі мүмкін. Осы үш құрылымды пайдалану арқылы қол жеткізуді басқарудың функционалдық мүмкіндіктеріне қол жеткізу 5.2 тармағында талқыланған.

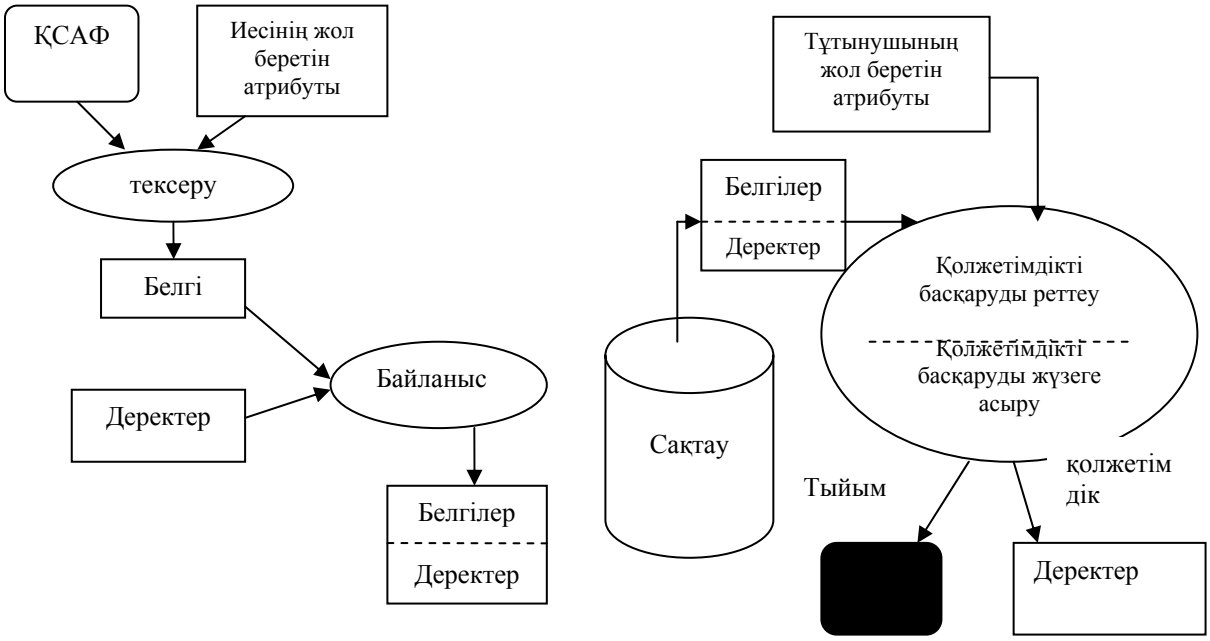


15-сурет – Объектілердің тең мәнді кластарын салыстыру

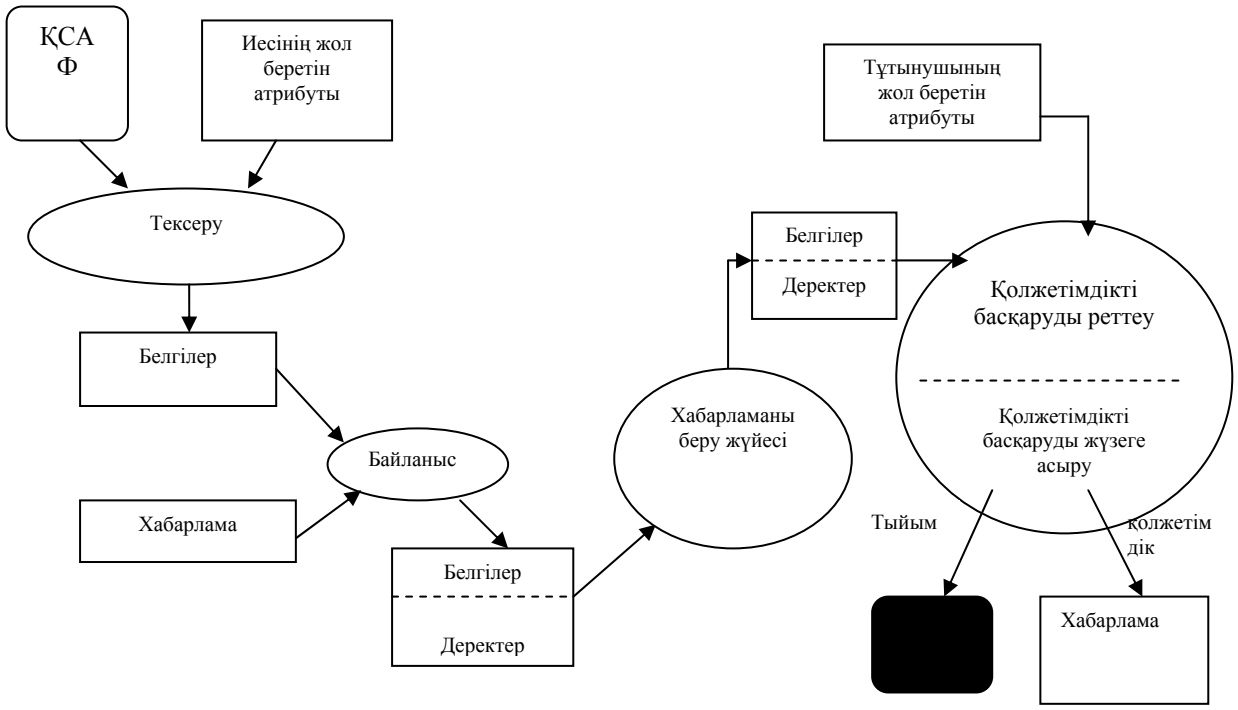
5.2 Қол жеткізуді басқару бойынша ақпараттық қорғау объектілерінің өзара әрекеті

Қол жеткізуді басқару құпиялық белгілердің мәні арқылы мақсатты объектілерге тағайындалатын өзгерістерді және жол беретін атрибутты пайдалану көмегімен бастамашылар немесе тұтынушылар үшін өкілеттілікті беру тұжырымдамасын қамтиды. ҚСАФ олардың өкілеттілігін және өзгертілетін параметрлерді талдау үшін пайдаланылады. Қолданбалы бағдарламалық қамтамасыз ету мақсаттарға өзгерістер қабылдау, белгілердегі өзгерістерді есептеу, сертификаттардағы өкілеттіліктерді есептеу және растау және қауіпсіздік саясатының әрекет аймағы үшін ұғымдық кескіндерді анықтау үшін ҚСАФ пайдаланылады.

Пайдаланылатын тетіктер жіктеу және санат ретінде ақпарат құпиялығын және өкілеттілікті береді. Жол беретін атрибутта бекітілген жіктеу және санат тұтынушы сертификатына салынады, содан соң осы тұтынушыға өкілеттілік беріледі. Объектінің құпиялық белгісінде бекітілген жіктеу және санат осы объектінің өзгерісін беруге қызмет етеді. Объектіге рұқсат тұтынушының жол беретін атрибутта берілген өкілеттілікке рұқсат етілгенде мақсат объектісінің құпиялық белгісіне берілген өзгерістермен салыстырғанда айтарлықтай негізделген. 16-сурет деректерді сақтау ортасында қол жеткізуді басқаруды қамтамасыз ететін осында анықталған АҚО арасындағы өзара әрекетті көрсетеді. Деректердің тиісті иесіне сертификатта қамтылған деректер иесінің жол беретін атрибуттағы өкілеттілік ҚСАФ-дан қандай өкілеттілік шектейтінін мақсат деректеріне арналған белгіде бекітуі мүмкін. Белгілер деректермен байланыстырылады және сақтау орнына орналастырылады. Деректерге қол жеткізу кезінде тиісті тұтынушыға сертификатта қамтылған тұтынушының жол беретін атрибуты қол жеткізуді басқаруды реттеу функциясында мақсат деректерімен байланысты белгілермен салыстырылады. Егер рұқсат етілген өзгерістер құпиялық белгісінде болса, жоқ дегенде олар құпиялық белгісінде әрбір рұқсат етілген тегада ұсынылған өзгерістердің бірі қол жеткізуді басқаруды жүзеге асыру функциясы арқылы мақсат деректерінің объектісіне қол жеткізуге рұқсат ете отырып, сертификатта да (рұқсат етілген өкілеттілік) рұқсат етуге кепілдік беру үшін тексеріледі. Хабарламалармен алмасу ортасы үшін қол жеткізуді басқарудың ұқсас сценарийі 17-суретте көрсетілген.



16-сурет – Сақтау жүйесіне қол жеткізуді басқару



17-сурет – Хабарламамен алмасуға қол жеткізуді басқару сценарийі

А қосымшасы
(ақпараттық)

ASN.1 тілде қол жеткізуді басқару бойынша ақпараттық қорғау объектілері

Осы қосымша ASN.1 тіл модуль түрінде осы стандарттағы ASN.1 тіл ақпараттық объекті класының барлық типтерді, мәндерді және анықтамаларды қамтиды.

```
SIOsAccessControl-MODULE  {

     joint-sio-itu sios(24) specification(0) modules(0) accessControl(0)
}

   DEFINITIONS IMPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

IMPORTS


id-at-clearance

  FROM EnhancedSecurity          -- ITU Rec. X.501 | ISO/IEC 9594-2 –-

ATTRIBUTE, Name

  FROM InformationFramework    -- ITU Rec. X.501 | ISO/IEC 9594-2 –-

Extensions

  FROM CertificateExtensions        -- ITU Rec. X.509 | ISO/IEC 9594-8 --


DirectoryString {}

  FROM SelectedAttributeTypes;    -- ITU Rec. X.520 | ISO/IEC 9594-6 --


id-ConfidentialityLabel OBJECT IDENTIFIER  ::=  {joint-iso-itu -t spec(24) specification(0)
securityLabels(1) confidentiality(0)}


ConfidentialityLabel  ::=  SET {

  security-policy-identifier  SecurityPolicyIdentifier OPTIONAL,

       security-classification  INTEGER(0..MAX)  OPTIONAL,

       privacy-mark                              PrivacyMark  OPTIONAL,

       security-categories                       SecurityCategories  OPTIONAL

}
(ALL EXCEPT ({-- none; at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER
PrivacyMark ::= CHOICE {

       pString     PrintableString (SIZE(1..ub-privacy-mark-length)),

       utf8String  UTF8String (SIZE(1..ub-privacy-mark-length))
}
```

```
    ub-privacy-mark-length INTEGER :: = 128 -- as defined in X.411

SecurityCategories ::= SET SIZE(1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
  type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
  value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                                        {SecurityCategoriesTable}{@type})
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= {
        ... -- objects defined as needed --
}
SecurityPolicyInformationFile ::= SIGNED { EncodedSPIF }

-- Type EncodedSPIF is an open type constrained to be a value
-- of type SPIF. This open type representation is an opaque
-- string of hexadecimal characters suitable for signature
-- and signature verification operations.

EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )

SPIF ::= SEQUENCE {
      versionInformation              VersionInformationData  DEFAULT v1,
      updateInformation               UpdateInformationData,
      securityPolicyIdData            ObjectIdData,
      privilegeId                     OBJECT IDENTIFIER,
      rbacId                          OBJECT IDENTIFIER,
      securityClassifications         [0] SecurityClassifications  OPTIONAL,
      securityCategories              [1] SPIF-SecurityCategories  OPTIONAL,
      equivalentPolicies                [2] EquivalentPolicies OPTIONAL,
      defaultSecurityPolicyIdData  [3] ObjectIdData OPTIONAL,
      extenisons                          [4] Extensions OPTIONAL
}
      VerisonInformationData ::= INTEGER { v1(0) } (0..MAX)
      UpdateInformationData ::= SEQUENCE {
          sPIFVerisonNumber          SPIFVersionNumber,
              creationDate                GeneralizedTime,
```

```
        originatorDistinguishedName  Name,
        keyIdentifier                OCTET STRING  OPTIONAL
}
SPIFVerisonNumber ::=  INTEGER (0..MAX)

ObjectIdData ::= SEQUENCE {
      objectId          OBJECT IDENTIFIER,
      objectIdName  ObjectIdName
}
ObjectIdName ::= DirectoryString { ubObjectIdNameLength }
SecurityClassifications ::=
      SEQUENCE SIZE(0..MAX) OF SecurityClassification
SPIF-SecurityCategories ::=
      SEQUENCE SIZE(0..MAX) OF SecurityCategory
EquivalentPolicies ::=
      SEQUENCE SIZE(0..MAX) OF EquivalentPolicy
SecurityClassification ::= SEQUENCE {
        labelAndCertValue          LabelAndCertValue,
        classificationName         ClassificationName,
        equivalentClassifications  [0] EquivalentClassifications  OPTIONAL,
        hierarchyValue             INTEGER,
        markingData                [1] MarkingDataInfo  OPTIONAL,
        requiredCategory           [2] OptionalCategoryGroups  OPTIONAL,
        obsolete                   BOOLEAN  DEFAULT FALSE
      }
      LabelAndCertValue ::= INTEGER(0..MAX)

      ClassificationName ::= DirectoryString { ubClassificationNameLength }

      EquivalentClassifications ::=
        SEQUENCE SIZE(0..MAX) OF EquivalentClassification
      EquivalentClassification ::= SEQUENCE {
        securityPolicyId   OBJECT IDENTIFIER,
        labelAndCertValue  LabelAndCertValue,
        applied                    Applied
      }
```

```
        Applied ::= INTEGER {
          encrypt (0),
          decrypt (1),
          both     (2)
    }
      (encrypt | decrypt | both)
        MarkingDataInfo ::= SEQUENCE SIZE (1..MAX) OF MarkingData

         MarkingData ::= SEQUENCE {
         markingPhrase  MarkingPhrase  OPTIONAL,
         markingCodes   MarkingCodes   OPTIONAL
     }
       (ALL EXCEPT({-- none; at least one component shall be present --}))

    MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }

    MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

    MarkingCode ::= INTEGER {
        pageTop              (1),
        pageBottom           (2),
        pageTopBottom        (3),
        documentEnd          (4),
        noNameDisplay        (5),
        noMarkingDisplay     (6),
        unused               (7),
       documentStart         (8),
       suppressClassName     (9)
    }
     OptionalCategoryGroups ::=
        SEQUENCE SIZE(1..MAX) OF OptionalCategoryGroup
    OptionalCategoryGroup ::= SEQUENCE {
        operation          Operation,
       categoryGroup  CategoryGroup

  }
  Operation ::= INTEGER {
```

```
        onlyOne          (1),
        oneOrMore     (2),
        all                 (3)
}
     (onlyOne | oneOrMore | all)
  CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData

  OptionalCategoryData ::= SEQUENCE {

        optCatDataId  OC-DATA.&id({CatData}),
        categorydata   OC-DATA.&Type({CatData}{@optCatDataId })
}

OC-DATA ::= TYPE-IDENTIFIER

CatData OC-DATA ::= {
      ... -- defined as needed –
}
EquivalentPolicy ::= SEQUENCE {
        securityPolicyId       OBJECT IDENTIFIER,
        securityPolicyName  SecurityPolicyName  OPTIONAL
}

SecurityPolicyName ::= DirectoryString { ubObjectIdNameLength }

clearance ATTRIBUTE ::= {
  WITH SYNTAX  Clearance
  ID                        id-at-clearance
}
Clearance ::= SEQUENCE {   -- Automatic tags applied
     policyId                          [0] OBJECT IDENTIFIER,
     classList                         [1] ClassList  DEFAULT { unclassified },
     securityCategories                [2] SecurityCategories  OPTIONAL
}

  ClassList ::= BIT STRING {
         unmarked       (0),
```

```
        unclassified     (1),
        restricted       (2),
        confidential     (3),
        secret           (4),
        topSecret        (5)
}
-- upper bound values

ubObjectIdNameLength            INTEGER ::= 256
ubClassificationNameLength      INTEGER ::= 256
ubMarkingPhraseLength           INTEGER ::= 256
-- information object classes --
ALGORITHM ::= CLASS {
        &id     OBJECT IDENTIFIER  UNIQUE,
      &Type  OPTIONAL
}
        WITH SYNTAX { OID &id [PARMS &Type] }

        - parameterized types –

SIGNED { ToBeSigned } ::= SEQUENCE {
        toBeSigned  ToBeSigned,
        algorithm     AlgorithmIdentifier{{SignatureAlgorithms}},
        signature      BIT STRING
}

AlgorithmIdentifier { ALGORITHM:IOSet } ::= SEQUENCE {
  algorithm    ALGORITHM.&id({IOSet}),
  parameters  ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}
SignatureAlgorithms ALGORITHM ::= {
   ... -- defined as needed --}
END  -- SecurityInformationObjects --
```

Б қосымшасы
(ақпараттық)

SECURITY-CATEGORY синтаксисін кеңейту

SECURITY-CATEGORY ақпараттық объекті класы Б.1 суретінде көрсетілгендей TYPE-IDENTIFIER жапсарлы класы ретінде анықталған.

```
SECURITY-CATEGORY ::= TYPE-IDENTIFIER
```

Б.1 суреті

Ақпараттық объектінің осы қолданылған класы Б.2 суретінде көрсетілгендей А қосымшасында [2] анықталған.

```
TYPE-IDENTIFIER ::= CLASS {
   &id   OBJECT IDENTIFIER UNIQUE,
  &Type
}
   WITH SYNTAX { &Type IDENTIFIED BY &id }
```

Б.2 суреті

SECURITY-CATEGORY класында &id және &Type деп аталған екі сызық бар. &id сызығы OBJECT IDENTIFER типіндегі мән болу үшін, ал &Type сызығы ашық типтегі мән болуы үшін анықталған. Ашық тип ASN.1.тілінің кез келген типі болуы мүмкін.

Осы кластың объектісі ақпараттық объекті тобының мүшесі ретінде пайдаланылса, &id сызығының анықтамасы топтағы әрбір объект объекті идентификаторының маңызды мәнін қамтуын талап етеді.

Класты анықтау SECURITY-CATEGORY класының ақпараттық объектілерін анықтау үшін пайдаланылуы мүмкін қосымшаны анықтайтын WITH SYNTAX бекітуді қамтиды.

SecurityCategoriesTable – SECURITY-CATEGORY класының ақпараттық объект тобы. Ол Б.3-суретте көрсетілгендей анықталады.

```
SecurityCategoriesTable SECURITY-CATEGORY ::= {
... -- objects defined as needed --
}
```

Б.3 суреті

SecurityCategoriesTable жиынтығы "...", кеңейту маркерін қамтиды, бірақ бір де бір ақпараттық объектіні қамтымайды.

SECURITY-CATEGORY класының объектісі классты анықтауда ұсынылған WITH SYNTAX деп белгіленген жүйені пайдалана отырып, жеке берілуі мүмкін.

Келесі мысалға алынған объекті ASN.1 тілдің кез келген типі, ол қарапайым немесе күрделі ме Б 4 суретінде көрсетілгендей ақпараттық объектіні құру үшін пайдаланылуы мүмкін.

```
                    -- Type 2 - hierarchical attributes

                    enumeratedAttributes SECURITY-CATEGORY ::= {

                            AttributeList IDENTIFIED BY id-enumeratedAttributes
        }

                    AttributeList ::= SET SIZE(1..MAX) OF LabelAttribute

                    -- Type 5 - all attributes in the range(s)

                    rangeSet SECURITY-CATEGORY ::= {
                            RangeList IDENTIFIED BY id-rangeSet
        }

                    RangeList ::= SET SIZE(1..MAX) OF LabelAttributeRange

                    -- Type 6 - release attributes

                    permissiveBitMap SECURITY-CATEGORY ::= {
                       PermissiveBitMap IDENTIFIED BY id-permissiveBitMap
                    }
                    PermissiveBitMap ::= BIT STRING

                    -- Type 7 – for markings with no formal access control –

                    freeFormField SECURITY-CATEGORY ::= {
                            FreeFormField IDENTIFIED BY id-freeFormField
        }
                    FreeFormField ::= SEQUENCE {
                        name   SECURITY-CATEGORY.&id({Fields}),
                           field    SECURITY-CATEGORY.&Type({Fields}{@name})
        }

                    Fields SECURITY-CATEGORY ::= {
                        ... -- defined as needed --
        }
```

Б.4 суреті

Мұнда объектілердің &Type сызығы AttributeFlags, AttributeList, RangeList, PermissiveBitMap және FreeFormField деп аталатын ASN.1 тіл типінен тұрады. &id сызығы id-restrictiveBitMap, id-enumeratedAttributes, id-rangeSet, id-permissiveBitMap және id-freeFormField деп аталатын объектінің идентификаторының маңызды мәнін қамтиды.

Осы объектілер Б.5 суретінде көрсетілгендей объектілерді біріктіруден қауіпсіздік санатының жиынын құрастыру үшін объектінің SecurityCategoriesTable атауымен орындау нұсқасына қосымша берілуі мүмкін.

```
                SecurityCategoriesTable SECURITY-CATEGORY ::= {
                    restrictiveBitMap |
                    enumeratedAttributes  |
                    rangeSet     |
                    permissiveBitMap
                    freeFormField,
                            ... -- expect other objects --
        }
```

Б.5 суреті

Объектінің баламасы, анықтамасы ретінде Б.6 суретінде көрсетілгендей SecurityCategoriesTable объектісінің ақпарат жиынына тікелей қосымша берілуі мүмкін.

```
SecurityCategoriesTable          SECURITY-CATEGORY          ::=          {
   --
   --                                                                    &Type

&id
            --
            {AttributeFlags  IDENTIFIED BY id-restrictiveBitMap } |
            {AttributeList   IDENTIFIED BY id-enumeratedAttributes}|
            {RangeList       IDENTIFIED BY id-rangeSet                  } |
            {PermissiveBitMapIDENTIFIED BY id-permissiveBitMap } |
            {FreeFormField   IDENTIFIED BY id-freeFormField},
      ... -- expect other objects --   }
```

Б.6 суреті

Қауіпсіздіктің санаты тобының осы түрі төрт қатарының кестесін көрсетеді, әрқайсысы екі бағаннан, бір баған &id үшін екінші баған &Type үшін.

SecurityCategory типі тип және мән деп аталатын екі құрауыштың жалғасы ретінде анықталады.

```
SecurityCategory ::= SEQUENCE {
                        type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
                        value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                                                    {SecurityCategoriesTable}{@type})
}
```

Б.7 суреті

Осы құрауыштардың әрқайсысы SECURITY-CATEGORY класының &id және &Type сызықтарының терминдерінде көрсетілген. Type құрауышы &id сызығының терминдерінде берілген және OBJECT IDENTIFIER типінің мәні болуға тиіс. Мән құрауышы &Type сызығымен берілген және ASN.1 тілінің кез келген типінің мәні болуы мүмкін.

SecurityCategoriesTable ақпараттық объектісінің жиыны type и value SecurityCategory құрауыштарының нақты мәніне арналған кестелерге шек қоймау үшін пайдаланылады. Кестеге шек қоймауда бірінде SECURITYCATEGORY класының әрбір сызығына арналған екі баған бар.

Type құрауышының &id сызығымен берілген объекті идентификаторының маңызды мәні кестенің қатарынан орын алады. @type белгісі таңдап алынған &id мәнімен байланысты &Type бағынын таңдайды. SecurityCategoriesTable жиынындағы кеңейту маркері қосымша жиында анықталғаннан басқа кез келген объектіні күтуі тиістігін көрсетеді.

Библиография

[1] МСЭ-Т Ұсыным X.680 (1997) МТС | ИСО/МЭК 8824-1:2002 Ақпараттық технология. 1 (ASN.1) нұсқасының астарлы синтаксисінің нотациясы. 1-бөлім. Базалық нотация спецификациясы.

[2] МСЭ-Т Ұсыным X.681 (1997) МТС | ИСО/МЭК 8824-2:2002 Ақпараттық технология. 1 (ASN.1) бір синтаксисінің нотациясы. 2-бөлім. Ақпараттық Объектілер спецификациясы.

[3] ИСО/МЭК 2382-8:1998 Ақпараттық технология. Сөздік. 8-бөлім. Құпия деректерді қорғау.

[4] ИСО/МЭК 7498-2:1989 Ақпаратты өңдеу жүйесі. Ашық жүйелердің өзара әрекеті. Базалық эталон моделі. 2-бөлім. Қорғау сәулеті.

[5] МСЭ-Т Ұсыным. X.509 (2000) МТС | ИСО/МЭК 9594-8:2005 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Директория. 8-бөлім. Жалпы түйіндігі және атрибуттарға арналған сертификаттың құрылымы.

[6] МСЭ-Т Ұсыным. X.501 (2001) МТС | ИСО/МЭК 9594-2:2005 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Директория. 2-бөлім. Модельдер.

[7] МСЭ-Т Ұсыным. X.411 (1999) МТС | ИСО/МЭК 10021-4:2003 Ақпараттық технология. Хабарламаларды өңдеу жүйесі (MHS). 4-бөлім. Астарлы сервистің анықтамалары мен рәсімдері.

[8] МСЭ-Т Ұсыным X.500 (2001) МТС | ИСО/МЭК 9594-1:2005 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Директория. 1-бөлім. Тұжырымдамаларға, модельдерге және қызметтерге шолу.

[9] МСЭ-Т Ұсыным. X.682 (1997) МТС | ИСО/МЭК 8824-3:2002 Ақпараттық технология. 1 (ASN.1) бір синтаксисінің нотациясы. 3-бөлім. Шектеу спецификациясы.

[10] МСЭ-Т Ұсыным. X.683 (1997) МТС | ИСО/МЭК 8824-4:1998 Ақпараттық технология – (ASN.1) нұсқасы деректерінің астарлы синтаксисі: ASN.1 спецификацияны параметризациялау.

[11] МСЭ-Т Ұсыным. X.690 (1997) МТС | ИСО/МЭК 8825-1:2002 Ақпараттық технология. ASN.1 Кодтау ережесі. 1-бөлім. Кодтаудың негізгі ережесінің (BER), кодтаудың канондық ережесінің (CER) және кодтаудың ерекшелік ережесінің (DER) спецификациясы.

[12] МСЭ-Т Ұсыным. X.722 (1992) МККТТ | ИСО/МЭК 10165-4:1992 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ақпаратты басқару жүйесі. 4-бөлім. Басқарылатын объектілерді анықтауға арналған басқаратын ереже.

[13] МСЭ-Т Ұсыным. X.741 (1995) МТС | ИСО/МЭК 10164-9:1995 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Жүйені басқару: 9-бөлім. Қол жеткізуді басқаруға арналған объектілер және атрибуттар.

14] МСЭ-Т Ұсыным. X.803 (1994) МТС | ИСО/МЭК 10745:1995 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Жоғары деңгейге арналған қауіпсіздік моделі.

[15] МСЭ-Т Ұсыным. X.810 (1995) МТС | ИСО/МЭК 10181-1:1996 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздіктің негізі. 1-бөлім. Шолу.

[16] МСЭ-Т Ұсыным. X.830 (1995) МТС | ИСО/МЭК 11586-1:1996 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Жоғары деңгейді жалпы қорғау. 1-бөлім. Шолу, модельдер және белгі жүйесі.

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: аралық бөлу, АҚО негізгі класы, ақпараттық объект, ақпараттық объекті класы, қауіпсіздік жөніндегі маман.

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ ЗАЩИТЫ
Объекты информационной защиты по управлению доступом

СТ РК ИСО/МЭК 15816-2009

ISO/IEC 15816:2002 Information technology. Security techniques.
Security information objects for access control, IDT

Издание официальное

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

Астана

Предисловие

1 ПОДГОТОВЛЕН И ВНЕСЕН Республиканским государственным предприятием «Казахстанский институт стандартизации и сертификации» и Техническим комитетом по стандартизации 63 «Системы, средства и услуги связи» (Товарищество с ограниченной ответственностью «Fidelis_2008»)

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 27 октября 2009 года № 534-од

3 Настоящий стандарт идентичен международному стандарту ISO/IEC 15816:2002 Information technology. Security techniques Security information Objects for access control (Информационная технология. Методы защиты. Объекты информационной защиты по управлению доступом).

Перевод с английского языка (en)
Степень соответствия - идентичная (IDT)

4 СРОК ПЕРВОЙ ПРОВЕРКИ **2014 год**
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ **5 лет**

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в Указателе "Нормативные документы по стандартизации", а текст изменений - в ежемесячных информационных указателях "Государственные стандарты". В случае пересмотра (отмены) или замены настоящего стандарта соответствующая информация будет опубликована в информационном указателе "Государственные стандарты"

Содержание

Введение

Настоящий стандарт по объектам информационной безопасности (ОИБ) по управлению доступом устанавливает определения объекта, потребность в которых возникает более чем в одном стандарте безопасности, чтобы избежать многократных и различных определений одной и той же функциональности. Точность данных определений достигнута при помощи языка ASN.1.

Цель управления безопасностью состоит в том, чтобы гарантировать, что имущество, включая информацию, защищены надлежащим образом и в рамках рентабельности. Чтобы защитить составляющие собственность интересы и права интеллектуальной собственности, организации должны управлять обработкой своей информации. Серьезный ущерб или затруднение могут быть причинены создателю или владельцу важной информации, например, если она попадет к лицам, не имеющим право на ее получение (нарушение конфиденциальности), или если она изменяется каким-либо образом (нарушение целостности). Каждой организации необходимо гарантировать, что она защищает свою собственную информацию и имущество должным образом во всех формах на время ее хранения, обработки и передачи между и внутри организации, по частным и общедоступным сетям. Организации должны быть уверены, что их имущество будет защищено должным образом, когда оно находится или обрабатывается другими лицами, когда деятельность осуществляется более распределено.

Мотивацией развития ОИБ по управлению доступом является достижение гибкости и способности к взаимодействию в управлении безопасностью, которое возникает от применения общих структур для сходных функций. Стандартизация категорий конфиденциальности и альтернативных методов по управлению доступом рассматривается в настоящем стандарте.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ ЗАЩИТЫ
Объекты информационной защиты по управлению доступом

Information technology. Security techniques.
Security information objects for access control

Дата введения 2010-07-01

1 Область применения

Настоящий стандарт применяется при:

а) закреплении руководящих принципов по определению теоретического синтаксиса общих и специфических объектов информационной защиты (далее - ОИБ) по управлению доступом;

б) детализации основ ОИБ по управлению доступом;

в) детализации специфичных особенностей ОИБ по управлению доступом.

Область применения данного стандарта охватывает только "статику" ОИБ через синтаксические определения описаний и дополнительных семантических пояснений в терминах языка ASN.1. Она не охватывает "динамику" ОИБ, как правила, касающиеся создания и удаления. Динамика ОИБ является проблемой локального выполнения.

2 Термины, определения и сокращения

В настоящем стандарте применяются термины по [1] , [2], [3], [4] , а также следующие термины с соответствующими определениями и сокращениями:

2.1 **Основной класс ОИБ** (generic SIO Class): Класс ОИБ, в котором полностью не определены типы данных для одного или более компонентов.

2.2 **Специалист по безопасности** (security authority): Лицо, ответственное за управление политикой безопасности в пределах зоны действия системы безопасности.

2.3 **Зона действия системы безопасности** (security domain): Совокупность пользователей и систем, относящихся к общей политике безопасности.

2.4 **Объект информационной безопасности** (security information object): Вариант класса ОИБ.

2.5 **Класс объекта информационной защиты** (security information object class): Класс информационного объекта, выполненный для безопасного использования.

2.6 **Информационный файл политики безопасности** (security policy information file): Концепция, которая передает специфическую для зоны действия системы безопасности информацию.

2.7 **Специфичный класс ОИБ** (specific SIO class): Класс ОИБ, в котором полностью определены типы данных для всех компонентов.

2.8 **Язык ASN.1** (abstract syntax notation one (ASN.1)): Язык для описания структур данных, служащих для кодирования, передачи и декодирования данных, используемых для взаимодействия открытых систем, представляет собой набор правил для описания структуры объектов, независимых от специфичных для оборудования методик кодирования, и формальную нотацию, которая позволяет избегать неоднозначностей.

Издание официальное

2.9. **БПУД - Базовые правила управления доступом** (rule based access control (RBAC)).

2.10. **МККТТ - Международный консультативный комитет по телеграфии и телефонии** (consultative Committee for International Telephone and Telegraphy (CCITT)).

3 Основные положения ОИБ

3.1 Описание класса ОИБ

Класс ОИБ включает:

– значение для идентификатора класса ОИБ;

– набор спецификаций одного и более типов данных, в каждом компоненте, содержащем класс ОИБ;

– изложение семантики, соответствующей используемому классу ОИБ.

3.2 Соответствие основному классу ОИБ

Основной класс ОИБ является классом ОИБ, в котором типы данных для одного или более компонентов полностью не определены. Специфический класс ОИБ - класс ОИБ, в котором полностью определены типы данных для всех компонентов. Общий класс ОИБ соответствует объединению специфических классов ОИБ.

3.3 Структура ОИБ

Спецификация каждого ОИБ в настоящем стандарте включает в себя следующие части:

– описание ОИБ;

– разъяснение использования ОИБ;

– описание компонентов ОИБ.

Описание компонентов ОИБ включает спецификацию языка ASN.1 и идентификатор объекта, класс которого определяется.

4 Спецификация объектов информационной защиты

Если для ОИБ определено новое техническое требование, следующие действия должны быть осуществлены, чтобы способствовать повторному использованию существующих спецификаций и уменьшить распространение различных спецификаций, содержащих одни и те же требования:

– если настоящий стандарт определяет ОИБ, который содержит новое требование, должно использоваться определение данного стандарта.

– компоненты ОИБ, определенные в настоящем стандарте, должны использоваться в определении нового ОИБ, если они удовлетворяют части нового требования.

Спецификации ОИБ, разработанные для поддержки управления доступом, включены в следующие подразделы. Полное определение языка ASN.1 для объектов информационной защиты, рассмотренных в этих подразделах, включено как модуль в Приложении А. Этот модуль идентифицируется в соответствии с Рисунком 1.

```
id-SIOsAccessControl-MODULE OBJECT IDENTIFIER ::= {
        joint-iso-itu-t sios(24) specification(0) modules(0) accessControl(0)}
```

Рисунок 1

4.1 Категория конфиденциальности

4.1.1 Введение

Организация должна иметь политику безопасности, установленные ею параметры безопасности, определяющие категорию конфедециальности, включающие в себя следующее:

а) уровень защиты, предоставленной данным, хранящимся в системе;

б) лиц, уполномоченных получать доступ к данным, процессам или ресурсам;

в) маркировки безопасности, отображающиеся на любом дисплее или печатном образце материала;

г) требования к маршрутизации и шифрованию данных, передаваемых между системами;

д) требования для защиты против несанкционированного копирования;

е) методы хранения данных;

ж) алгоритмы кодирования, которые будут использоваться;

и) методы авторизации субъектов;

к) необходимость проверки действий, применимых к объекту;

л) требование к предотвращению отказа получения объекта получателями;

м) статус необходимости цифровых подписей для подтверждения подлинности данных.

Когда данные считываются из информационной системы (ИС), или когда они передаются электронным способом между системами, данные маркируются, для указания категории безопасности, к которой эти данные принадлежат и для определения каким образом данные должны быть обработаны системой в плане безопасности. Метка может идентифицироваться отдельно от защищенной информации, но логически указывать на нее.

Целостность меток конфиденциальности, и их привязка к информации должны быть гарантированы. Это позволяет информационным системам и сетям принимать соответствующие области безопасности решения, такие как управление доступом и маршрутизация, без необходимости получать доступ к информации, которая была защищена. Метка конфиденциальности может быть связана с каждым объектом данных в информационной системе, как, например, документы, сообщения электронной почты, отображаемые окна, записи базы данных, элементы директорий и электронные формы. Метки предназначены для использования во время хранения объектов, перемещения (особенно между системами), и обработки приложениями, которые действуют по метке, включая приложения, создающие новые объекты из уже существующих.

Когда содержащая метку информация передается между различными зонами действия информационной безопасности, зоны действия должны согласовывать политику информационной безопасности, чтобы обеспечить принятие этих данных. Если принятые в зоне информационной безопасности метки отличаются от меток, определенных политикой совместно используемых данных, то политика совместно используемых данных должна определять согласно какому набору меток передавать данные.

Сами по себе метки не гарантируют в достаточной степени безопасность информации. Принятую политику информационной безопасности необходимо применять каждой организации до тех пор, пока имеющая метку информация находится в рамках их управления. Все организации, отдельные представители, системы информационных технологий, которые обрабатывают информационные сообщения, считаются ознакомленными с политикой информационной безопасности этой информации. Организациям, обменивающимся информацией, необходимо установить договоренности друг с другом, чтобы быть уверенными в том, что управление информацией

осуществляется в соответствии с согласованной политикой информационной безопасности. Эта договоренность обычно устанавливается в виде официального соглашения.

4.1.2 Спецификация метки конфиденциальности языка ASN.1

Метка конфиденциальности идентифицируется следующим образом, как представлено на Рисунке 2

```
.
id-ConfidentialityLabel OBJECT IDENTIFIER ::= {
        joint-iso-itu sios(24) specification(0) securityLabels(1) confidentiality(0)}
ConfidentialityLabel ::= SET {
        security-policy-identifier          SecurityPolicyIdentifier OPTIONAL,
        security-classification             INTEGER(0..MAX) OPTIONAL,
        privacy-mark                        PrivacyMark OPTIONAL,
        security-categories                 SecurityCategories OPTIONAL }
(ALL EXCEPT ({-- none; at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

PrivacyMark ::= CHOICE {
  pString                                   PrintableString (SIZE(1..ub-privacy-mark-length)),
  utf8String                                UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128 -- as defined in ITU-T Rec. X.411 | ISO/IEC 10021-4

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
        type [0]   SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
        value      [1]   SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type})
}
SECURITY-CATEGORY ::= TYPE-IDENTIFIER

                        SecurityCategoriesTable SECURITY-CATEGORY ::=

                                        {…}
```

Рисунок 2

Пример расширения информационного класса объекта TYPE-IDENTIFIER представлен в Приложении Б.

4.1.3 Методы привязки меток конфиденциальности

4.1.3.1 Метод привязки 1

Копия данных (D) и копия метки конфиденциальности (L) хранятся вместе, как запись данных, внутри границ системы безопасности. Предполагается, что система способна к защите целостности метки конфиденциальности и целостности данных настолько, насколько возможно. Защита, предоставленная системой, должна быть такой, чтобы неавторизованный пользователь или приложение не могли изменить данные или метку конфиденциальности, привязанную к этим данным. Данному методу привязки не нужна никакая шифровальная функция для связывания данных и метки конфиденциальности.

4.1.3.2 Метод привязки 2

Несекретная цифровая подпись (S) вычислена на D и L с использованием алгоритма

цифровой подписи (SigAlg) и персонального ключа (X) алгоритма криптосистемы с открытым ключом, как представлено на Рисунке 3.

S = SigAlg(X,f(D),L)

Рисунок 3

Цифровая подпись хранится вместе с D и L в записи данных. Сгенерированная цифровая подпись связывает L с D. В этом определении f - открытая функция, таким образом, f (D) не показывает информацию о D.

В данном методе привязки, L и S не должны храниться внутри границ системы безопасности. Если шифровальная служба запущена с неправильным значением L, D или S, обнаруживается несовместимость. Это исполняется посредством использования алгоритма открытого ключа в качестве ключа подтверждения подписи.

4.1.3.3 Метод привязки 3

Несекретный код аутентификации сообщений (Message authentification code, MAC) вычисляется на D и L, с использованием режима MAC-generation алгоритма шифрования (MacAlg) и секретного ключа алгоритма MAC (K-MAC), как показано на Рисунке 4.

MAC = MacAlg(K-MAC,f(D),L)

Рисунок 4

MAC хранится вместе с D и L в записи данных. Созданный MAC связывает L с D. В данном определении f - открытая функция, таким образом, f (D) не показывает информацию о D.

В данном методе привязки, L и MAC не должны храниться внутри границ системы безопасности. Если шифровальная служба запущена с неправильным значением L, D или MAC, обнаруживается несовместимость. Это исполняется посредством вычисления соотносящегося MAC, с использованием предоставленных значений L и D и копии K-MAC, и сравнения результата с предоставленным MAC.

4.2 Информационный файл политики безопасности

4.2.1 Введение

Политика безопасности в ее самой простой форме является совокупностью критериев для обеспечения работы служб безопасности. С учетом политики управления доступом, политика безопасности является подмножеством высшего системного уровня политики безопасности, которая определяет средства для того, чтобы осуществлять политику управления доступом между инициаторами и целями.

Механизмы управления доступом должны:

– разрешать передачу информации, где позволяет специфичная политика;

– не допускать передачу информации, где специфичная политика явно не разрешает.

Политика безопасности является основанием для принятия решений механизмами управления доступом. Специфическая для зоны действия информация политики безопасности передается через Информационный файл политики безопасности.

Информационный файл политики безопасности содержит последовательность следующего:

a) verionInformation – указывает версию синтаксиса языка ASN.1 и сопутствующую

семантику спецификации информационного файла политики безопасности;

б) updateInformation – указывает действенность данных информационного файла политики безопасности;

в) securityPolicyIdData – идентифицирует политику безопасности, к которой применяется Информационный файл политики безопасности;

г) privilegeId – указывает идентификатор объекта (ИО), который идентифицирует синтаксис, включенный в допускающий атрибут категории безопасности доверенных сертификатов, используемых в соединении с информационным файлом политики безопасности. Синтаксис, обозначенный privilegeId, должен быть совместим с обозначенным rbacId;

д) securityClassifications – преобразовывает классификацию метки конфиденциальности в классификацию в допускающем атрибуте, а также обеспечивает эквивалентность описаний;

е) rbacId – правило, основанное идентификатором объекта управления доступом, который идентифицирует синтаксис, включенный в категорию безопасности securityLabel, которая используется в соединении с информационным файлом политики безопасности. Синтаксис, обозначенный rbacId, должен быть совместим с обозначенным privilegeId;

ж) securityCategories – преобразовывает категории безопасности метки конфиденциальности в категории безопасности в допускающем атрибуте, а также обеспечивает эквивалентность описаний;

и) equivalentPolicies – объединяет все эквивалентные политики в ИФПБ;

к) defaultSecurityPolicyIdData – идентифицирует политику безопасности, которая будет применяться, если данные будут получены без метки конфиденциальности;

л) extensions – обеспечивает механизм включения дополнительных возможностей в качестве будущих идентифицируемых требований.

Информационный файл политики безопасности является объектом, подписанным с целью защиты от несанкционированных изменений.

4.2.2 Спецификация языка ASN.1 информационного файла политики безопасности

Информационный файл политики безопасности определен следующим синтаксисом, как показано на Рисунке 5.

```
SecurityPolicyInformationFile ::= SIGNED {EncodedSPIF}

EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )

SPIF ::= SEQUENCE    {
    versionInformation                          VersionInformationData DEFAULT v1,
    updateInformation                           UpdateInformationData,
    securityPolicyIdData                        ObjectIdData,
    privilegeId                                 OBJECT IDENTIFIER,
    rbacId                                      OBJECT IDENTIFIER,
    securityClassifications             [0]     SEQUENCE OF SecurityClassification OPTIONAL,
    securityCategories                  [1]     SEQUENCE OF SecurityCategory OPTIONAL,
    equivalentPolicies                  [2]     SEQUENCE OF EquivalentPolicy OPTIONAL,
    defaultSecurityPolicyIdData         [3]     ObjectIdData OPTIONAL,
    extensions                          [4]     Extensions OPTIONAL }
```

Рисунок 5

4.2.2.1 Информация о версии

Поле versionInformation указывает версию синтаксиса языка ASN.1, а заодно и сопутствующую семантику, как показано на Рисунке 6.

```
VersionInformationData:: = INTEGER { v1(0) } (0..MAX)
```

Рисунок 6

4.2.2.2 Информация об обновлении

UpdateInformationData является последовательностью информации, имеющей отношение к определенной версии данных ИФПБ. sPIFVersionNumber дифференцируется между различными версиями информации ИФПБ для политики безопасности, идентифицированной securityPolicyIdData в ИФПБ. creationDate указывает, когда ИФПБ был произведен. originatorDistinguishedName идентифицирует лицо, подписывающее ИФПБ. keyIdentifier идентифицирует ключ, используемый для подписания ИФПБ, как показано на Рисунке 7.

```
UpdateInformationData ::= SEQUENCE                {
    sPIFVersionNumber                             INTEGER (0..MAX),
    creationDate                                  GeneralizedTime,
    originatorDistinguishedName                   Name,
    keyIdentifier                                 OCTET STRING OPTIONAL }
```

Рисунок 7

4.2.2.3 Политика безопасности данных ID

SecurityPolicyIdData идентифицирует политику безопасности, к которой применяется ИФПБ. securityPolicyIdData определен как ObjectIdData, где ObjectIdData является последовательностью objectId и objectIdName. objectId является идентификатором объекта (ИО), назначенным на определенный объект, в то время как objectIdName является последовательностью, идентифицирующей определенный объект, как показано на рисунке 8.

```
ObjectIdData ::= SEQUENCE {
    objectId                                      OBJECT IDENTIFIER,
    objectIdName                                  ObjectIdName }
ObjectIdName ::= DirectoryString {ubObjectIdNameLength}
```

Рисунок 8

4.2.2.4 Идентификатор привилегии

Идентификатор объекта privilegeId идентифицирует синтаксис, который включен в категорию безопасности доверенных сертификатов допускающего атрибута, используемых в соединении с ИФПБ.

4.2.2.5 Идентификатор базовых правил управления доступом

Идентификатор объекта rbacId идентифицирует синтаксис, который включен в категорию безопасности securityLabel, используемую в соединении с ИФПБ. Синтаксис, обозначенный rbacId, должен быть совместим с обозначенным privilegeId.

4.2.2.6 Классификации безопасности

Последовательность SecurityClassification присутствует в ИФПБ для каждого значения классификации безопасности, определенной для политики безопасности, идентифицированной в securityPolicyIdData. Это - дополнительный элемент.

labelAndCertValue представляет значение, назначенное для данной классификации в метке конфиденциальности, и значение целого числа, отображающее местоположение бита данной классификации безопасности в допускающем атрибуте classList BIT STRING.

classificationName является строкой, идентифицирующей данную классификацию, используемую приложением, для определения текста, который будет показан пользователю, выбирающему или просматривающему значение классификации в метке конфиденциальности.

equivalentClassifications является последовательностью значений классификации (определенные в политике безопасности, кроме securityPolicyIdData), которые эквивалентны SecurityClassification labelAndCertValue.

hierarchyValue указывает относительное положение SecurityClassification labelAndCertValue в иерархии классификаций безопасности в политике безопасности, обозначенной securitypolicyIdData. hierarchyValue должен быть уникальным в пределах политики безопасности.

markingData идентифицирует информацию маркировки, приложенную к объекту данных. markingData составлен из строк и кодовой маркировки, которые идентифицируют, где строка физически показана. Если markingPhrase отсутствует, то markingCode относится к SecurityClassification classificationName.

Когда категория безопасности или классификация безопасности избраны для включения в метку конфиденциальности, сопутствующая ИФПБ область requiredCategory, если представлена, указывает на категории безопасности, которые должны также быть включены в метку конфиденциальности в объединении с отобранным значением. Если область requiredCategory не присутствует, то у отобранного значения нет никаких зависимостей от любых категорий безопасности.

Если операция OptionalCategoryGroup является onlyOne, то одна (и только одна) категория безопасности, включенная в categoryGroup, должна быть включена в метку конфиденциальности. Если операция OptionalCategoryGroup является oneOrMore, то одна или более категорий безопасности, включенных в categoryGroup, должны быть включены в метку конфиденциальности. Если операция OptionalCategoryGroup является всем, то все категории безопасности, включенные в categoryGroup, должны быть включены в метку конфиденциальности. Пользователь должен выбрать каждое значение. Если множитель OptionalCategoryGroups присутствует в requiredCategories, то требование, выраженное всеми OptionalCategoryGroups, должно быть удовлетворено. categoryGroup является последовательностью OptionalCategoryData. Идентификатор объекта optCatDataId должен определить синтаксис для использования в OptionalCategoryData области categorydata, которая совместима с определенным типом идентификаторов объекта rbacId, privilegeId и SPIF SecurityCategory.

Obsolete компонент, когда установлен в значении TRUE, указывает, что прежде действительная классификация является теперь устаревшей. Такая классификация может быть связана со старыми объектами данных, но она не должна быть связана с новыми, как показано на Рисунке 9.

```
SecurityClassification ::= SEQUENCE   {

    labelAndCertValue
    classificationName
    equivalentClassifications [0]     EquivalentClassifications OPTIONAL,
    hierarchyValue                    INTEGER,
    markingData               [1]     MarkingDataInfo OPTIONAL,
    requiredCategory          [2]     OptionalCategoryGroups OPTIONAL,
    obsolete                          BOOLEAN DEFAULT FALSE      }

LabelAndCertValue ::= INTEGER (0..MAX)
ClassificationName ::= DirectoryString { ubClassificationNameLength }
EquivalentClassifications ::= SEQUENCE SIZE(0..MAX) OF EquivalentClassification
```

```
EquivalentClassification ::=          SEQUENCE {
        securityPolicyId              OBJECT IDENTIFIER,
        labelAndCertValue             LabelAndCertValue,
        applied Applied }
Applied ::= INTEGER {
     encrypt (0),
     decrypt (1),
     both     (2) }
(encrypt | decrypt | both)

MarkingDataInfo ::= SEQUENCE SIZE(1..MAX) OF MarkingData
MarkingData ::= SEQUENCE {
     markingPhrase                    MarkingPhrase OPTIONAL,
     markingCodes                     MarkingCodes OPTIONAL }
(ALL EXCEPT {-- none; at least one component shall be present --})

MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }

MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

MarkingCode ::= INTEGER {
        pageTop          (1),
        pageBottom       (2),
        pageTopBottom    (3),
        documentEnd      (4),
        noNameDisplay    (5),
        noMarkingDisplay (6),
        unused           (7),
        documentStart    (8),
        suppressClassName (9)  }
OptionalCategoryGroups ::=SEQUENCE SIZE(1..MAX)

OptionalCategoryGroup ::=SEQUENCE {
        operation        Operation,
        categoryGroup    CategoryGroup }
Operation ::= INTEGER {
         onlyOne         (1),
         oneOrMore       (2),
         all             (3)}
  (onlyOne | oneOrMore | all)
CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData
OptionalCategoryData ::= SEQUENCE {
         optCatDataId    OC-DATA.&id({CatData}),
         categorydata    OC-DATA.&Type({CatData}{@optCatDataId }) }
OC-DATA ::= TYPE-IDENTIFIER
CatData OC-DATA ::= { … }
```

Рисунок 9

4.2.2.7 Категории безопасности

Последовательность SecurityCategory присутствует в ИФПБ для каждой категории безопасности, определенной для политики безопасности, идентифицированной в securityPolicyIdData. Синтаксис SecurityCategory определен в метке конфиденциальности, данной в 5.1. Синтаксис определен для использования в области значения SecurityCategory, которая обозначена идентификатором объекта типа SecurityCategory и должна быть совместимой с синтаксисами, обозначенными идентификаторами объекта privilegeId, rbacId и optCatDataID.

4.2.2.8 Эквивалентные политики

equivalentPolicies является перечнем всей политики безопасности, для которой значения были включены в ИФПБ как эквивалентные значения. securityPolicyId является идентификатором объекта, который идентифицирует эквивалентную политику безопасности. securityPolicyName является дополнительной директивной строкой, идентифицирующей название эквивалентной политики безопасности, как показано на Рисунке 10.

```
EquivalentPolicy ::= SEQUENCE {
        securityPolicyId                    OBJECT IDENTIFIER,
        securityPolicyName                  SecurityPolicyName OPTIONAL}

SecurityPolicyName ::= DirectoryString {ubObjectIdNameLength}
```

Рисунок 10

4.2.2.9 Идентификатор политики безопасности, заданный по умолчанию

Значение для defaultSecurityPolicyIdData поддерживает возможность взаимодействия с приложениями, которые не поддерживают функцию управления доступом. На данный идентификатор объекта ссылаются, когда не используется ни одна метка конфиденциальности.

Заметьте, что политика безопасности по умолчанию будет иметь простой уровень классификации. Когда значение категории защиты будет преобразовано в политику безопасности, заданную по умолчанию, тогда SEQUENCE ИФПБ SecurityClassification для обозначенного значения будет включать SEQUENCE equivalentClassification, в которой policyId установлен в идентификатор объекта политики безопасности, заданной по умолчанию.

4.2.2.10 Расширения

Поле extension является последовательностью информации, которое позволяет в будущем расширять ИФПБ по мере идентификации дополнительных требований, поддерживая возможность взаимодействия с предыдущими реализациями ИФПБ. Оно содержит компоненты extnId, critical, и extnValue. Синтаксис введен [5].

Расширение может быть обозначено как критическое или некритическое. Система, использующая ИФПБ, должна отклонить ИФПБ, если она сталкивается с критическим расширением, и не может его распознать; однако, некритическое расширение может быть проигнорировано, если оно не распознано. Сигнал предупреждения должен выдаваться при принятии любых критических расширений, использование которых возможно предотвратить в основном контексте, как показано на Рисунке 11.

```
Extensions ::= SEQUENCE OF Extension
Extension ::= SEQUENCE {
        extnId                              EXTENSION.&id ({ExtensionSet}),
        critical                            BOOLEAN DEFAULT FALSE,
        extnValue                           OCTET STRING

                        -- contains a DER encoding of a value of type &ExtnType
                        -- for the extension object identified by extnId -- }
ExtensionSet EXTENSION ::= { … }
EXTENSION ::= CLASS {
      &id                                   OBJECT IDENTIFIER UNIQUE,
      &ExtnType }
WITH SYNTAX { SYNTAX &ExtnType IDENTIFIED BY &id }
```

Рисунок 11

4.3 Допускающий атрибут

4.3.1 Введение

Допускающий атрибут используется, чтобы определить полномочия, предоставленные определенному пользователю или прикладному компоненту. Полномочия, предоставленные пользователю или прикладному компоненту, могут быть подмножеством всеобъемлющей политики (или политик) безопасности организации. Чередуясь, полномочия могут полностью охватить политику обеспечения безопасности.

Допускающий атрибут содержит три компонента: policyId, classList, и, дополнительно, securityCategory как показано на Рисунке 12.

Идентификатор объекта policyId определяет, какие дополнительные компоненты должны присутствовать. Компонент classList определяет предоставленные и иерархические разрешения доступа пользователей согласно classList, который определен [6]. Другие неиерархические списки классов могли быть определены в другом месте для включения в другие ОИБ или адресованы в категории безопасности. Компонент securityCategory идентифицирует любое число ограничительных и разрешающих категорий безопасности в битах так же, как и ограничительных и разрешающих перечисленных категорий безопасности, назначенных пользователю. Данная структура проиллюстрирована на рисунке 13.

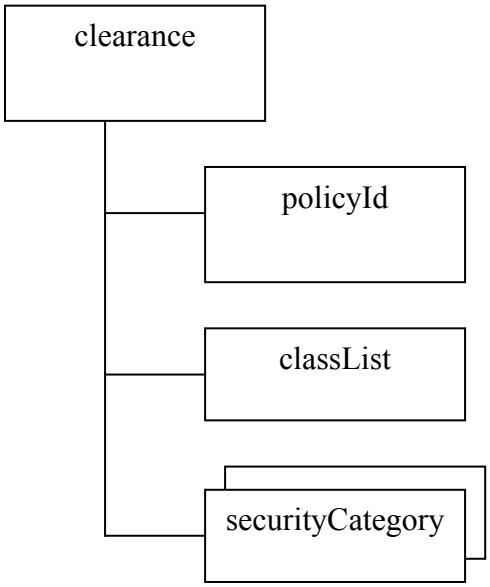


Рисунок 12 – Структура допускающего атрибута

допуск		
Последовательность		
Policyld	classList	securityCategory (optional)
Идентификатор объекта, определяющий политику безопасности	не отмеченный (0) не классифицированный (1)	Уровень доступа определяется по зонам действия:

	ограниченный (2) конфиденциальный (3) секретный (4) совершенно секретный (5)	-Полный доступ (только у одного лица) -Ограниченный доступ (у всех пользователей) -Нумерованный доступ (например, Государственный доступ)

T0733170/d02

Рисунок 13 - Области допускающего атрибута

4.3.2 Определение допускающего атрибута

Допускающий атрибут определяется, как показано на Рисунке 14.

```
clearance ATTRIBUTE ::= { WITH SYNTAX Clearance
        ID                                              id-at-clearance }

id-at-clearance OBJECT IDENTIFIER ::= {
        joint-iso-itu (2) ds (5) attributeType (4) clearance (55) }

Clearance ::= SEQUENCE {
        policyId                                        OBJECT IDENTIFIER,
        classList                                       ClassList DEFAULT
                                                        {unclassified},
        securityCategories                              SecurityCategories OPTIONAL}

ClassList ::= BIT STRING {
        unmarked                                        (0),
        unclassified                                    (1),
        restricted                                      (2),
        confidential                                    (3),
        secret                                          (4),
        topSecret                                       (5)     }

SecurityCategories ::= SET SIZE(1..MAX) OF SecurityCategory
    -- SecurityCategory is defined in the confidentiality label given in subclause 6.1.2
```

Рисунок 14

5 Взаимодействие объекта информационной защиты

5.1 Сравнение структуры класса ОИБ

Для сравнения показаны структуры метки конфиденциальности допускающего атрибута [6] и ИФПБ на рисунке 15. Равнозначные компоненты в этих структурах могут быть исследованы в прикладном программном обеспечении для достижения определенных функциональных возможностей. Достижение функциональных возможностей управления доступом с использованием данных трех структур обсуждено в пункте 5.2.

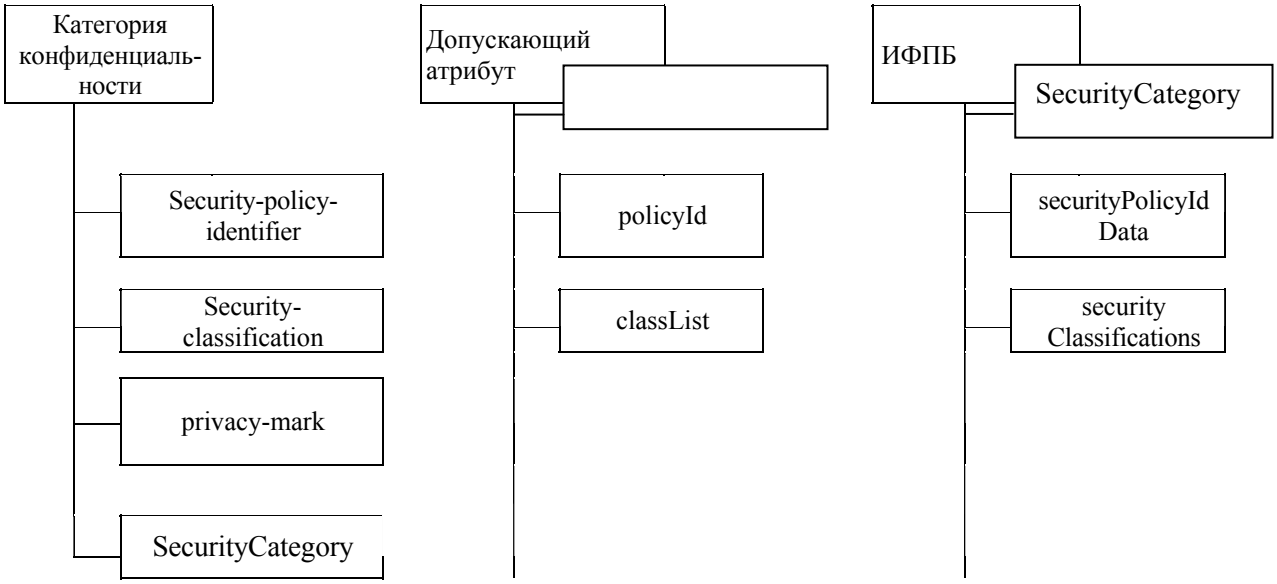
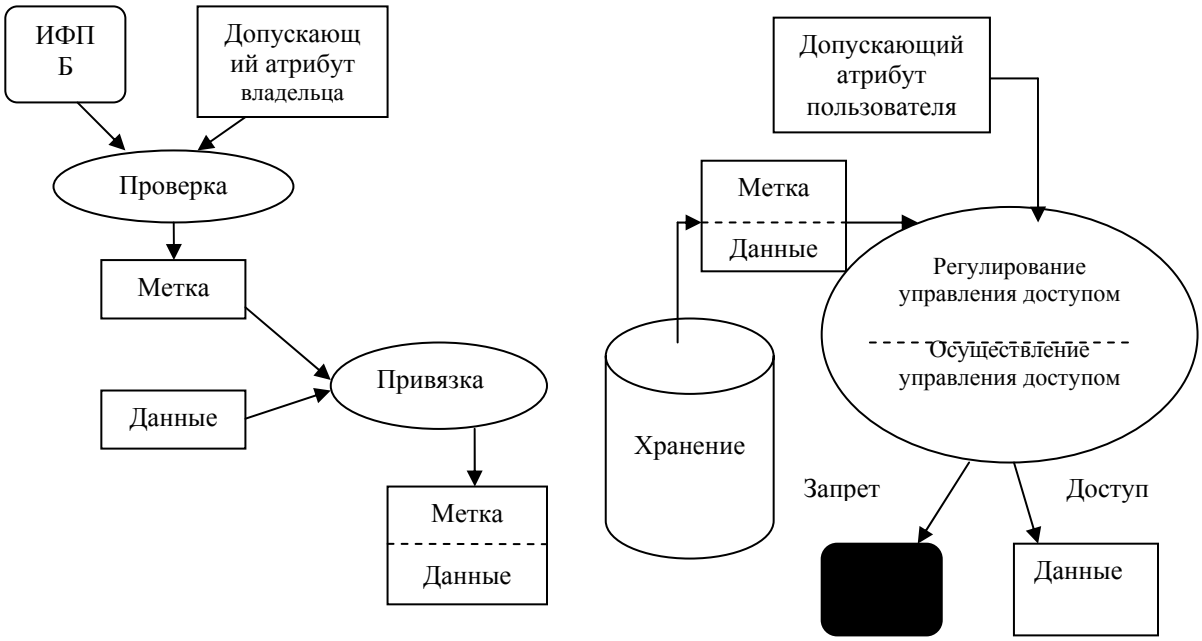


Рисунок 15 – Сравнение равнозначных классов объектов

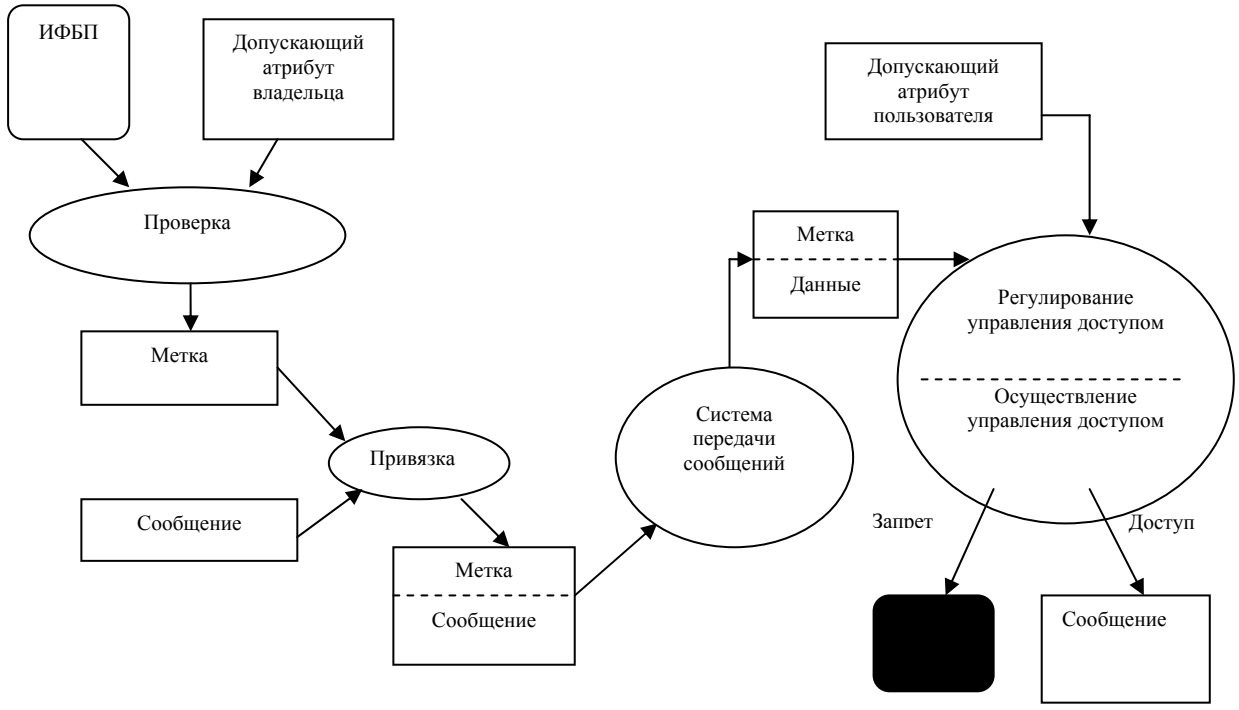
5.2 Взаимодействие объектов информационной защиты по управлению доступом

Управление доступом включает концепцию передачи полномочий для инициаторов или пользователей с помощью использования допускающего атрибута и назначаемых изменений целевым объектам через значения меток конфиденциальности. ИФПБ используется для толкования их полномочий и изменяемых параметров. Прикладное программное обеспечение использует ИФБП, чтобы применить изменения к целям, считать изменения с меток, считать и подтвердить полномочия в сертификатах, и определить разумные отображения через зоны действия политики безопасности.

Используемые механизмы передают полномочия и конфиденциальную информацию, как классификации и категории. Классификации и категории, утвержденные в допускающем атрибуте, вкладываются в сертификат пользователя, посредством чего передаются полномочия этому пользователю. Классификации и категории, так же утвержденные в метке конфиденциальности объекта, служат средством передачи изменений этого объекта. Доступ к объекту разрешен, когда полномочия, переданные в допускающем атрибуте пользователя, достаточно обоснованы в сравнении с изменениями, переданными в метке конфиденциальности объекта цели. Рисунок 16 иллюстрирует взаимодействия среди ОИБ, определенных здесь, обеспечивающие управление доступом в среде хранения данных. Полномочия в допускающем атрибуте владельца данных, содержащиеся в сертификате, соответствующем владельцу данных, ограничивают, какие полномочия из ИФПБ владелец может утвердить в метке для данных цели. Метка связывается с данными и помещается в хранилище. При доступе к данным в устройстве хранения данных, допускающий атрибут пользователя, содержащийся в сертификате, соответствующем пользователю, сравнивается с меткой, связанной с данными цели в функции регулирования управления доступом. Если разрешенные изменения существуют в метке конфиденциальности, они проверяются, чтобы гарантировать, что по крайней мере одно из изменений, представленных в каждом разрешающем теге в метке конфиденциальности, также разрешено и в сертификате (разрешенное полномочие(я)), разрешая доступ к объекту данных цели через функцию Осуществление управлением доступа. Подобный сценарий управления доступом для среды обмена сообщениями показан на Рисунке 17.



Рисунке 16 – Управление доступом к системе хранения



Рисунке 17 – Сценарий управления доступом к обмену сообщениями

Приложение А
(информационное)

Объекты информационной защиты по управлению доступом в языке ASN.1

Данное приложение включает все типы, значения и определения класса информационного объекта языка ASN.1, содержащиеся в настоящем стандарте в форме модуля языка ASN.1.

```
SIOsAccessControl-MODULE  {

      joint-sio-itu sios(24) specification(0) modules(0) accessControl(0)
}

   DEFINITIONS IMPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

IMPORTS


id-at-clearance

  FROM EnhancedSecurity          -- ITU Rec. X.501 | ISO/IEC 9594-2 –-

ATTRIBUTE, Name

  FROM InformationFramework    -- ITU Rec. X.501 | ISO/IEC 9594-2 –-

Extensions

  FROM CertificateExtensions        -- ITU Rec. X.509 | ISO/IEC 9594-8 --


DirectoryString {}

  FROM SelectedAttributeTypes;    -- ITU Rec. X.520 | ISO/IEC 9594-6 --


id-ConfidentialityLabel OBJECT IDENTIFIER  ::=  {joint-iso-itu -t spec(24) specification(0)
securityLabels(1) confidentiality(0)}


ConfidentialityLabel  ::=  SET {

  security-policy-identifier  SecurityPolicyIdentifier OPTIONAL,

       security-classification  INTEGER(0..MAX)  OPTIONAL,

       privacy-mark                              PrivacyMark  OPTIONAL,

       security-categories                       SecurityCategories  OPTIONAL

}
(ALL EXCEPT ({-- none; at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER
PrivacyMark ::= CHOICE {

       pString     PrintableString (SIZE(1..ub-privacy-mark-length)),

       utf8String  UTF8String (SIZE(1..ub-privacy-mark-length))
```

```
    }

    ub-privacy-mark-length INTEGER :: = 128 -- as defined in X.411

SecurityCategories ::= SET SIZE(1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
  type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
  value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                                        {SecurityCategoriesTable}{@type})
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= {
        ... -- objects defined as needed --
}
SecurityPolicyInformationFile ::= SIGNED { EncodedSPIF }
-- Type EncodedSPIF is an open type constrained to be a value
-- of type SPIF. This open type representation is an opaque
-- string of hexadecimal characters suitable for signature
-- and signature verification operations.
EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )

SPIF ::= SEQUENCE {
      versionInformation                VersionInformationData  DEFAULT v1,
      updateInformation                 UpdateInformationData,
      securityPolicyIdData              ObjectIdData,
      privilegeId                       OBJECT IDENTIFIER,
      rbacId                            OBJECT IDENTIFIER,
      securityClassifications           [0] SecurityClassifications  OPTIONAL,
      securityCategories                [1] SPIF-SecurityCategories  OPTIONAL,
      equivalentPolicies                   [2] EquivalentPolicies OPTIONAL,
      defaultSecurityPolicyIdData  [3] ObjectIdData OPTIONAL,
      extenisons                           [4] Extensions OPTIONAL
}
      VerisonInformationData ::= INTEGER { v1(0) } (0..MAX)
      UpdateInformationData ::= SEQUENCE {
          sPIFVerisonNumber          SPIFVersionNumber,
```

```
        creationDate                    GeneralizedTime,

        originatorDistinguishedName  Name,
        keyIdentifier                   OCTET STRING  OPTIONAL
}
SPIFVerisonNumber ::=  INTEGER (0..MAX)

ObjectIdData ::= SEQUENCE {
      objectId          OBJECT IDENTIFIER,
      objectIdName  ObjectIdName
}
ObjectIdName ::= DirectoryString { ubObjectIdNameLength }
SecurityClassifications ::=
      SEQUENCE SIZE(0..MAX) OF SecurityClassification
SPIF-SecurityCategories ::=
      SEQUENCE SIZE(0..MAX) OF SecurityCategory
EquivalentPolicies ::=
      SEQUENCE SIZE(0..MAX) OF EquivalentPolicy
SecurityClassification ::= SEQUENCE {

        labelAndCertValue               LabelAndCertValue,
        classificationName              ClassificationName,
        equivalentClassifications       [0] EquivalentClassifications  OPTIONAL,
        hierarchyValue                  INTEGER,
        markingData                     [1] MarkingDataInfo  OPTIONAL,
        requiredCategory                [2] OptionalCategoryGroups  OPTIONAL,
        obsolete                        BOOLEAN  DEFAULT FALSE
      }
      LabelAndCertValue ::= INTEGER(0..MAX)

      ClassificationName ::= DirectoryString { ubClassificationNameLength }

      EquivalentClassifications ::=
        SEQUENCE SIZE(0..MAX) OF EquivalentClassification
      EquivalentClassification ::= SEQUENCE {
        securityPolicyId   OBJECT IDENTIFIER,
```

```
        labelAndCertValue  LabelAndCertValue,
        applied                        Applied
      }

      Applied ::= INTEGER {

        encrypt (0),

        decrypt (1),

        both     (2)
}

   (encrypt | decrypt | both)

      MarkingDataInfo ::= SEQUENCE SIZE (1..MAX) OF MarkingData


        MarkingData ::= SEQUENCE {

        markingPhrase  MarkingPhrase  OPTIONAL,

        markingCodes   MarkingCodes    OPTIONAL
 }

     (ALL EXCEPT({-- none; at least one component shall be present --}))

MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }

MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

MarkingCode ::= INTEGER {

      pageTop                (1),

      pageBottom             (2),

      pageTopBottom          (3),

      documentEnd            (4),

      noNameDisplay          (5),

      noMarkingDisplay       (6),

      unused                 (7),

     documentStart           (8),

     suppressClassName       (9)

}

 OptionalCategoryGroups ::=

      SEQUENCE SIZE(1..MAX) OF OptionalCategoryGroup

OptionalCategoryGroup ::= SEQUENCE {

      operation          Operation,

     categoryGroup  CategoryGroup
```

```
}
Operation ::= INTEGER {
      onlyOne         (1),
      oneOrMore    (2),
       all              (3)
}
    (onlyOne | oneOrMore | all)
  CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData

  OptionalCategoryData ::= SEQUENCE {

      optCatDataId  OC-DATA.&id({CatData}),
      categorydata   OC-DATA.&Type({CatData}{@optCatDataId })
}

OC-DATA ::= TYPE-IDENTIFIER

CatData OC-DATA ::= {
     ... -- defined as needed –
}
EquivalentPolicy ::= SEQUENCE {
      securityPolicyId       OBJECT IDENTIFIER,
     securityPolicyName  SecurityPolicyName  OPTIONAL
}

SecurityPolicyName ::= DirectoryString { ubObjectIdNameLength }

clearance ATTRIBUTE ::= {
  WITH SYNTAX  Clearance
  ID                      id-at-clearance
}
Clearance ::= SEQUENCE {   -- Automatic tags applied
    policyId                          [0] OBJECT IDENTIFIER,
    classList                         [1] ClassList  DEFAULT { unclassified },
    securityCategories                [2] SecurityCategories  OPTIONAL
}
```

```
ClassList ::= BIT STRING {
        unmarked       (0),
        unclassified    (1),
        restricted      (2),
        confidential    (3),
        secret          (4),
        topSecret       (5)
}
-- upper bound values

ubObjectIdNameLength            INTEGER ::= 256
ubClassificationNameLength      INTEGER ::= 256
ubMarkingPhraseLength           INTEGER ::= 256
-- information object classes --
ALGORITHM ::= CLASS {
        &id     OBJECT IDENTIFIER  UNIQUE,
      &Type  OPTIONAL
}
        WITH SYNTAX { OID &id [PARMS &Type] }
        - parameterized types –
SIGNED { ToBeSigned } ::= SEQUENCE {
        toBeSigned  ToBeSigned,
        algorithm     AlgorithmIdentifier{{SignatureAlgorithms}},
        signature      BIT STRING
}
AlgorithmIdentifier { ALGORITHM:IOSet } ::= SEQUENCE {
   algorithm    ALGORITHM.&id({IOSet}),
   parameters  ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}
SignatureAlgorithms ALGORITHM ::= {
    ... -- defined as needed --}
END  -- SecurityInformationObjects --
```

Приложение Б
(информационное)

Расширение синтаксиса SECURITY-CATEGORY

Класс информационного объекта SECURITY-CATEGORY определен как встроенный класс TYPE-IDENTIFIER, как показано на Рисунке Б.1.

```
SECURITY-CATEGORY  ::=  TYPE-IDENTIFIER
```

Рисунок Б.1

Данный применимый класс информационного объекта определен в Приложении А [2], как показано на Рисунке Б.2.

```
                    TYPE-IDENTIFIER ::= CLASS {
                        &id    OBJECT IDENTIFIER UNIQUE,
                        &Type
}
                        WITH SYNTAX { &Type IDENTIFIED BY &id }
```

Рисунок Б.2

В классе SECURITY-CATEGORY есть два поля, названные &id и &Type. Поле &id определено, чтобы быть значением типа OBJECT IDENTIFER, а поле &Type - открытого типа. Открытый тип может быть любым типом языка ASN.1.

Когда объекты данного класса используются в качестве членов группы информационного объекта, определение поля &id требует, чтобы каждый объект в группе содержал уникальное значение идентификатора объекта. Определение класса также включает утверждение WITH SYNTAX, которое определяет приложение, которое может использоваться для определения информационных объектов класса SECURITY-CATEGORY.

SecurityCategoriesTable – группа информационного объекта класса SECURITY-CATEGORY. Она определяется как показано на Рисунке Б.3.

```
                    SecurityCategoriesTable SECURITY-CATEGORY ::= {
    ... -- objects defined as needed --
}
```

Рисунок Б.3

Совокупность SecurityCategoriesTable содержит маркер расширения, "...", но ни одного информационного объекта. Объекты класса SECURITY-CATEGORY могут быть заданы индивидуально, используя систему обозначения WITH SYNTAX, предоставленную в определении класса. Следующие объекты примера показывают, что любой тип языка ASN.1, простой или сложный, может использоваться для создания информационного объекта, как показано на Рисунке Б.4.

```
                    -- Type 2 - hierarchical attributes

                    enumeratedAttributes SECURITY-CATEGORY ::= {

                            AttributeList IDENTIFIED BY id-enumeratedAttributes
        }

                    AttributeList ::= SET SIZE(1..MAX) OF LabelAttribute

                    -- Type 5 - all attributes in the range(s)

                    rangeSet SECURITY-CATEGORY ::= {
                            RangeList IDENTIFIED BY id-rangeSet
        }

                    RangeList ::= SET SIZE(1..MAX) OF LabelAttributeRange

                    -- Type 6 - release attributes

                    permissiveBitMap SECURITY-CATEGORY ::= {
                       PermissiveBitMap IDENTIFIED BY id-permissiveBitMap
                    }
                    PermissiveBitMap ::= BIT STRING

                    -- Type 7 – for markings with no formal access control –

                    freeFormField SECURITY-CATEGORY ::= {
                            FreeFormField IDENTIFIED BY id-freeFormField
        }
                    FreeFormField ::= SEQUENCE {
                        name   SECURITY-CATEGORY.&id({Fields}),
                           field    SECURITY-CATEGORY.&Type({Fields}{@name})
        }

                    Fields SECURITY-CATEGORY ::= {
                        ... -- defined as needed --
        }
```

Рисунок Б.4

Здесь поля &Type объектов содержат типы языка ASN.1, названные AttributeFlags, AttributeList, RangeList, PermissiveBitMap и FreeFormField. Поля &id содержат уникальные значения идентификатора объекта, названные id-restrictiveBitMap, id-enumeratedAttributes, id-rangeSet, id-permissiveBitMap и id-freeFormField.

Данные объекты могут быть добавлены к версии выполнения SecurityCategoriesTable названием объекта, чтобы сформировать набор категории безопасности из объединения объектов, как показано на Рисунке Б.5.

```
                SecurityCategoriesTable SECURITY-CATEGORY ::= {
                    restrictiveBitMap |
                    enumeratedAttributes  |
                    rangeSet     |
                    permissiveBitMap
                    freeFormField,
                            ... -- expect other objects --
        }
```

Рисунок Б.5

В качестве альтернативы, определения объекта могут быть добавлены непосредственно к набору информации объекта SecurityCategoriesTable, как показано на Рисунке Б.6.

```
SecurityCategoriesTable          SECURITY-CATEGORY          ::=          {
   --
   --                                                                    &Type

&id
            --
            {AttributeFlags  IDENTIFIED BY id-restrictiveBitMap } |
            {AttributeList   IDENTIFIED BY id-enumeratedAttributes}|
            {RangeList       IDENTIFIED BY id-rangeSet                  } |
            {PermissiveBitMapIDENTIFIED BY id-permissiveBitMap } |
            {FreeFormField   IDENTIFIED BY id-freeFormField},
      ... -- expect other objects --   }
```

Рисунок Б.6

Данный вид группы категорий безопасности показывает таблицу четырех рядов, каждый имеет две колонки, одну колонку для &id и другую для &Type.

Тип SecurityCategory определяется как последовательность двух компонентов, называемых типом и значением.

```
SecurityCategory ::= SEQUENCE {
                        type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
                        value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                                                    {SecurityCategoriesTable}{@type})
}
```

Рисунок Б.7

Каждый из данных компонентов указан в терминах полей &id и &Type класса SECURITY-CATEGORY. Компонент type задан в терминах поля &id и должен быть значением типа OBJECT IDENTIFIER. Компонент значения задан полем &Type и может быть значением любого типа языка ASN.1.

Набор информационного объекта SecurityCategoriesTable используется, чтобы образовать разграничение таблицы на действительные значения компонентов type и value SecurityCategory. У разграничения таблицы есть две колонки, по одной для каждого поля класса SECURITYCATEGORY.

Уникальное значение идентификатора объекта, заданное полем &id компонента type, выбирает ряд в таблице. Обозначение @type выбирает столбец &Type, связанный со значением &id выбранного ряда. Маркер расширения в наборе SecurityCategoriesTable указывает, что приложение должно ожидать любой объект, кроме тех, которые явно определены в наборе.

Библиография

[1] МСЭ-Т Рекомендация X.680 (1997) МТС | ИСО/МЭК 8824-1:2002 Информационные технологии. Нотация абстрактного синтаксиса версии 1 (ASN.1). Часть 1. Спецификация базовой нотации.

[2] МСЭ-Т Рекомендация X.681 (1997) МТС | ИСО/МЭК 8824-2:2002 Информационные технологии. Нотация абстрактного синтаксиса один (ASN.1). Часть 2. Спецификация информационных объектов.

[3] ИСО/МЭК 2382-8:1998 Информационные технологии. Словарь. Часть 8. Защита конфиденциальных данных

[4] ИСО/МЭК 7498-2:1989 Системы обработки информации. Взаимодействие открытых систем. Базовая эталонная модель. Часть 2: Архитектура защиты.

[5] МСЭ-Т Рекомендация X.509 (2000) МТС | ИСО/МЭК 9594-8:2005 Информационные технологии. Взаимосвязь открытых систем. Директория. Часть 8. Структура сертификата на общий ключ и атрибуты.

[6] МСЭ-Т Рекомендация X.501 (2001) МТС | ИСО/МЭК 9594-2:2005 Информационные технологии. Взаимосвязь открытых систем. Директория. Часть 2. Модели.

[7] МСЭ-Т Рекомендация X.411 (1999) МТС | ИСО/МЭК 10021-4:2003 Информационные технологии. Системы обработки сообщений (MHS). Часть 4. Определение и процедуры абстрактного сервиса.

[8] МСЭ-Т Рекомендация X.500 (2001) МТС | ИСО/МЭК 9594-1:2005 Информационные технологии. Взаимосвязь открытых систем. Директория. Часть 1. Обзор концепций, моделей и услуг.

[9] МСЭ-Т Рекомендация X.682 (1997) МТС | ИСО/МЭК 8824-3:2002 Информационные технологии. Нотация абстрактного синтаксиса один (ASN.1). Часть 3. Спецификация ограничений.

[10] МСЭ-Т Рекомендация X.683 (1997) МТС | ИСО/МЭК 8824-4:1998 Информационные технологии – Абстрактный синтаксис данных версии 1 (ASN.1): Параметризация спецификаций ASN.1.

[11] МСЭ-Т Рекомендация X.690 (1997) МТС | ИСО/МЭК 8825-1:2002 Информационные технологии. Правила кодирования ASN.1. Часть 1. Спецификация основных правил кодирования (BER), канонических правил кодирования (CER) и различительных правил кодирования (DER).

[12] МСЭ-Т Рекомендация X.722 (1992) МККТТ | ИСО/МЭК 10165-4:1992 Информационные технологии. Взаимосвязь открытых систем. Структура информации управления. Часть 4. Руководящие положения для определения управляемых объектов.

[13] МСЭ-Т Рекомендация X.741 (1995) МТС | ИСО/МЭК 10164-9:1995 Информационные технологии. Взаимодействие открытых систем. Управление системами: Часть 9. Объекты и атрибуты для контроля за доступом.

[14] МСЭ-Т Рекомендация X.803 (1994) МТС | ИСО/МЭК 10745:1995 Информационные технологии. Взаимосвязь открытых систем. Модель безопасности для высоких уровней.

[15] МСЭ-Т Рекомендация X.810 (1995) МТС | ИСО/МЭК 10181-1:1996 Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Часть 1. Обзор.

[16] МСЭ-Т Рекомендация X.830 (1995) МТС | ИСО/МЭК 11586-1:1996 Информационные технологии. Взаимодействие открытых систем. Общая защита верхних уровней. Часть 1. Обзор, модели и система обозначений.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: Пространственное разделение, основной класс ОИБ, информационный объект, класс информационного объекта, специалист по 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