**ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ**

# Ақпараттық технологиялар
# Қауіпсіздікті қамтамасыз етудің құралдары мен әдістері
# Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемдері

## 1-бөлім

## КІРІСПЕ ЖӘНЕ ЖАЛПЫ ҮЛГІ

# Информационные технологии
# Методы и средства обеспечения безопасности
# Критерии оценки безопасности информационных технологий

## Часть 1

## ВВЕДЕНИЕ И ОБЩАЯ МОДЕЛЬ

**ҚР СТ ISO/IEC 15408-1-2017**

*(ISO/IEC 15408-1:2009 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model, IDT)*

**Ресми басылым**

**Қазақстан Республикасы Инвестициялар және даму министрлігінің**
**Техникалық реттеу және метрология комитеті**
**(Мемстандарт)**

**Астана**

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ**

# Ақпараттық технологиялар

# Қауіпсіздікті қамтамасыз етудің құралдары мен әдістері

# Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемдері

# 1-бөлім

# КІРІСПЕ ЖӘНЕ ЖАЛПЫ ҮЛГІ

**ҚР СТ ISO/IEC 15408-1-2017**

*(ISO/IEC 15408-1:2009 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model, IDT)*

**Ресми басылым**

**Қазақстан Республикасы Инвестициялар және даму министрлігінің**
**Техникалық реттеу және метрология комитеті**
**(Мемстандарт)**

**Астана**

## Алғысөз

**1** «Зерде» Ұлттық инфокоммуникация холдингі» АҚ **ӘЗІРЛЕП ЕНГІЗДІ**

**2** Қазақстан Республикасы Инвестициялар және даму министрлігі Техникалық реттеу және метрология комитеті Төрағасының 2017 жылғы «24» қарашадағы №334-од бұйрығымен **БЕКІТІЛІП, ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

**3** Осы стандарт ISO/IEC 15408-1:2009 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. АТ-дың қауіпсіздігін бағалау өлшемдері. 1-бөлім. Кіріспе және жалпы модель) халықаралық стандартымен бірдей.

Мемлекеттік және орыс тіліндегі мәтін ресми нұсқасы болып табылады.

Халықаралық стандартты ISO/IEC JTC 1 Ақпараттық технологиялары, SC 31, Автоматты сәйкестендіру және деректерді жинау технологиялары техникалық комитеті әзірледі.

Ағылшын тілінен (en) аударылған.

Негізінде осы ұлттық стандарт дайындалған және оларға сілтемелер берілген стандарттардың ресми даналары Нормативтік техникалық құжаттардың бірыңғай мемлекеттік қорында бар.

Стандарттардың (мемлекетаралық) сілтемелі халықаралық стандарттарға сәйкестігі туралы мәліметтер В.А қосымшасында көрсетілген.

Сәйкестік дәрежесі - бірдей (IDT).

**4** Осы стандартта Қазақстан Республикасының 2004 жылғы 9 қарашадағы № 603-II «Техникалық реттеу туралы» және 2015 жылғы 24 қарашадағы № 418-V ҚРЗ «Ақпараттандыру туралы» Заңдарының нормалары іске асырылды

**5 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ** 2024 жылы
**ТЕКСЕРУ КЕЗЕҢДІЛІГІ** 5 жыл

**6** ҚР СТ ГОСТ Р ИСО/МЭК 15408-1-2006 Ақпараттың технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық технологиялар қауіпсіздігін бағалау критериялары. 1-бөлім. Кіріспе және жалпы модель. **ОРНЫНА ЕНГІЗІЛДІ**

*Осы стандартқа енгізілетін өзгерістер туралы ақпарат жыл сайын шығарылатын «Стандарттау жөніндегі нормативтік құжаттар» ақпараттық сілтемесінде, ал өзгерістер мен түзетулер мәтіні ай сайын басып шығарылатын «Ұлттық стандарттар» ақпарттық сілтемесінде жарияланады. Осы стандарт қайта қаралған (ауыстырылған) немесе күші жойылған жағдайда, тиісті хабарлама ай сайын басып шығарылатын «Ұлттық стандарттар» ақпарттық сілтемесінде жарияланады*

## Кіріспе

ISO/IEC 15408 Ақпараттық технологияның жалпы атауымен. Қауіпсіздікті қамтамасыз ету әдістері. АТ қауіпсіздігін бағалау критерийлері келесі бөлімдерден тұрады:

- 1-бөлім: Кіріспе және жалпы модель
- 2-бөлім: Қауіпсіздікті қамтамасыз етудің функционалдық компоненттері
- 3-бөлім: Қауіпсіздік кепілдігін қамтамасыз ету компоненттері

ISO/IEC 15408 қауіпсіздікті тәуелсіз бағалау нәтижелерінің салыстырмалылығына жол береді. ISO/IEC 15408 оны IT-өнімдер қауіпсіздігінің функционалдық мүмкіндіктеріне қойылатын талаптардың жалпы жиынын және қауіпсіздікті бағалау барысында осы IT-өнімдерге қолданылатын сенім шараларын ұсыну жолымен істейді. Бұл IT-өнімдер аппараттық құралдарда, тігу мен бағдарламалық қамтамасыз етуде іске асырылуы мүмкін.

Бағалау процесі осы IT-өнімдер қауіпсіздігінің функционалдық мүмкіндіктері мен осы IT-өнімдерге қолданылатын сенім шаралары осы талаптарға сәйкес келетініне сенімділік деңгейін белгілейді. Бағалаудың нәтижелері тұтынушыларға осы IT-өнімдер олардың қауіпсіздік қажеттіліктерін қаншалықты қанағаттандыратының анықтауға көмектесе алады.

ISO/IEC 15408 қауіпсіздік функцияларымен IT-өнімдерін әзірлеу, бағалау және/ немесе сатып алу бойынша басшылық ретінде қолданылады.

ISO/IEC 15408 IT-өнімдер бүтін қатарының қауіпсіздік қасиеттерінің қатары үшін бағалау әдістерінің бірнешеуін қолдануға мүмкіндік беретін икемді болып табылады. Осыған байланысты, стандарттың пайдаланушыларына осы икемділіктің дұрыс пайдаланылмауын қадағалау ұсынылады. Мысалы, ISO/IEC 15408-ні бағалаудың қолайсыз әдістерімен, қауіпсіздіктің релеванттық емес қасиеттерімен немесе лайықсыз IT-өнімдермен бірге тіркесте пайдалану бағалаудың мағынасыз нәтижелеріне әкелуі мүмкін.

IT-өнімді бағалау фактісі бағаланған қауіпсіздік қасиеттері мен пайдаланылған бағалау әдістерінің тұрғысында ғана маңызды болады. Бағалау органдарына, бағалаудан шығатын нәтижелердің мағыналық маңызын анықтау мақсатында өнімдерді, олардың қасиеттерін және әдістерді мұқият тексеру ұсынылады. Сонымен қоса, бағаланған өнімді сатып алушыларға бағаланған өнімді, олардың нақты жағдайлары мен қажеттіліктеріне жарамдылығы мен қолайлылығын анықтау үшін осы тұрғыда мұқият қарастыру ұсынылады.

ISO/IEC 15408 активтерді рұқсатсыз ашудан, өзгертуден немесе пайдалануын жоғалтудан қорғау мәселелерін қозғайды. Қауіпсіздікті бұзудың осы үш түріне қатысты қорғау санаттары әдетте тиісінше құпиялылық, тұтастық және қолжетімділік деп аталады. Сондай-ақ, ISO/IEC 15408 осы үш қасиеттен тыс IT қауіпсіздігінің аспектілеріне де қолданылуы мүмкін. ISO/IEC 15408 адам қызметімен байланысты (зиянды немесе басқа) тәуекелдерге, сондай-ақ, адаммен байланысты емес қызметтермен түйіндес тәуекелдерге қатысты қолданылады. IT қауіпсіздігінен басқа, ISO/IEC 15408 басқа IT салаларда қолданылуы мүмкін, бірақ осы салалардағы қолайлылыққа қойылатын талаптарды көрсетпейді.

Кейбір тақырыптар, олар мамандандырылған технологияларға байланысты немесе IT қауіпсіздігіне жанама түрде қатысты болғандықтан, ISO/IEC 15408 стандартынан тыс шыққан болып саналады. Олардың кейбіреулері төменде көрсетілген:

а) ISO/IEC 15408 IT қауіпсіздігінің функционалдығымен тікелей байланысты емес әкімшілік қауіпсіздік шараларына қатысты қауіпсіздіктің бағалау өлшемдерін қамтымайды. Сонымен қоса, ұйымдық, кадрлық, физикалық және процедуралық бақылау сияқты әкімшілік шаралар көбінесе қауіпсіздіктің айтарлықтай деңгейіне жетеді немесе қолдауға ие болады деп танылады.

b) Электромагниттік сәулеленуді басқару сияқты IT қауіпсіздігінің кейбір техникалық физикалық аспектілерін бағалау нақты қарастырылмайды, бірақ қаралған тұжырымдардың көбісі осы салаға қатысты болып табылады.

c) ISO/IEC 15408 стандартында өлшемдер қолданылуы тиіс бағалау әдістемесі қарастырылмайды. Бұл әдістеме ISO / IEC 18045 стандартында көрсетілген.

d) ISO/IEC 15408 стандартында әкімшілік және құқықтық шеңберлер қарастырылмайды, олармен сәйкес өлшемдер бағалау органдарымен қолданыла алады. Алайда, ISO/IEC 15408 бағалау мақсаттары үшін мұндай негіздеме аясында пайдаланылатын болады деп күтілуде.

e) Аккредиттеуде бағалау нәтижелерін пайдалану рәсімдері ISO/IEC 15408 стандартын қолдану аясына кірмейді. Аккредиттеу IT-ның өнімді (немесе оның жиынтығын) АТ-ға қатысы жоқ оның барлық бөліктерін қоса алғанда, оның толық жұмыс істеу ортасында пайдалануға рұқсат беретін әкімшілік процесс болып табылады. Бағалау процесінің нәтижелері аккредитация процесінің бір бөлігі болып табылады. Дегенмен, IT-мен байланысты емес қасиеттерді және олардың IT қауіпсіздік бөлігіне қатыстылығын бағалау мақсатында, басқа әдістер неғұрлым лайықты болса, аккредиттелетін тұлғалар осы аспектілер бойынша бөлек ережелерді жасауы керек.

f) Криптографиялық алгоритмдерге тән қасиеттерді бағалау өлшемдерінің мәні ISO/IEC 15408 стандартында қарастырылмайды. Криптографияның математикалық қасиеттерін тәуелсіз бағалау қажет болған жағдайда бағалау кезінде ISO/IEC 15408 пайдаланылатын бағалау схемасы ұсынылуы тиіс.

Бар құжатта пайдаланылған «мүмкін», «анықтамалық сипат», «мүмкін», «нормативтік», «міндеттенеді» және «міндетті» сияқты ISO стандарттары ISO директивтерінде, 2-бөлімінде белгіленген. «Міндетті» термині осы стандартта қолданған кезде қосымша мағынаға ие екеніне назар аударыңыздар. Төмендегі ескертуді қараңыз. ISO/IEC 15408 стандартында «міндетті» терминін пайдалану үшін келесі анықтама берілген:

Міндетті - нормативтік мәтінде «міндетті» деген сөз «бірнеше мүмкіндіктің ішінде олардың бірі неғұрлым қолайлы ретінде ұсынылады, басқаларды ескерусіз және шығарусыз, немесе іс-әрекеттің белгілі курсы оңтайлы, бірақ міндетті тәртіпте талап етілмейді» дегенді көрсетеді (ISO/IEC директивалары, 2-бөлім).

Ескертпе - ISO/IEC 15408 стандарты «міндетті түрде талап етілмейді» дегенді басқа мүмкіндікті таңдау себептерді негіздеуді талап етеді, олар бойынша оңтайлы нұсқа таңдалған жоқ деп түсіндіреді.

**Мазмұны**

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ**

# Ақпараттық технологиялар
# Қауіпсіздікті қамтамасыз етудің құралдары мен әдістері
# Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемдері

## 1-бөлім

## КІРІСПЕ ЖӘНЕ ЖАЛПЫ МОДЕЛЬ

**Енгізілген күні 2019-01-01**

## 1 Қолданылу саласы

Осы стандарт ақпараттық технология (АТ) қауіпсіздігінің негізгі түсініктері мен бағалау қағидаларын бекітеді, сонымен бірге АТ өнімдері қауіпсіздігінің сипаттамасын бағалау кезінде пайдалану үшін тағайындалған бағалаудың жалпы мөделін анықтайды.

Осы стандартта ISO/IEC 15408 барлық бөлімдеріне жалпы шолу және сипаттама берілген; ISO/IEC 15408 барлық бөлімінде қолданылуы тиіс терминдер мен қысқартулар анықталған; бағалау объектісі (БО), бағалау контесктінің негізгі түсініктері бекітілген, бағалау критерийлеріне бағытталған мақсатты аудитория сипатталған. АТ өнімдерін бағалауға қажетті қауіпсіздіктің негізгі ережелері берілген.

Осы стандарт рұқсат етілген операцияларда пайдалану үшін бейімделуі мүмкін функционалдық компоненттер мен қауіпсіздікке кепілдік компоненттері ISO/IEC 15408-2 және 15408-3-те келтірілген операцияларды белгілейді.

Осы стандартта қорғаныс профильдерінің (ҚП) түсініктері, қауіпсіздік талаптары топтамалары, сондай-ақ сәйкестік туралы тұжырымдамаларға байланысты мәселелер қарастырылады, бағалаудың қорытындылары мен оның нәтижелері сипатталды. Осы стандартта қауіпсіздік бойынша ғимараттар спецификациясы бойынша нұсқамалар берілген және барлық модель шектілігінде компоненттердің құрылымы сипаттамасы берілген.

ISO/IEC 18045-те бағалаудың методологиясы және бағалау жүйесі әрекеттерінің ауданы туралы жалпы ақпарат берілген.

## 2 Нормативтік сілтемелер

Осы стандартты қолдану үшін келесі сілтемелік құжаттар қажет. Күні белгіленген сілтемелер үшін сілтемелік құжаттың көрсетілген баспасы ғана қолданылады, күні белгіленбеген сілтемелер үшін сілтемелік құжаттың соңғы баспасы ғана қолданылады (оның барлық өзгерістерін қоса алғанда):

ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security -Part 2: Security functional components (Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. IT-дегі қауіпсіздікті бағалау критерийлері. 2-бөлім. Қауіпсіздікті қамтамасыз етудің функционалдық компоненттері.)

ISO/IEC 15408-3:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security functional components (Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. IT-дегі қауіпсіздікті бағалау өлшемдері. 3-бөлім. Қауіпсіздік кепілдігін қамтамасыз ету компоненттері)

ISO/IEC 18045:2008 Information technology - Security techniques – Methodology for IT security evaluation (Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. IT қауіпсіздігін бағалау методологиясы)

## 3 Терминдер мен анықтамалар

Осы стандартта тиісті анықтамалармен терминдер қолданылады:

Ескертпе - Осы бөлімде ISO/IEC 15408-те пайдаланылатын терминдер ғана қамтылған. ISO/IEC 15408-те пайдаланылатын арнайы терминдер өздері қолданылған мәнмәтінде анық болуы үшін түсіндіріледі және осы тарауға енгізуді талап етпейді.

### 3.1 ISO/IEC 15408 қолданылатын терминдер мен анықтамалар

3.1.1 **Зиянды әсерлер** (adverse actions): Ресурсқа қатысты қауіп-қатер агенті жүзеге асыратын іс-әрекеттер

3.1.2 **Активтер** (assets): Мақсатты бағалау кезінде баса мән берілетін объектілер (TOE)

3.1.3 **Иемдену** (assignment): ISO/IEC 15408 компонентінде кейбір параметрлерді сәйкестендіру спецификациясы немесе талап ету

3.1.4 **Кепілдік** (assurance): Бағалауда сенімділік негіздері сәйкес келетін объект

3.1.5 **Шабуыл әлеуеті** (attask potential): Бағалау объектісінің шабуылына кететін шараларды күшейту, шабуылдаушының тәжірибесін, ресурсын және қызығушылығын есепке алу

3.1.6 **Аугментация** (augmentation): Бағдарламалық топтамаға бір немесе бірнеше талаптарды қосу

3.1.7 **Аутентификация деректері** (authentication data): Пайдаланушының мәлімделген сәйкестігін верификациялау үшін қолданылатын ақпарат

3.1.8 **Тіркелген қолданушы** (authorized user): Қауіпсіздіктің функционалдық талаптарына сәйкес барлық операцияларды жүргізе алатын бағалау объектісін пайдаланушы (SFR)

3.1.9 **Класс** (class): Жалпы бағыттылығын бөлісетін ISO/IEC 15408 тұқымдастық жиынтығы

3.1.10 **Когеренттік** (coherent): Логикалық реттелген және айқын мағынасы бар

Ескертпе - Құжаттарда бұл мәтінге және құжат құрылымына, мақсатты аудиторияға түсінікті болуы үшін қажет.

3.1.11 **Толық** (complete): Объектінің барлық қажетті бөліктері берілгенін білдіретін қасиет

Ескертпе – Құжаттамаға келер болсақ құжаттамадағы барлық тиісті ақпарат егжей-тегжейлі қаралды, сондықтан абстракцияның бұл деңгейінде қосымша түсініктер талап етілмейді.

3.1.12 **Компонент** (component): Талаптар негіз болуы мүмкін аз бөлінген элементтердің жиынтығы

3.1.13 **Құрамдас кепілді топтама** (composed assurance package): ISO/IEC 15408-3 –тен (негізінен ACO сыныбынан) алынған талаптардан тұратын кепілдік топтама, ISO/IEC 15408 алдын ала белгілеген және кепілдік шкаласының құрамына көзқарасын білдіреді

3.1.14 **Растау** (confirm): тәуелсіз ұйғарымы жеткілікті бір жағдайды немесе бір нәрсені егжей-тегжейлі қарастыруды мәлімдеу

Ескертпе – Қаталдықтың қажетті деңгейі құралдың сипатына байланысты. Бұл термин тек бағалаушының іс-әрекетінде ғана қолданылады.

3.1.15 **Қосылу** (connectivity): Мақсатты бағалаудан тысқары жатқан және IT–дің өзге объектілерімен қосылуға мүмкіндігі бар екендігін білдіретін бағалау объектісінің құрамы

Ескертпе - Бұл сымды немесе сымсыз құралдардың көмегімен қандай да бір қашықтықта, ортада немесе конфигурацияда деректер алмасуды қамтиды.

3.1.16 **Келісілген** (consistent): Бір-біріне деген ешқандай қарама-қарсылығы жоқ екі немесе одан да көп субъектілер арасындағы қарым-қатынас сипаты

3.1.17 **Қарама-қарсы, етістік** (counter, verb): Шабуылды қарсы алу: осыдан нақты қауіп-қатердің әсері жұмсарады, бірақ жойылуы міндетті емес

3.1.18 **Көрсетілім сәйкестігі** (demonstrable conformance): PP–дағы қауіпсіздіктің типтік проблемасын шешетін, ST шешім ұсынатын ST мен PP арасындағы байланыс

Ескертпе - PP және ST мүлде әр түрлі өтініштерден тұруы мүмкін, бұл өтініштер әр түрлі объектілерді талқылайды, әр түрлі концепцияларды пайдаланады және т.б. Көрсетілім сәйкестігі TOE типіне келеді,мұнда бірнеше PP ұқсастық бар, бұл ST авторына күш үнемдеуге, бір мезгілде PP-ның бұған сәйкестігін мәлімдеуге мүмкіндік туғызады.

3.1.19 **Көрсету** (demonstrate): "Дәлелге" қарағанда аз дәрежедегі қатаң талдау нәтижесінде алынған қорытындыны ұсыну

3.1.20 **Тәуелділік** (dependency): Компоненттер арасындағы байланыс: егер тәуелді компонентке негізделген талап PP, ST немесе топтамаға енсе,онда тәуелділік бастау алатын компонентке негізделген талап та PP, ST немесе топтамаға енгізілуі тиіс

3.1.21 **Сипаттау** (deseribe): Объект бойынша нақты бөлшектерді ұсыну

3.1.22 **Анықтау** (determine): Нақты тұжырымға жету мақсатындағы тәуелсіз талдауға негізделген нақты қорытындыны бекіту

Ескертпе - бұл терминді пайдалану әдетте кейбір алдыңғы талдау болмаған жағдайдағы шын мәніндегі тәуелсіз талдауды білдіреді» Растау» немесе «тексеру» терминдерімен салыстырыңыз, өйткені бұл терминдер талдаудың орындалғанын және оны қайта қарастыруды білдіреді.

3.1.23 **Әзірлеу ортасы** (development environment): TOE бағасының объектісін әзірлеу ортасы

3.1.24 **Элемент** (element): Қауіпсіздіктің қажеттіліктерін қамтамасыз ететін бөлінбейтін оператор

3.1.25 **Қамтамасыз ету** (ensure): Іс-әрекет пен оның салдары арасындағы берік себепті байланысты кепілдендіру

Ескертпе - бұл терминнің алдында «көмек» сөзі болса, онда оның салдары бір ғана әрекетке негізделгендіктен толық анық бола алмайтынын көрсетеді.

3.1.26 **Баға** (evaluation): PP, ST немесе TOE-ны айқын өлшемдер бойынша бағалауды жүргізу

3.1.27 **Бағаның кепілдік деңгейі** (evaluation assurance level): ISO/IEC 15408-3 стандартына сәйкес құралған кепілдікке арналған талаптар жиынтығы, ISO/IEC 15408 анықтаған кепілдіктер шкаласының көзқарасын білдіреді, бұлар кепілдік топтамасын қалыптастырады

3.1.28 **Өкілетті бағалаушы орган** (evaluation authority): Бағаның сапасын бақылаушы және стандарттарды белгілейтін орган,органдар мұны нақты қауымдастықта

өткізеді және оны ISO/IEC 15408-ге бұл қауымдастық арқылы сызбасын бағалауды енгізеді

3.1.29 **Баға сызбасы** (evaluation scheme): Әкімшілік және нормативтік база, оған сәйкес ISO/IEC 15408 нақты қауымдастық шеңберінде өкілетті бағалаушы органда қолданылады

3.1.30 **Сарқып алу** (exhaustive): Әдістемелік тәсілдің сипаттамасы, бұл талдауды өткізуге немесе нақты жоспарға сай қызметті қабылдау үшін қажет

Ескертпе - Бұл термин ISO/IEC 15408 –де талдау жүргізуге немесе басқа қызметке қолданылады. Ол жүйемен байланысқан, бірақ барынша күшті болып табылады, өйткені әдістемелік тәсілдің тек қана талдау өткізуге немесе анық жоспарға сай қызметті өткізуге қолданғанын ғана көрсетпейді, сондай-ақ сақталған жоспардың барлық мүмкін жолдарды жүзеге асыруын қамтамасыз еткенін анықтайды

3.1.31 **Түсіндіру** (explain): аргумент беруге, анықтаушы себебін таңдау белгілі бір әрекеттер жүрісін таңдау себебін түсіндіретін аргумент беру

Ескертпе - Бұл терминнің «сипаттау» мен «көрсетуден» айырмашылығы бар. Ол «Неге?» деген сұраққа жауап беруге арналады және таңдалған әрекеттер курсы оңтайлы болғандығын нақты міндетті емес түрде бекітеді.

3.1.32 **Кеңейту** (extension): ISO/IEC 15408-2-де жоқ ST немесе PP-ны функционалдық талаптармен немесе ISO/IEC 15408-3-те жоқ кепілдік талаптармен толықтыру

3.1.33 **Сыртқы субъект** (external entity): TOE шекарасынан тыс TOE-нің бағалау объектісіне өзара іс-қимыл жүргізуге рұқсаты бар IT адамы немесе субъект

Ескертпе - Сыртқы субъект те қолданушы болып есептеледі.

3.1.34 **Отбасылық** (family): Акцент немесе қаталдығынан ерекшеленетін ұқсас мақсаттары бар компоненттер жиынтығы

3.1.35 **Формальды** (formal): Айқын анықталған математикалық түсініктерге негізделген нақты семантикалық синтаксис тілімен шектелген ерекшелік немесе айқындылық

3.1.36 **Әдістемелік құжаттама** (guidance documentation): Жүзеге асыруды, дайындықты, операцияларды, басқаруды немесе TOE-ны пайдалануды сипаттайтын құжаттар

3.1.37 **Ұқсастық** (identity): TOE тұрғысындағы ұқсас объектіні (мысалы, қолданушыны, процесті немесе дискіні) ұсыну

Ескертпе - Осындай ұсыныстарға жол да жатады /жазудағы/ Қолданушы адамға ұсыныс толық немесе қысқартылған атпен немесе лақап атпен берілуі мүмкін.

3.1.38 **Бейресми** (informal): Қарапайым тілмен мазмұндалған

3.1.39 **TSF арасындағы өткелдер** (inter TSF transfers): TOE және IT-дің басқа да сенімді өнімдерінің қауіпсіздік функционалы арасындағы деректерді беру

3.1.40 **Коммуникацияның ішкі арналары** (internal communication channel): TOE-ның жекелген бөліктері арасындағы байланыс арнасы

3.1.41 **TOE-ға ішкі ауысу** (internal TOE transferi): TO-нің жекелеген бөліктері арасындағы деректерді беру

3.1.42 **Іштей келісілген** (internally consistent): Субъектінің қандай да бір аспектілері арасындағы айқын қайшылықтардың болмауы

Ескертпе - Құжаттаманың бөлігінде бұл құжаттамада бір-біріне ешқандай қайшылықтың, өтініштердің мүлдем болмайтындығын білдіреді.

3.1.43 **Итерация** (iteration): Екі немесе одан да көп талаптарды білдіруде бір ғана компонентті пайдалану

3.1.44 **Негіздеме** (justification): Қорытындыға әкелетін талдау

Ескертпе - Көрсетілімге қарағанда «негіздеме» анағұрлым қатаң термин. Бұл термин логикалық аргументтің әрбір қадамын мұқият және егжей-тегжейлі түсіндіруде айрықша қатаңдықты талап етеді.

3.1.45 **Объект** (object): TOE-дегі белсенді емес құрылым, ол ақпаратты қабылдаушы және сақтаушы, объект төңірегінде субъектілер операциялар орындайды

3.1.46 **Операция** (operation) : Модификация немесе компоненттің қайталануы

Ескертпе - Компоненттерге рұқсат етілген операциялар- иемдену, итерация, нақтылау және таңдау.

3.1.47 **Операция** (operation): Субъектінің объект үстінен жүргізетін нақты қимыл түрі

3.1.48 **Операциялық орта** (operational environment): TOE өңделетін орта

3.1.49 **Қауіпсіздікті қамтамасыз ететін ұйымдастырушылық саясат** (organisational security policy): Қандай да бір ұйым үшін ережелер, рәсімдер, нұсқаулықтар жинағы

Ескертпе - Саясат нақты операциялық ортаға жатуы мүмкін.

3.1.50 **Топтама** (paskage): Қауіпсіздікті қамтамасыз ету кепілдігінің талаптары немесе қауіпсіздік фунциясының атаулы жинағы

Ескертпе - «EAL 3» үлгі топтамасы болып табылады.

3.1.51 **Қорғау профилінің бағасы** (Protection Profile evaluation): Белгілі өлшемдер бойынша PP-ны қорғау профилінің бағасы

3.1.52 **Қорғау профилі** (Protection Profile): TOE қауіпсіздігін қамтамасыз ету қажеттіліктері туралы жүзеге асырылатын тәуелсіз өтініш

3.1.53 **Дәлелдеу** (prove): Сәйкестікті математикалық мағынадағы формальды талдау жолымен көрсету

Ескертпе - Барлық жағынан мүлде қатаң термин.Әдетте «дәлелдеу»қатаңдықтың жоғары деңгейінде TSF-тің екі ұсынысының арасындағы сәйкестікті көрсетуге мүмкіндік болғанда қолдану

3.1.54 **Нақтылау** (refienement) Компонентке бөлшектерді қосу

3.1.55 **Рөлі** (role): Қолданушы мен TOE арасындағы рұқсат етілген өзара қарым-қатынасты белгілейтін алдын ала айқындалған ережелер жиынтығы

3.1.56 **Құпия** (secret): Нақты SFR орындау мақсатындағы TSF немесе тіркелген қолданушыға ғана таныс ақпарат

3.1.57 **Қауіпсіз жағдай** (secure state): TSF-тегі деректер келісілген және TSF SFR-ді дұрыс орындауды жалғастыратын жағдай

3.1.58 **Қауіпсіздік атрибуты** (security attribute): SFR-ді айқындауда пайдаланатын және SFR-ді сақтауды қамтамасыз ету үшін қолданылатын маңызы бар субъектілердің, қолданушының (IT-дің ішкі өнімдерін қоса алғанда), объектілердің, ақпараттардың, сеанстардың және ресурстардың сипаты

3.1.59 **Қауіпсіздікті қамтамасыз ету функцияларының саясаты** (security function policy): SFR –дің жиынтық түріндегі айқындылығы және TSF орындайтын нақты қауіпсіздік тәртібін сипаттайтын ережелер жиынтығы

3.1.60 **Қауіпсіздікті қамтамсыз ету мақсаты** (security objective): анықталған қауіпке қарсы тұру ниетін білдіретін өтініш немесе ұйым қауіпсіздігінің айқын саясаткерлеріне немесе жіберілгендерге сәйкес болу

3.1.61 **Қауіпсіздік мәселесі** (security problem): TOE-мен жұмыс істейтіндерге қауіпсіздік саласы мен сипатын формальды түрде айқындайтын өтініш

Ескертпе - Берілген бекіту мыналардан тұрады:
-TOE мен оның операциялық ортасы төтеп беретін қауіп-қатерлер;
-TOE және оның жұмыс ортасы қолданатын OSP;
-TOE-нің операциялық ортасын қолдауға арналған енгізулер

3.1.62 **Қауіпсіздік талаптары** (security requirement): TOE үшін қауіпсіздік мақсатына жетуге ықпал етуге арналған стандарт тілінде берілген талап

3.1.63 **Қауіпсіздік мақсаты** (Security Target): Нақты сәйкестендірілген TOE-ға арналған қауіпсіздік қажеттіліктері туралы тиісті жүзеге асырылатын өтініш

3.1.64 **Таңдау** (selection): Компоненттегі тізімнен бір немесе бірнеше элементтердің ерекшеленуі

3.1.65 **Жартылай формальды** (semiformal): Белгілі бір семантикалық синтаксистің шектелген тілінде айқындалған

3.1.66 **Нақтылау** (specify): Субъект туралы қатаң және нақты бейнеде айқын бөлшектерді ұсыну

3.1.67 **Қатаң сәйкестік** (strict comformance): PP мен ST арасындағы иерархиялық байланыс, PP-дағы барлық талаптар ST-да да бар.

Ескертпе - Бұл қатынасты шамамен «ST қамтуы тиіс барлық бекіту сияқты анықтауға болады, олар PP-да бар,, бірақ көп болуы мүмкін". Болжам бойынша,бұл дәл сәйкестік бірыңғай бейнеде сақтауға қажет қатаң талаптарға қатысты қолданылады.

3.1.68 **ST бағасы** ( ST evaluation): Айқын критерийлер бойынша ST бағасы

3.1.69 **Субъект** (subject): Объектілер үстінен операциялар жүргізетін TOE-дегі белсенді тұлға

3.1.70 **Баға мақсаты** (target of evaluation): Басшылық сүйемелдейтін бағдарламалық немесе аппараттық қамтамасыз етудің жиынтығы

3.1.71 **Қауіп-қатер агенті** (threat agent): Ресурстар үстінен жағымсыз әрекет жасай алатын субъект

3.1.72 **TOE бағасы** (TOE evaluation): Белгілі критерийлер бойынша TOE бағасы

3.1.73 **TOE ресурсы** (TOE resource): TOE-де пайлаланылатын және тұтынылатын бірдеңелер

3.1.74 **TOE қауіпсіздігінің функционалдығы** (TOE security functionality): SFR–ды дұрыс пайдалануға міндетті түрде сүйенетін TOE тігісі мен бағдарламалық қамтамасыз ету, барлық аппараттық қамтамасыз етудің аралас функционалды мүмкіндіктері

3.1.75 **Қадағалау, етістік** (trace, verb): Қатаңдықтың аз деңгейінде екі субъект арасында бейресми талдау сәйкестігін жүргізу

3.1.76 **TOE- ден тыс өткелдер** (transfers outside of the TOE): TSF бақылауынан тыс орналасқан TSF объектілеріне деректерді беру

3.1.77 **Беру** (translation): Қауіпсіздіктің сипатталған талаптарының стандартты тілде сипаттау процесін көрсетеді

Ескертпе- Бұл тұрғыда «аудару» терминін қолдану сөзбе-сөз болып табылмайды, стандартталған тілдегі әрбір SFR қайтадан қауіпсіздік мақсаттарға берілуі мүмкін.

3.1.78 **Сенімді арна** (trusted channel): TSF және келесі сенімді IT өнімінің көмегімен қажетті сенімділікпен өзара әсер ете алатын құрал

3.1.79 **Сенімді IT өнімі** (trusted IT product): IT өнімі TOE болып табылмайды, ол TOE-мен әкімшілік тұрғыда басқарылатын қауіпсіздіктің функционалды талаптарына ие және ол өзінің қауіпсіздігінің функционалдық талаптарын дұрыс орындауда деп есептелінеді.

Ескертпе - Сенім білдірілген IT өнімінің мысалына жеке бағаланған да жатады.

3.1.80 **Сенімді жол** (trusted path): Оның көмегімен қолданушы мен TSF қажетті сенімділікпен хабарласа алатын құрал

3.1.81 **TSF деректері** (TSF data): SFR қолданылатын TOE-ге арналған жұмыстардың деректері

3.1.82 **TSF интерфейсі** (TSF interface): Құралдар, олардың көмегімен ішкі объектілер (немесе субъектілер TOE-да, TOE-дан тыс) TSF-ке деректер ұсынады, TSF-тен деректерді қабылдайды және TSF-тен қызметтерді шақырады

3.1.83 **Қолданушының деректері** (user data): Қолданушыға арналған TSF жұмысына әсер етпейтін деректер

3.1.84 **Верифицирлеу** (verify): Тәуелсіз ұйғарым жеткіліктілігі бөлшектерінде қатаң қарастыру

3.1.85 **Жағымсыз әрекеттер** (adverse actions): Активтерге қатысты қауіп көзінен орындалатын әрекеттер

3.1.86 **Активтер** (assets): ОО қолданушысы үшін болжамды түрде құндылықты ұсынушы мәні

3.1.87 **Тағайындау** (assignment): Компонентте немесе талаптағы белгілі параметрдің спецификациясы

3.1.88 **Сенім** (assurance): ОО нақты TOE-ге жауап беретіндігіне сенімді болуға негіз

3.1.89 **Шабуыл әлеуеті** (attack potential): Құзыреттілік, ресурстар мен бұзушы мотивациясы көрсеткіштерінде айқын көрсетілген ОО-ға шабуыл жасау кезінде кететін күш шамалары

3.1.90 **Күшею** (augmentation): Топтамаға бір немесе бірнеше талаптарды қосу

3.1.91 **Баламалық деректер** (authentication data): Ұсынылған пайдаланушының идентификаторын верификациялау үшін қолданылатын ақпарат

3.1.92 **Құзыретті пайдаланушы** (authorised user): ФТБ-ға сәйкес кейбір операцияларды орындауға рұқсат етілген ОО пайдаланушысы

3.1.93 **Класс** (class): Жалпы тағайындаумен бірлескен отбасылы жинақ

3.1.94 **Нақты** (coherent): Логикалық тізімделген және түсінікті мәні бар

Ескертпе – Құжаттама жағдайында бұл осы мәтінге және сол сияқты мақсатты аудиторияға оның түсінікті болуы мағынасында құжаттың құрылымына қатысты.

3.1.95 **Толық** (complete): Кейбір мәндердің барлық қажетті бөлімдерінде бар қасиет.

Ескертпе – Құжаттамаға қатысты абстракцияның осы деңгейінде бұдан әрі түсінік беруді талап етпейтін бөлшектеу деңгейінде қажетті ақпараттың барлығы құжаттамада көрсетілгендігін білдіреді

3.1.96 **Компонент** (component): Талаптар негізделуі мүмкін элементтердің аз таңдалатын жиынтығы

3.1.97 **Сенімнің құрамды топтамасы** (composed assurance package): Сенімнің алдын ала болжалған құрамдық шкаласында кейбір ережені ұсынатын сенім топтамасы

3.1.98 **Растау** (confirm): Жеткіліктіні тәуелсіз анықтау арқылы ненің бөлшекті тексерілгендігін декларациялау

Ескертпе – Қарастырылатын заттың типіне байланысты қатаңдылықтың талап етілуші деңгейі. Бұл термин бағалаушының әрекеттеріне ғана қолданылады.

3.1.99 **Сыртқы байланыстылық** (connectivity): ОО-ға қатысты сыртқы, АТ мәндерімен оған әрекеттесуге мүмкіндік беруші ОО қасиеті

Ескертпе – Бұл әрекеттесу кез келген ортада немесе кез келген конфигурацияда, кез келген қашықтықта желілік немесе сымсыз құралдармен деректермен алмасуды қосады.

3.1.100 **Қайшылықсыз** (consistent): Екі немесе одан да көп мәндердің арасындағы байланысты, осы мәндердің арасында ешқандай айқын қайшылық жоқ екендігін сипаттайды

3.1.101 **Қарсы тұру** (counter): Кейбір басқыншылыққа қарсы тұруды іске асырулардың жағымсыз, салдарынан кейбір нақты қауіп-қатер азаяды, бірақ міндетті түрде толықтай емес

3.1.102 **Көрсетілетін сәйкестік** (demonstrable conformance): ҚП-да анықталған ҚТ қауіпсіздіктің жалпы проблемаларының шешімін қамтамасыз ететін ҚТ және ҚП арасындағы байланыс

Ескертпе – ҚТ және ҚП әртүрлі түсінікті және т.б. қолданатын, түрлі мәндерге қатысты мүлдем әртүрлі бекітулерден құрылуы мүмкін. Көрсетілетін сәйкестік БО типі үшін келісті болып табылады, ҚТ әзірлеушісіне осы барлық ҚП бір уақытта сәйкестік туралы бекітуге және еңбек шығындарын экономдауға мүмкіндік береді.

3.1.103 **Көрсету** (demonstrate): «Дәлелге» ("proof") қарағанда азырақ қатаң болып табылатын талдау процесінде алынған қорытындыны беру

3.1.104 **Тәуелділік** (dependency): Компоненттер арасындағы арақатынас, егер тәуелді компонентке негізделген кейбір талаптар ҚП, ҚТ немесе топтамаға қосылған болса, онда жоғарыда көрсетілген компонентке тәуелді компонентке негізделген талап та әдетте ҚП, ҚТ немесе топтамаға қосылған

3.1.105 **Бейнелеу** (describe): Кейбір негіздер туралы нақты толықтық беру

3.1.106 **Қорытынды жасау** (determine): Осы қорытындыға жету үшін тәуелсіз талдауға негізделген кейбір қорытындыларды растау

Ескертпе – Осы терминді қолдану қандай да бір алдыңғы талдаудың болмағандығы жағдайында шынайы тәуелсіз талдау орындау түсінігін береді. "Қорытынды жасау" термині талдаудың ерте орындалуын тексеру қажеттілігін жобалайтын «растау» ("confirm") немесе «баламалау» ("verify") терминдерінен ерекшеленеді.

3.1.107 **Әзірлеу ортасы** (development environment): БО әзірлеуі жүзеге асырылатын орта.

3.1.108 **Элемент** (element): Қауіпсіздіктегі кейбір қажеттіліктердің үздіксіз баяндамасы

3.1.109 **Қамтамасыз ету** (ensure): Кейбір әрекеттер және оның салдары арасындағы күшті себепті-тергеулік байланысқа кепілдік беру

Ескертпе – Бұл терминге «көмектесу» термині алдыңғы болса, онда бұл берілген бір әрекет салдарды толық анықтамайтындығын көрсетеді.

3.1.110 **Бағалау** (evaluation): Нақты критерийлер бойынша ҚП, ҚТ және БО-ны бағалау

3.1.111 **Сенімнің бағалау деңгейі** (evaluation assurance level): Сенімнің алдыңғы шкаласында және сенімнің құрамды топтамасында кейбір ережелерді ұсынатын сенім талаптарының жиыны

3.1.112 **Бағалау органы** (evaluation authority): Бағалау жүйесі жолымен осы қоғамдастық үшін ISO/IEC 15408 іске асыруды қамтамасыз ететін және белгілі қоғамдастық шектеуінде ұйымдармен жүргізілетін стандарттарды белгілейтін және бағалаудың сапасын бақылайтын ұйым

3.1.113 **Бағалау жүйесі** (evaluation scheme): Шектеуінде белгілі қоғамдастықта бағалау органдары ISO/IEC 15408 қолданатын әкімшілік-құқықтық құрылым

3.1.114 **Түпкілікті** (exhaustive): Нақты баяндалған жоспарға сәйкес талдау немесе әрекет жүргізуге қарай қолданылатын әдістемелік тәсілдің сипаттамасы

Ескертпе – Бұл термин талдау немесе басқа әрекетті жүргізуге қарай қолданылады. «Жүйелі» ("systematic") терминіне балама болады, бірақ қатаңырақ, өйткені талдау немесе басқа әрекет жүргізудің кейбір нақты баяндалған жоспарына сәйкес әдістемелік тәсіл қолданғандығы ғана көрсетілмейді, сонымен бірге бұл жоспардың барлық мүмкін бағыттар бойынша зерттеу жүргізуді қамтамасыз етуі үшін жеткілікті екендігі көрсетіледі.

3.1.115 **Түсіндіру** (explain): Қолданылатын әрекеттер жолын таңдау үшін негізден тұратын аргументтерді ұсынады

Ескертпе – Бұл термин "суреттеу" ("describe") және "көрсету" ("demonstrate") терминдерінен өзгеше. Аргументке талпыныссыз "Неге?" сұрағына жауап қолданылатын әрекеттердің жолы міндетті түрде оптималдылығымен тағайындалған.

3.1.116 **Кеңейту** (extension): ISO/IEC 15408-2 құрамында жоқ ҚТ немесе ҚП функционалдық талаптардың қосылуы және/немесе ISO/IEC 15408-3 құрамында жоқ сенім талаптары

3.1.117 **Сыртқы мәні** (external entity): БО шекараларының шектеуі салдарынан БО-мен өзара әрекеттесуші адам немесе АТ-мәні

Ескертпе – Сыртқы мәні ретінде БО қолданушысы қарастырылуы мүмкін.

3.1.118 **Отбасылық** (family): Акцент немесе қатаңдығымен ерекшеленетін ұқсас мақсаттарға жетуге бағытталған компоненттер жиынтығы

3.1.119 **Формалды** (formal): Шектелген синтаксисі мен бекітілген математикалық түсінікке негізделген белгілі семантикасы бар тілде беріледі.

3.1.120 **Басшылық құжаттамасы** (guidance documentation): Жеткізу, бекіту, конфигурациялану, пайдалану, басқару және/немесе БО қолдануды суреттейтін құжаттама

3.1.121 **Сәйкестендіруші** (identity): Нақты БО мәнмәтінінде біртекті сәйкестендіруші мәнді (мысалы, пайдаланушы, процесс немесе диск) ұсыну

Ескертпе – Бұл ұсынымның үлгісі символдардың тармақтары болуы мүмкін. Пайдаланушы-адамға мұндай ұсыным толық немесе қысқартылған атау (бірегей) немесе лақап ат болуы мүмкін.

3.1.122 **Формалды емес** (informal): Табиғи тілде білдіріледі

3.1.123 **ФБО арасындағы тапсырыс** (inter TSF transfers): БО және ИТ басқа сенімді өнімдері қауіпсіздігінің функционалдық мүмкіндіктері арасында деректердің тапсырысы.

3.1.124 **Байланыстың ішкі каналы** (internal communication channel): БО бөлінген бөліктері арасындағы байланыс каналы

3.1.125 **БО шектеуіндегі тапсырыс** (internal TOE transfer): БО бөлінген бөліктері арасындағы деректер тапсырысы

3.1.126 **Іштей қайшылықсыз** (internally consistent): Кез келген мәндің аспектілері арасындағы айқын қайшылықтардың жоқтығын сипаттайды.

Ескертпе – Басқаға қайшылық білдіруші ретінде қабылданатын қандай да бір нәрсенің баяндалуы мүмкін еместікті білдіретін құжаттарда қолданылады.

3.1.127 **Итерация** (iteration): Екі немесе одан жеке талаптарды көрсету үшін компонентті қолдану.

3.1.128 **Логикалық негіздеме** (justification): Қорытынды алуға әкелетін талдау

Ескертпе - "Логикалық негіздеме" термині «көрсету» терминіне қарағанда қатаңырақ болып табылады. Бұл термин логикалық талқыламалардың әр қадамының дәл және толық түсіндірмені талап етеді.

3.1.129 **Объект** (object): Ақпараттан тұратын немесе оны алатын және одан субъектілер операцияны орындайтын БО шектеуіндегі пассивті мәні

3.1.130 **Операция** (компонентте) (operation): Компонентті модификациялау немесе қайта қолдану.

Ескертпе – Компоненттегі рұқсат етілген операциялар тағайындау, итерация, нақтылау және таңдау болып табылады.

3.1.131 **Операция** (объектідегі) (operation): Объектіге қатысты субъектімен орындалатын әрекеттің шекті типі.

3.1.132 **Жұмыс істеу ортасы** (operation environment): БО жұмыс істейтін орта.

3.1.133 **Ұйым қауіпсіздігі саясаты** (organisational security policies): Кейбір ұйымдар үшін қауіпсіздік саласында ережелер, процедуралар немесе басқарушы принциптердің жиынтығы.

Ескертпе – Саясат жұмыс істеудің қандай да бір ортасына жатқызылуы мүмкін.

3.1.134 **Топтама** (package): Қауіпсіздікке сенім қауіпсіздігі немесе талаптардың жұмыс істеу талаптарының аталған жиынтығы

Ескертпе – Топтаманың үлгісі "ОУДЗ" болады.

3.1.135 **Қорғау профилін бағалау** (protection profile evaluation): Белгілі критерийлер бойынша ТҚ бағалау.

3.1.136 **Қорғау профилі** (protection profile): Кейбір БО типтері үшін қажеттіліктердің баяндалуының іске асырылуынан тәуелсіз.

3.1.137 **Дәлелдеу** (prove): Математикалық тұрғыда формальды талдау тәсілімен көрсету

Ескертпе – Дәлелдеу барлық қатынаста толық қатаң болуы тиіс. "Дәлелдеу"терминін қатаңдықтың жоғары деңгейінде ФБО-ның екі ұсынымы арасындағы сәйкестікті көрсету қажеттілігінде қолданады.

3.1.138 **Анықтау** (refinement): Компонентке бөлшектердің қосылуы

3.1.139 **Маңызы** (role): Қолданушы мен БО арасындағы рұқсат етілген өзара қарым-қатынасты белгілейтін алдын ала айқындалған ережелер жиынтығы

3.1.140 **Құпия** (secret): Нақты SFR орындау мақсатындағы TSF немесе тіркелген қолданушыға ғана таныс ақпарат

3.1.141 **Қауіпсіз жағдай** (secure state): TSF-тегі деректер келісілген және TSF SFR-ді дұрыс орындауды жалғастыратын жағдай

3.1.142 **Қауіпсіздік атрибуты** (security attribute): SFR-ді айқындауда пайдаланатын және SFR-ді сақтауды қамтамасыз ету үшін қолданылатын маңызы бар субъектілердің, қолданушының (IT-дің ішкі өнімдерін қоса алғанда), объектілердің, ақпараттардың, сеанстардың және ресурстардың сипаты

3.1.143 **Қауіпсіздікті қамтамасыз ету функцияларының саясаты** (security function policy): SFR –дің жиынтық түріндегі айқындылығы және TSF орындайтын нақты қауіпсіздік тәртібін сипаттайтын ережелер жиынтығы

3.1.144 **Қауіпсіздікті қамтамсыз ету мақсаты** (security objective): анықталған қауіпке қарсы тұру ниетін білдіретін өтініш немесе ұйым қауіпсіздігінің айқын саясаткерлеріне немесе жіберілгендерге сәйкес болу

3.1.145 **Қауіпсіздік мәселесі** (security problem): БО-мен жұмыс істейтіндерге қауіпсіздік саласы мен сипатын формальды түрде айқындайтын өтініш

Ескертпе - Берілген бекіту мыналардан тұрады:
- БО мен оның операциялық ортасы төтеп беретін қауіп-қатерлер;
- БО және оның жұмыс ортасы қолданатын OSP;
- БО-нің және оның жұмыс істеу ортасын қолдауға арналған енгізулер

3.1.146 **Қауіпсіздік талаптары** (security requirement): БО үшін қауіпсіздік мақсатына жетуге ықпал етуге арналған стандарт тілінде берілген талап

3.1.147 **Қауіпсіздік тапсырмасы** (Security Target): Нақты сәйкестендірілген БО-ға арналған қауіпсіздік қажеттіліктері туралы тиісті жүзеге асырылатын мұқтаждық

3.1.148 **Таңдау** (selection): Компоненттегі тізімнен бір немесе бірнеше элементтердің ерекшеленуі

3.1.149 **Жартылай формальды** (semiformal): Белгілі бір семантикалық синтаксистің шектелген тілінде айқындалған

3.1.150 **Нақтылау** (specify): Қатаң және нақты нысандағы кейбір мәндердің айқын бөлшектерін ұсыну

3.1.151 **Қатаң сәйкестік** (strict comformance): PP мен ST арасындағы иерархиялық байланыс, PP-дағы барлық талаптар ST-да да бар.

Ескертпе - Бұл қатынасты шамамен «ST қамтуы тиіс барлық бекіту сияқты анықтауға болады, олар PP-да бар,, бірақ көп болуы мүмкін". Болжам бойынша,бұл дәл сәйкестік бірыңғай бейнеде сақтауға қажет қатаң талаптарға қатысты қолданылады.

3.1.152 **Қауіпсіздік тапсырмасының бағасы** ( ST evaluation): Айқын критерийлер бойынша ҚТ бағасы

3.1.153 **Субъект** (subject): Объектілер үстінен операциялар жүргізетін ҚТ-дағы белсенді тұлға

3.1.154 **Бағалау объектісі** (target of evaluation): Басшылық сүйемелдейтін бағдарламалық-аппараттық және/немесе аппараттық қамтамасыз етудің жиынтығы

3.1.155 **Қауіп-қатер көзі** (threat agent): Активтерге жағымсыз әсер ететін мән

3.1.156 **БО бағасы** (TOE evaluation): Белгілі критерийлер бойынша БО бағасы

3.1.157 **БО ресурсы** (TOE resource): БО-де пайлаланылатын және тұтынылатындар

3.1.158 **БО қауіпсіздігінің фунциональды мүмкіндіктері** (TOE security functionality): SFR–ды дұрыс пайдалануға міндетті түрде сүйенетін БО бағдарламалық қамтамасыз ету және барлық аппараттық қамтамасыз етудің фунциональды мүмкіндіктері

3.1.159 **Қадағалау немесе сәйкестендіру** (trace): Қатаңдықтың аз деңгейінде екі мән арасында бейресми талдау сәйкестігін жүргізу

3.1.160 **БО-ден тыс табыстау** (transfers outside TOE): TSF бақылауынан тыс мәні деректерін табыстаудың шектелген TSF

3.1.161 **Трансляция** (translation): Қауіпсіздіктің сипатталған талаптарының стандартты тілде сипаттау процесін көрсетеді

3.1.162 **Сенім білдірілген арна** (trusted channel): TSF және келесі сенім білдірілген IT өнімінің көмегімен қажетті сенімділікпен өзара әсер ете алатын құрал

3.1.163 **Сенім білдірілген IT өнімі** (trusted IT product): IT өнімі БО болып табылмайды, ол БО-мен әкімшілік тұрғыда басқарылатын қауіпсіздіктің функционалды талаптарына ие және ол өзінің қауіпсіздігінің функционалдық талаптарын дұрыс орындауда деп есептелінеді.

Ескертпе - Сенім білдірілген IT өнімінің мысалына жеке бағаланған да жатады.

3.1.164 **Сенімді жол** (trusted path): Оның көмегімен қолданушы мен TSF қажетті сенімділікпен өзара араласатын құрал

3.1.165 **TSF деректері** (TSF data): SFR қодданылатын БО-ге арналған жұмыстардың деректері

3.1.166 **TSF интерфейсі** (TSF interface): Құралдар, олардың көмегімен ішкі объектілер (немесе субъектілер TOE-да,TOE-дан тыс) TSF-ке деректер ұсынады, TSF-тен деректерді қабылдайды және TSF-тен қызметтерді шақырады

3.1.167 **Қолданушының деректері** (user data): Қолданушыға арналған TSF жұмысына әсер етпейтін деректер

3.1.168 **Верифицирлеу** (verify): Тәуелсіз ұйғарым жеткіліктілігі бөлшектерінде қатаң қарастыру

Ескертпе - «Растауды» қараңыз. Бұл терминнің аса қатаң коннотациясы бар». Верифицирлеу» термині бағалаушыдан тәуелсіз күш талап етілгенде бағалаушының іс-әрекет тұрғысында қолданылады.

### 3.2.1 Терминдер мен анықтамалар

Ескертпе - Келесі терминдер бағдарламалық қамтамасыз етудің ішкі құрылымдау талаптарында қолданылады.Олардың кейбіреуі IEEE Std 610.12-1990, бағдарламалық инженерияның стандарттық глоссарий терминологиясынан, Электроника және электротехника инженерлері институтынан алынды.

3.2.1 **Әкімгер** (administrator): TSF-те жүзеге асырылатын барлық саясатқа қатысты сенім деңгейі бар тұлға

Ескертпе - Әкімшіге біркелкі сенім деңгейін PP немесе ST-ның барлығы ұсынбайды.Әдетте әкімшілер әрқашан ST TOE-дегі саясаттарды ұстанады.Олардың кейбір саясаты TOE-нің функционалдығымен байланысты болуы мүмкін,басқалары операциялық ортамен байланысты болуы мүмкін.

3.2.2 **Шақыру ағашы** (call tree): Қай модульдер бір-бірін шақыратындығын көрсететін диаграмма түріндегі системадағы модульдерді идентифицирлейді

Ескертпе - IEEE Std 610.12-1990-дан бейімделген.

3.2.3 **Байланыстылық** (cohesion): [IEEE Std 610.12-1990] бойынша бір-бірімен байланысты ,бір бағдарламалық модульмен орындалатын міндеттердің тәсілі мен дәрежесі

Ескертпе - Байланыстылық түрлері өзіне дәл келуді, коммуникацияны, функционалдылықты, логикалықты, реттілікті, уақытшалықты қамтиды. Байланыстылықтың бұл түрлері тиісті терминологиялық жазбамен сипатталады.

3.2.4 **Кездейсоқ байланыстылық** (coincidental cohesion): [IEEE Std 610.12-1990] бір-бірімен әлсіз байланысқан іс-қимылмен немесе байланыссыз орындалған мінездемесі бар модуль

Ескертпе - мына байланыстылықты қараңыз 3.2.3

3.2.5 **Коммуникациялық байланыстылық** (communicational cohesion): Функциясы бар және олар қорытынды шығаратын немесе [IEEE Std 610.12-1990] модулінде басқа функция қолданатын модуль

Ескерту

1. Байланыстылықты қараңыз (3.2.3)

2. Тексеріске қол жеткізу әрі өзінде міндетті дискрециялық тексерістерді және мүмкіндіктер тексерісін қамтитын модуль коммуникациялық-байланыс модулінің үлгісі болып табылады.

3.2.6 **Талдау күрделілігі** (complexity): Бағдарламалық қамтамасыз етуді, талдау, тестілеу және [IEEE Std 610.12-1990] қолдауды түсінуге арналған шаралар күрделілігі

Ескертпе - Күрделілік деңгейінің төмендеуі - бұл модульдік декомпозицияны, жіктелуді және азайтуды пайдаланудың түпкі мақсаты. Бұл мақсатқа жетуге белгілі дәрежедегі тіркелу мен байланыстылық бақылауы ықпал етеді.

Бағдарламалық қамтамасыз ету әзірлемелері аумағында күрделі соңғы кодтың бағасы үшін метрика әзірлемесіне көп күш жұмсалды. Осы көрсеткіштердің көпшілігі операторлар мен операндтардың саны сияқты,бағандар ағынын басқарудың күрделілігі (цикломатикалық күрделілік), бастапқы кодтың жолдар саны,комментарийлердің орындалатын кодқа қатысын және аналогиялық шаралар сияқты бастапқы кодтың жеңіл есептелетін сипатын пайдаланады. Код қою стандарты оңай түсінілетін кодтың генерирленуі үшін пайдалы аспап болып табылатындығы анықталды.

TSF (ADV INT) класының ішкі объектілері барлық компоненттегі талдау күрделілігін талап етеді. Бұл әзірлеуші қысқарту күрделілігі жеткілікті орын алғанда, осыған қатысты наразылықты қолдауды ұсынады. Бұл қолдау өзіне әзірлеушінің бағдарламалық стандартын қосады және барлық модульдердің стандартқа сәйкес екендігін көрсетеді (немесе кейбір ерекшеліктердің бар екендігін,олардың бағдарламалық қамтамасыз етудің аргументтерімен ақталды). Ол бастапқы кодтың кейбір сипатын өлшеу үшін қолданылатын аспаптар нәтижесін қамтиды немесе әзірлеуші қажет деп тапқан басқа қолдауды қоса алады.

3.2.7 **Ілінісу** (coupling): [IEEE Std 610.12-1990] бағдарламалық модульдері арасындағы бір-біріне тәуелділіктің тәсілі және дәрежесі

Ескертпе - Ілінісу түрлері шақыруды,жалпы және контентті интерфейсті қамтиды. Олар төменде сипатталады.

3.2.8 **Шақырулар ілінісі** (call coupling): Өздерінің құжатталған шақырулар функциясы арқылы бір-бірімен қатаң байланысқан екі модуль арасындағы байланыс

Ескертпе - Деректер, белгі және басқару шақырулар ілінісінің үлгісі болып табылады.

3.2.9 **Шақырулар ілінісі** (call coupling): Деректердің жекелеген элементтерін ұсынатын тек шақырулар параметрін пайдалану арқылы байланысты жүзеге асыратын екі модуль арасындағы байланыс

Ескертпе - Сондай-ақ шақырулар ілінісін қараңыз (3.2.8 ).

3.2.10 **Шақырулар ілінісі** (call coupling): Екі модуль арасындағы байланыс, бұл байланыс бірнеше өрісті немесе маңызды ішкі құрылымдарды қамтитын шақыру параметрлерін пайдаланатын байланысты жүзеге асырады

Ескертпе - Сондай-ақ шақырулар ілінісін қараңыз (3.2.8 ).

3.2.11 **Шақырулар ілінісі** (call coupling): Өзге біреудің ішкі логикасына әсер етуге арналған ақпарат берілген жағдайдағы екі модуль арасындағы байланыс

Ескертпе - Сондай-ақ шақырулар ілінісін қараңыз (3.2.8 ).

3.2.12 **Жалпы бөлім бойынша ілініс** (common coupling): Жалпы деректер аумағын немесе басқа жалпы жүйелік ресурстарды қолданатын екі модуль арасындағы өзара байланыс

Ескертпе - Жаһандық айнымалы көрсеткендей, жаһандық айнымалыны қолданатын модульдер жалпы болып табылады. Әдетте жаһандық айнымалы арқылы жалпы байланысқа жол беріледі,бірақ шектеулі деңгейде ғана жол беріледі.

Мысалы, жаһандық аймаққа өзгермелі орналастырылған ,бірақ бір ғана модульде қолданылғандықтан,дұрыс орналаспаған және оларды жою қажет.Жаһандық айнымалыны бағалау кезінде жарамдылықтарын міндетті түрде ескеретін өзге факторлар:

Жаһандық айнымалыны өзгертетін модульдер саны: Жалпы алғанда,бір ғана модуль жаһандық айнымалы мазмұнын бақылауды жүзеге асыруы қажет, алайда екінші модуль де бұл жауапкершілікті бөлісуі мүмкін жағдайлар да болады. Мұндай жағдайда жеткілікті негіздememен қамтамасыз ету тиіс.Бұл жауапкершіліктің екі модульден артық бөлінуіне жол беруге болмайды. (Бұл бағаны өткізу барысында модульді анықтауға көңіл бөлу керек,өйткені ол айнымалы мазмұнына іс жүзінде жауап береді: мысалы, егер айнымалыны өзгертуге жалғыз ғана рәсім қолданылса,бірақ кіші бағдарлама жай ғана модификацияны орындайды,бұл модификацияны шақырушы тарап сұрата-ды, ол шақырушы модуль болып табылады,мүмкін осындай бір модуль ретінде де жауапты болып табылады). Ары қарай күрделілік анықталған бөлімде егер екі модуль жаһандық айнымалы мазмұнына жауапты болса,онда олардың арасындағы өзгеріс координациясы туралы нақты ұсыныстар болуы тиіс.

Жаһандық айнымалыға негізделген модульдер саны: Жаһандық айнымалыға негізделген модульдер санына шектеу жоқ,көптеген модульдер осындай сілтеме жасаған жағдайда дұрыстылығы мен қажеттілігі тұрғысынан тексерілуі тиіс.

3.2.13 **Ілініс мазмұны** (content coupling): Өзгенің ішкі элементтеріне тікелей сілтеме жасайтын екі модуль арасындағы өзара байланыс

Ескертпе - Үлгілер осы модульдің ішкі бағандарына сілтеме немесе код модификациясын қамтиды. Нәтижесінде кейбір бөлімдер немесе бір модульдің барлық мазмұны басқаға тиімді қосылады. Контент ілінісін модульдердің лицензиясыз интерфейстерді пайдалану ретінде қарастыру қажет.

3.2.14 **Нысандық аймақтарды бөлу** (domain separation) Қауіпсіздік сәулетінің сипаты, ол арқылы TSF әрбір қолданушының және TSF үшін жекелеген домендерін анықтайды және TSF немесе басқа қолданушының қауіпсіздік доменінің мазмұнына ешбір пайдаланушылық процесс әсер ете алмайтындығына кепілдік береді

3.2.15 **Функционалдық байланыстылық** (functional cohesion): [IEEE Std 610.12-1990] бір мақсатта байланысқан іс-әрекетті орындайтын функционалдық сипат

Ескертпе - Функционалдық байланыстырғыш модулі кезек менеджері немесе десте менеджері сияқты бір енгізу түрін бір шығару түріне түрлендіреді.Сондай-ақ байланыстырғышты қараңыз (3.2.3 ).

3.2.16 **Өзара әрекет** (interaction): Жалпы субъектілер арасындағы коммуникативтік қызмет

3.2.17 **Интерфейс** (interface): Компонентпен немесе модульмен өзара әрекет құралдары

3.2.18 **Қабаттану** (layering): Әзірлеме әдісі ,онда модульдердің жекелеген топтары бөлек міндеттерге ие болу үшін иерархиялы ұйымдасқан: бір деңгей иерархия бойынша өз деңгейінен төмен қызметтер үшін тәуелді және өзінің астыңғы қабаттарына ғана өз қызметтерін ұсына алады.

Ескертпе - Қатаң қабаттану шектеу қояды,соған сәйкес әрбір қабат өзінің тікелей астындағы қабаттың қызметтерін пайдаланады,ал тікелей өзінің үстінде орналасқан деңгейге ғана өз қызметін ұсына алады.

3.2.19 **Логикалық байланыстылық** (loqical cohesion): Деректердің әр түрлі құрылымында ұқсас әрекеттерді орындайтын модуль сипаттамасының рәсімдік байланыстылығы

Ескертпе - Егер модульдің функциялары бір-бірімен байланысты, бірақ әр түрлі кіруде әр түрлі операцияларды орындаса ,модуль логикалық байланыстылықты көрсетеді.

3.2.20 **Модульдік декомпозиция** (modular decomposition): [IEEE Std 610.12-1990] бағалауды және әзірлеуді, жобалауды жеңілдету мақсатында жүйені компоненттерге бөлшектеу процесі

3.2.21 **Айналып өту мүмкін еместігі** (non-bypassability): Қауіпсіздік сәулетінің сипаты, соның салдарынан SFR-мен байланысты барлық әрекеттер TSF орталығына топтасады

3.2.22 **Нысандық аймақтардың бөлінуі** (security domains): Сенімсіз тұлғалардың қолдануына арналған TSF ұсынған орталар,өйткені бұл орталар бір-бірінен оқшауланған және қорғалған болуы тиіс

3.2.23 **Ретті байланыстылық** (sequential cohesion): Функциялары бар модуль, олардың әрбірі [IEEE Std 610.12-1990] модулінде келесі фунцияларға арналған деректерді шығарады

Ескертпе - Ретті байланыстылық модулінің үлгісі аудит жазбаларын фиксациялау функцияларын қамтитын және аудиттің анықталған түріндегі бұзушылықтардың жиналған санының ағымдағы есебін жүргізу.

3.2.24 **Бағдарламалық инженерия** (software engineering): Жүйелі тәртіпті, сандық бағалауға келетін әзірлеу тәсілін және бағдарламалық қамтамасыз етуді қолдауды қолдану; яғни [IEEE Std 610.12-1990] бағдарламалық қамтамасыз етуге инжинирингті қолдану.

Ескертпе - Толықтай инженерлік тәжірибе жағдайында инженерлік принциптерді қолданғанда айқын принциптерге сүйену қажет.Таңдауға тек қана модульдік декомпозиция,қабаттылық, минимизацияшараларын қолдану ғана емес,көп факторлар әсер етеді.Мысалы,әзірлеуші бастапқыда жүзеге асырылмайтын көзделген ұсыныстар системасын /жүйесін/ жобалай алады.

Әзірлеуші осы толық жүзеге аспайтын болашақ жүйені өңдеу үшін кейбір логиканы қосуды таңдай алады; сондай-ақ әзірлеуші кейбір шақыруларды әлі жүзеге аспаған модульдерге,шақыруларға бітеуіш қалдыра отырып қоса алады.Әзірлеушінің негіздемесі жақсы құрылымдық бағдарламалардан ауытқу үшін принциптерді қолдану арқылы бағалануы қажет,сондай-ақ бағдарламалық қамтамасыз етудің әзірлемесіне тиісті шаралар қолданылады.

3.2.25 **Уақытша байланыстылық** (temporal cohesion): Белгілі мерзім ішінде орындалатын функциялары бар модульдің мінездемесі.

Ескертпе
1. [IEEE Std 610.12-1990]-нан бейімделген
2. Уақытша байланыстылық модульдерінің үлгілері инициализация модульдерін,қалпына келтіру мен жұмысты аяқтауды қамтиды.

3.2.26 **TSF-тің өзін-өзі қорғауы** (TSF self-protection): TSF-ті TSF-ке жатпайтын код немесе объектілер зақымдай алмайтын сәулеттік қауіпсіздік құралы.

### 3.3 Басшылық класына қатысты терминдер мен анықтамалар

3.3.1 **Орнату /құру/** (installation): ТОЕ-ге оның операциялық ортасына енетін және оны жұмыс жағдайына ауыстыратын қолданушы орындайтын рәсім

Ескертпе - Бұл операция әдетте бір рет қана орындалады, ТОЕ-ны алуда және қабылдауда қолданылады. ТОЕ-нің ST рұқсат еткен конфигурацияға жететіні күтіледі. Егер осыған ұқсас процестерді әзірлеуші орындаса,өмірлік циклге қолдауды, ALC ішінде «генерация» ретінде белгіленеді. Егер ТОЕ бастапқы іске қосуды талап етсе және оны жүйелі түрде қайталау қажет болмаса,онда бұл процесс орнату немесе құру ретінде жіктеледі.

3.3.2 **Операция** (operation): ТОЕ-ны қолдану кезеңі, «қалыпты қолдануды» қоса, әкімшіліктендіру және ТОЕ-ге жеткізу және дайындаудан кейін қызмет көрсету

3.3.3 **Дайындық** (preparation): өнімнің өмірлік цикл кезеңіндегі қызметі, тапсырыс берушінің ТОЕ-ны қабылдауын және орнатуын қоса, жүктемені, инициализацияны, ТОЕ-ны жұмысқа дайындық жағдайында қосу және жүргізуді қамтиды.

### 3.4 Тіршілік циклін қолдау класына қатысты терминдер мен анықтамалар

3.4.1 **Қабылдау критерийлері** (acceptance criteria): Қабылдау процедураларын орындауда қолданылатын өлшемдер (мысалы, құжаттарды табысты қарау, аппараттық немесе бағдарламалық қамтамасыз етуге негізделген бағдарламалық қамтамасыз ету жағдайында табысты тестілеу)

3.4.2 **Қабылдау процедуралары** (acceptance procedures): жаңадан құрылған немесе конфигурацияның өзгертілген элементтерін ТОЕ-ның бөлігі ретінде қабылдау үшін немесе оларды келесі өмірлік цикл кезеңіне ауыстыруда қолданылатын процедуралар

Ескертпе - Бұл процедуралар қабылдауға, өлшемдерге жауапты тұлғалардың рөлін айқындайды.

Қабылдау жағдаятының бірнеше түрі бар, олардың кейбіреуі бір-бірімен қайшы келуі келуі мүмкін:

a) конфигурацияны басқару жүйесіне объектіні бастапқы қабылдау,атап айтқанда, бағдарламалық қамтамасыз етуді қосу, ТОЕ-ның басқа өндірушілерінің аппараттық компоненттері және тігістері;

b) ТОЕ-ның әрбір құрылым кезеңдерінде конфигурация элементтерінің келесі өмірлік цикл фазасына өтуі (мысалы, модуль, бақылау, ТОЕ-ның дайын сапасын бақылау, ішкі жүйесі);

c) әзірлеменің әр түрлі жақтарының арасындағы конфигурация элементтерін бөлу кезегі (мысалы, ТОЕ-ның бөлімдері немесе алдын-ала өнімдерінің)

d) ТОЕ-ны тұтынушыға жеткізгеннен кейін

3.4.3 **СМ конфигурацияларын басқару** (configuration management): Техникалық және әкімшілік басшылық сондай-ақ конфигурация элементтері мінездемесінің тұлғалық және функционалдық құжаттандыруын және сәйкестендіруді бақылауды жүзеге асыратын шара, бұл мінездемелердің өзгерісін, жазбасын және өзгерісін өңдеу, жүзеге асыру жағдайын, көрсетілген талаптарға сәйкестігін тексеруді бақылайды

Ескертпе - [IEEE Std 610.12-1990]-нан бейімделген

3.4.4 **Құжаттама СМ** (CM documentation): СМ-ның барлық құжаттары жатады, оған СМ-нен шығу, СМ тізімі (конфигурация тізімі), СМ-ның жүйелі жазбасы, СМ-ды қолдану және СМ жоспары бойынша құжаттама кіреді

3.4.5 **Конфигурацияны басқарудың шынайылығы** (configuration management evidence): СМ жүйесінің жұмысының дұрыстығын растау үшін қолданылатын барлық нәрсе

Ескертпе - Мысалы, әзірлеуші ұсынған негіздемелер, СМ-нен шығу, бақылаулар, эксперименттер /тәжірибелер / немесе әзірлеушінің объектіні аралаған кездегі алған сауалнамалары жатады.

3.4.6 **Конфигурациялар бірлігі** (configuration item): ТОЕ-ны әзірлеу кезіндегі СМ жүйесі басқаратын объект

Ескертпе - Бұл ТОЕ-ның бөлімдері,немесе әзірлеменің құралдары және бағалау құжаттары сияқты ТОЕ-ны әзірлеуге байланысты объектілер болуы мүмкін.СМ элементтері тікелей СМ жүйесінде (мысалы, файлдар) немесе өзінің нұсқаларымен бірге сілтемеде (мысалы, жабдықтардың бөліктері) сақталуы мүмкін.

3.4.7 **Конфигурациялар тізімі** (configuration list): Конфигурацияны басқарудың шығару құжаты, онда өнімнің толық нақты нұсқаларына жататын конфигурацияны басқарудың әрбір элементінің нақты нұсқаларымен қоса нақты өнім үшін конфигурация элементтерінің барлығы тізімделген.

Ескертпе - Бұл тізім өнімнің нұсқаларын бағалауға жататын элементтерді өнімнің өзге нұсқаларына жататын, элементтерді өзге нұсқалардан ажыратуға мүмкіндік береді. Конфигурацияны басқарудың соңғы тізімі- бұл нақты өнімнің нақты нұсқаларына арналған нақты құжат. (Әрине, тізім конфигурацияны басқарудың ішкі аспабында электрондық құжат болуы мүмкін,бұндай жағдайда оны жүйеге шығу емес,жүйенің бөлігі ретінде және жүйеге ерекше көзқарас ретінде қарастыру керек.Конфигурация тізімін бағалауды қолдану бағалау құжаттамасының бөлімі ретінде қаралады.) Конфигурация тізімінде конфигурацияны басқару үшін ALC_CMC басқаруындағы элементтер көрсетілген.

3.4.8 **Конфигурацияны басқару нәтижелері** (configuration management output): Конфигурацияны басқару жүйесі енгізген немесе құрған конфигурацияны басқаруға байланысты нәтижелер

Ескертпе - Бұл нәтижелерде конфигурацияны басқарумен байланысты құжаттар түрі болуы мүмкін (мысалы, толтырылған қағаз бланкілер,конфигурацияны басқару жүйесінің жазбалараы,журналдардағы мәліметтер,мөр басылған көшірмелер және электрондық мәліметтер). Конфигурацияны басқарудың мұндай нәтижелерінің үлгілеріне конфигурация тізімдері,конфигурацияны басқару жоспары немесе өнімнің өмірлік циклы барысындағы тәртібі жатады.

3.4.9 **Конфигурацияны басқару жоспары** (configuration management plan): ТОЕ-ге арналған конфигурацияны басқару жүйесін қолданудың сипаттамасы.

Ескертпе - Конфигурацияны басқару жоспары қызметкерлердің нені орындау керектігін анық білуі мақсатында шығарылды.Конфигурацияны басқарудың жалпы жүйесі тұрғысынан бұны шығыс құжаты ретінде қарастыруға болады (өйткені ол конфигурацияны басқару жүйесінің қосымша бөлігі ретінде құрылуы мүмкін). Нақты жобалау тұрғысынан қарағанда бұл құжат қолдану құжаты болып табылады,өйткені жобалық топ мүшелері оны жобалау барысында өздері орындайтын қадамдарды түсіну үшін қолданады. Конфигурацияны басқару жобасы нақты өнімге арналған жүйені қолдануды айқындайды; бұл жүйе өзге өнімдер үшін әр түрлі деңгейде қолданыла алады.Бұл конфигурацияны басқару жоспарында ТОЕ –ны әзірлеу барысында қолданылатын компанияның конфигурациялық басқару жүйесінен шығуды айқындайды және сипаттайды.

3.4.10 **Конфигурацияны басқару жүйесі** (configuration management system): Процедуралар мен құралдар жиынтығы (құжаттаманы қоса алғанда),әзірлеуші өз өнімінің конфигурациясын өмірлік цикл барысында қолдау және өңдеу үшін қолданады.

Ескертпе - Конфигурацияны басқару жүйелерінде қатаңдықтың әр түрлі дәрежесі және функционалдықтар болады.Конфигурацияны басқару жүйесінің жоғары деңгейінде дефектілер жойылып,автоматтандырылады, өзгерісті бақылайды және өзге механизмдерді қадағалайды.

3.4.11 **Конфигурацияны басқару жүйесінің жазбалары** (configuration management system records): Конфигурацияны басқару бойынша маңызды әрекеттерді көрсететін, конфигурацияны басқару жүйесінің жұмысы барысында алынған нәтиже.

Ескертпе - Конфигурацияны басқару жүйесінің жазбаларының үлгілері конфигурацияны басқару элементтерін өзгертудің басқару формалары немесе конфигурацияны басқару элементтерінің бекіту формаларына қол жеткізу болып табылады.

3.4.12 **Конфигурацияны басқару құралдары** (configuration management tools): Конфигурацияны басқару жүйесін қолдайтын немесе жүзеге асыратын қолдан басқарылатын немесе автоматтандырылған құралдар

Ескертпе - Мысалы,ТОЕ бөлімдері нұсқаларын басқаруға арналған құралдар

3.4.13 **Конфигурацияны басқаруда қолданылатын құжаттамалар** (configuration management usage documentation): Конфигурацияны басқару жүйесінің анықтамасы сипатталатын және анықтамалықты,ережелерді немесе құралдар құжаттамалары және процедураларды қолдана отырып пайдалану

3.4.14 **Жеткізу** (delivery): Өндіріс ортасынан дайын ТОЕ-ны тапсырыс берушінің қолына беру

Ескертпе - Өнімнің өмірлік циклының бұл фазасы өзіне қаптама мен әзірлемені орнында сақтауды қамти алады, бірақ аяқталмаған ТОЕ-ны тасымалдауды қамтымайды.

3.4.15 **Әзірлеуші** (developer): ТОЕ –ны әзірлеуге жауапты ұйым.

3.4.16 **Әзірлеме** (development): ТОЕ-ны жүзеге асыруды ұсынуды құрумен байланысты өнімнің өмірлік циклінің кезеңдері

Ескертпе - ALC-тың барлық кезеңіндегі: өмірлік циклды қолдау талаптары,өндіріс пен әзірлемені жалпы мағынада білдіру,әзірлеме және онымен байланысты терминдер.

3.4.17 **Әзірлеме құралдары** (development tools): ТОЕ өндірісі мен әзірлемесін қолдайтын құралдар егер қолданылса, тестілеу бағдарламасын қамтамасыз етуді қосу)

Ескертпе - Мысалы ТОЕ-ны бағдарламалық қамтамасыз ету үшін бағдарламалау тілдері, компиляторлар, компоновщиктер және генерациялайтын құралдар әзірлеме құралдары болып табылады.

3.4.18 **Жүзеге асыруды ұсыну** (implementation representation): TSF-ты абстрактылы ұсыну,оның ішінде TSF-тың өзінің дизайнын нақтылаусыз құруға қолданылатынын жатқызуға болады

Ескертпе - компилирленетін бастапқы код,немесе жабдықтау сызбасы,шынайы жабдықтауды құруға арналып қолданылып жүрген сызба жүзеге асыруды ұсынған бөліктердің үлгісі болып табылады.

3.4.19 **Өмірлік цикл** (life-cycle): Объектінің белгілі уақытта өмір сүру кезеңдерінің реттілігі (мысалы өнімнің немесе жүйенің)

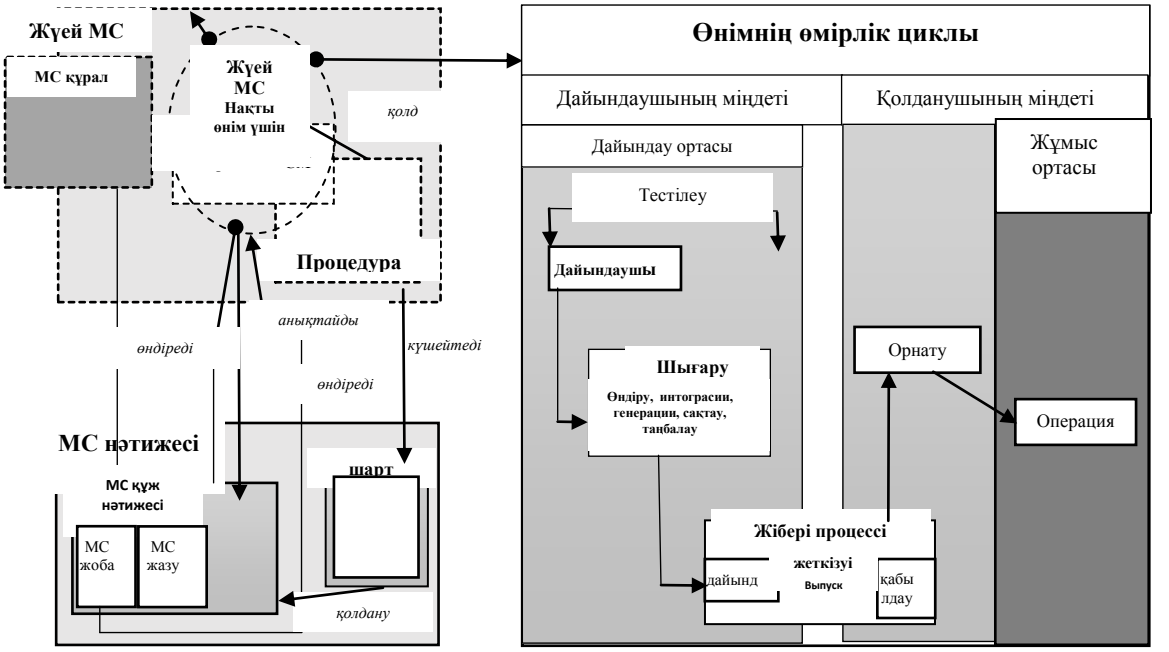
3.4.20 **Өмірлік циклды анықтау** (life-cycle definition ): Өмірлік циклдың моделін анықтау

3.4.21 **Өмірлік цикл моделі** (life-cycle model): Кезеңдерді,олардың өзара байланысын сипаттау, олар нақты объектінің өмірлік циклын басқаруда қолданылады, кезеңдер реттілігін және кезеңдері бар жоғары деңгейлі мінездеулерді сипаттайды

Ескертпе - 1-суретті қараңыз

3.4.22 **Өндіріс** (production): Өндірістің өмірлік циклының фазасы әзірлеме кезеңдерінен кейін керек және ТОЕ-ны іске асыруды әзірлеуде жасалады,өйткені бұл жағдай тапсырыс берушіге жеткізуге қолайлы

Ескертпе – Бұл кезең жасауды, интеграцияны, генерациялауды, ішкі тасымалдауды, ТОЕ-ны сақтау және таңбалауды қамтуы мүмкін.




**1-сурет – СМ және өнімнің тіршілік циклының терминологиясы.**

### 3.5 Осалдылықты бағалау класына қатысты треминдер мен анықтамалар

3.5.1 **Жасырын арна** (covert channel): Қорғалған, көрсетілмеген сигналды канал, ол бөлшектенудің көпдеңгейлі саясатына және ТОЕ бақыланбайтын талаптарына қолданушыға құпия қарсы тұруға мүмкіндік береді.

3.5.2 **Табылған әлеуетті осалдық** (encountered potential vulnerabilities): ТОЕ-ның әлеуетті әлсіз жақтары,оны бағалау әрекеттерін орындау барысында бағалаушы анықтаған, бұлар SFR-ды бұзу үшін пайдаланылуы мүмкін

3.5.3 **Пайдалану осалдығы** (exploitable vulnerabilitiey): ТОЕ-ның әлсіз жақтары, олар ТОЕ-ның жұмыс аясында SFR-ды бұзу үшін қолданылуы мүмкін.

3.5.4 **Мониторингтік шабуылдар** (monitoring attacks): Шабуылдар әдістерінің типтік категориясы, олар пассивті талдау әдістерін қамтиды, бұл әдістер басшылық құжаттамаларымен сәйкес келетін ТОЕ-ны пайдалану арқылы ТОЕ-ның басшылық құжаттарына сәйкес сезімтал ішкі деректерді ашуға бағытталған.

3.5.5 **Потенциалдық осалдық** (potential vulnerabilitiey): Күдікті бірақ расталмаған әлсіз жақ

Ескертпе - Күдік негізінде постулированного жолдары шабуыл бұзу мақсатында SFR-ды бұзу мақсатында постулирленген шабуыл жолдары негізінде күдіктену.

3.5.6 **Қалдық әлсіздігі** (residual vulnerabilitiey): ТОЕ үшін жұмыс аясында қолдануға болмайтын әлсіз жақ,алайда оны ТОЕ үшін жұмыс аясында күткеннен гөрі SFR-ды бұзу үшін шабуылдаушы үлкен әлеует ретінде қолдануға болады.

3.5.7 **Әлсіздік** (vulnerabilitiey): Қандай да бір ортада SFR-ды бұзу үшін қолданылатын ТОЕ-дегі әлсіз жер

**3.6 Композиция класына қатысты терминдер мен анықтамалар**

3.6.1 **База компоненті** (base component): TOE құрамасындағы субъект, оның өзі бағалау нысаны болдыжәне тәуелді компонентке ресурстар мен қызметтерді ұсынды

3.6.2 **Үйлесімді компоненттер** (compatible components): Келісілген жұмыс жағдайында әр компоненттің сәйкес интерфейстері арқылы өзге компоненттің талап етуімен қызметтерді ұсынуға қабілетті компоненттің сипаты

3.6.3 **TOE компоненті** (component TOE): Басқа TOE-ның бөлігі болып табылатын сәтті бағаланған TOE

3.6.4 **Құрамдас TOE** (composed TOE): Бағалаудан сәтті өткенекі немесе одан да көп компоненттен тұратын TOE

3.6.5 **Тәуелді компонент** (dependent component): Өзі бағалау нысаны болып табылатын TOE құрамындағы субъект,ол базалық компонент көмегімен қызметтер туралы ережеге сүйенеді

3.6.6 **Функционалдық интерфейс** (functional interface): Ішкі интерфейс,ол қолданушыға TOE-ның функционалдық мүмкіндіктеріне қол жеткізуді қамтамасыз етеді, өзі қауіпсіздіктің функционалдық талаптарын қамтамасыз етуге тікелей қатыспайды

Ескертпе – TOE құрамы - бұл интерфейстер, оларды базалық компонент ұсынған, өйткені құрамдас TOE-ның жұмысын қолдау үшін тәуелді компоненттен талап етіледі.

**4 Белгілер мен қысқартулар**

API Application Programming Interface – қолданбалы бағдарламалаудың интерфейсі
CAP Composed Assurance Package – кепілдемелердің құрамдас топтамасы
CM Configuration Management – конфигурацияны басқару
DAC Discretionary Access Control – шектеулі қол жетімді бақылау
EAL Evaluation Assurance Level – бағалау кепілдемесінің деңгейі
GHz Gigahertz - гигагерц
GUI Graphical User Interface – қолданушылық графикалық интерфейс
IC Integrated Circuit - интегралды сызба
IOCTL Input Output Control – кіру мен шығуды басқару
IP Internet Protocol - интернет-хаттама
IT Information Technology – ақпараттық технологиялар
MB Mega Byte - мегабайт
OS Operating System – операциялық система /жүйе/
OSP Organisational Security Policy – қауіпсіздік ұйымының саясаты
PC Personal Computer - ПК, дербес компьютер
PCI Peripheral Component Interconnect - периферийлы компоненттерді қосу
PKI Public Key Infrastructure – ашық кілттің инфрақұрылымы
PP Protection Profile - қорғаныс профилі
RAM Random Access Memory – оперативтік есте сақталатын құрылғы
RPC Remote Procedure Call – дистанциондық шақыру процедураларының хаттамасы
SAR Security Assurance Requirement - кепілдік қауіпсіздігінің талабы
SFR Security Functional Requirement – қауіпсіздіктің функционалдық талабы
SFP Security Function Policy –қауіпсіздік функцияларын қамтамасыз ету саясаты
SPD Security Problem Definition – қауіпсіздік проблемаларын анықтау
ST Security Target – қауіпсіздік бойынша тапсырма
TCP Transmission Control Protocol – TCP хаттамасы, алыс-берістің басқарушы хаттамасы
TOE Target of Evaluation – бағалау объектісі

TSF TOE Security Functionality - TOE қауіпсіздігінің функционалдық мүмкіндіктері
TSFI TSF Interface - TSF интерфейсі
VPN Virtual Private Network – виртуальды жеке желі

## 5 Шолу

### 5.1 Жалпы ережелер

Бұл бөлімде ISO/IEC 15408-дің негізгі тұжырымдамалар ұсынылған. Онда тұжырымдамасы анықталды TOE тұжырымдамасы , мақсатты аудитория ISO/IEC 15408-дің мақсатты аудиториясы және ISO/IEC 15408 –дің қалған бөліктеріне материал ұсыну үшін тәсіл анықталды.

### 5.2 Бағалау объектісі (БО)

ISO/IEC 15408 ISO/IEC 15408 бағалау төңірегінде икемділікке ие,сондықтан ол IT өнімдеріне тәуелді емес.Осыған байланысты ISO/IEC 15408-дің бағалау тұрғысында TOE термині қолданылады (бағалау объектісі).

TOE басшылықтың сүйемелдеуінің арқасында бағдарламалық қамтамасыз етудің, аппараттық қамтамасыз етудің жинағы ретінде айқындалады.

Бұл TOE IT –өнімінен құралғандықтан міндетті емес.TOE IT өнімі,IT өнімінің бөлшегі, IT өнімдерінің жинағы,бірегей технология болып табылғандықтан,олардың комбинациясына,өнімдеріне айнала алмайды.

ISO/IEC 15408-ке келетін болсақ, TOE және IT –дің кез келген өнімінің арасындағы нақты қарым-қатынас бір ғана аспектіде маңызды болып саналады:IT өнімінің бөлшегі ғана бар TOE-ның бағасы барлық IT өнімінің бағасы ретінде қарастырылмауы қажет.

TOE үлгілері:

-бағдарламалық қосымша;

-операциялық жүйе;

-операциялық жүйеге сәйкесетін бағдарламалық қосымша;

-операциялық жүйеге және жұмыс станциясына сәйкесетін бағдарламалық қосымша;

-жұмыс станциясымен сәйкесетін операциялық жүйе;

-смарт-карталардың интегралды сызбасы;

-смарт-карталардың интегралды сызбасының криптографиялық сопроцессоры;

-жергілікті желі,оған барлық терминалдар,серверлер,желілік жабдықтау және бағдарламалық қамтамасыз ету жатады;

-әдетте мағлұматтар базасымен байланысты жойылған клиенттің бағдарламалық қамтамасыз етілуінен басқа мағлұматтар базасының қосымшасы.

#### 5.2.1 БО-ның әр түрлі ұсыныстары

ISO/IEC 15408-те TOE бірнеше ұсыныстарды кездестіреді,мысалы (бағдарламалық TOE үшін) :

-конфигурациялық басқару жүйесіндегі файлдар тізімі;

-жаңа ғана скомпилирленген жалғыз көшірме;

-клиентке жіберуге дайын тұрған компакт-диск және пайдалануға арналған басшылық сақталған қорап;

-белгіленген және атқарушы нұсқа.

Бұлардың барлығы TOE болып саналады: ISO/IEC 15408 қалған бөлігінде және барлық жерде қолданылатын TOE термині тұрғысында анықталады.

### 5.2.2 ТОЕ-ның әр түрлі конфигурациялары

IT өнімдері толықтай әр түрлі болуы мүмкін: әр түрлі параметрлері қосылған немесе айырылған,әр түрлі құрылған. ISO/IEC 15408-ді бағалауда ТОЕ-ның айқын талаптарға жауап бере алу немесе алмауы айқындалған,конфигурациядағы бұл икемділік проблемаларға алып келуі мүмкін,өйткені ТОЕ-дегі барлық конфигурациялар талаптарға сай болуы қажет.

Осындай себептерге байланысты ТОЕ-ның басшылық бөлімі ТОЕ-ның конфигурацияларын жиі әрі қатаң шектейді. Бұл ТОЕ басшылығының IT өнімінің жалпы басшылығынан ерекшеленетінін білдіреді. Операциялық жүйенің IT өнімі мұның үлгісі болып табылады. Бұл өнім әр түрлі болуы мүмкін (қолданушылар түрлері,қолданушылар саны,рұқсат етілген және рұқсат етілмеген ішкі қосылулар,қосылған-айырылған опциялар). Егер IT –дің бір өнімі ТОЕ болып табылса және талаптардың жиынтығымен дұрыс бағаланса,онда конфигурация бұдан да қатаң бақылауда болуы қажет,өйткені көптеген опциялар (ішкі қосылудың барлық түрлеріне рұқсат беру немесе жүйелік администраторға аутентификация талап етілмейді). Сол себептен әдетте IT өнімі басшылығы мен ТОЕ басшылығы арасында айырмашылық болды (көптеген конфигурациялар жіберіледі,бір ған және қауіпсіздік тәсілдерінен айырмашылық жоқ конфигурациялар). Егер ТОЕ басшылығы бұрынғыдай бірнеше конфигурацияға рұқсат етсе, онда бұл конфигурациялар толықтай ТОЕ болып аталатынын және осындай конфигурация ТОЕ ұсынған талаптарды қанағаттандыруы қажет екеніне назар аудару қажет.

## 5.3 ISO/IEC 15408 пайдаланушылары

ТОЕ қауіпсіздігін бағалауда жалпы қызығушылық тудыратын үш топ бар: тұтынушы, әзірлеуші және бағалаушылар. ISO/IEC 15408-дің 1 бөлімі ұсынған өлшемдер барлық үш топтың қажеттілігін қолдауға құрылған. Үш топқа арналған өлшемдердің пайдалы жағы келесі параграфтарда түсіндіріледі.

### 5.3.1 Тұтынушылар

ISO/IEC 15408 тұтынушылардың қажеттіліктерін бағалаудың сәйкестігін қамтамасыз ету үшін жазылған, өйткені бұл бағалау процесінің негізі және басты мақсаты. Тұтынушылар нәтижелерді шешім шығару үшін пайдалана алады, ТОЕ олардың қажеттіліктерінің қауіпсіздіктерін қанағаттандыратынын анықтайды. Қауіпсіздік төңірегіндегі бұл қажеттіліктер саясат бағытында тәуекел талдауы нәтижесінде айқындалады. Тұтынушылар әр түрлі ТОЕ-ларды салыстыру үшін бағалау нәтижесін қолдана алады.

ISO/IEC 15408 тұтынушыларға,оның ішінде тұтынушылар топтарына және қауымдастықтарына құрылымды жүзеге асыруға тәуелсіз көзқарас ұстанатындарға PP қорғаныс профилі қауіпсіздік талаптарын нақты айқындап ұсынады.

### 5.3.2 Әзірлеушілер

ISO/IEC 15408 ТОЕ бағалауға көмек көрсетуге және әзірлеушілерді даярлауға қолдау көрсетуге және бұл ТОЕ-лар орындайтын қауіпсіздік талаптарын айқындауға арналған. Бұл талаптар ST қауіпсіздігінің мақсатты тапсырмасында бар және конструкцияны жүзеге асыруға тәуелді.

ST бір немесе бірнеше PP-да құрылуы мүмкін, ТОЕ-ның тұтынушылар қауіпсіздігі талаптарына сай екендігін көрсету үшін ISO/IEC 15408 PP-ларда берілгендей. Сондай-ақ міндеттерді айқындауға және бұл талаптарға қатысты ТОЕ бағасын қолдауға қажетті

дәлелдемелерді ұсыну мақсатындағы әрекеттерді ұсынуға қолданылады. Ол дәлелдемелердің мазмұнын анықтайды және бұл дәлелдемелерді ұсынады.

### 5.3.3 Бағалаушылар

ISO/IEC 15408 құрамында өлшемдер бар, оларды бағалаушылар қолдана ал ТОЕ-ның қауіпсіздік талаптарына сәйкес қалыптасқан талқылауларда қолдана алады.

ISO/IEC 15408 бағалаушы орындауға тиісті жалпы әрекеттер жиынтығын сипаттайды. ISO/IEC 15408 бұл әрекеттерді орындау барысында қажет процедураларды анықтамайтынына назар аударыңыз. Бұл процедуралар туралы мейлінше толық ақпаратты 5.5.-бөлімінен табуға болады.

### 5.3.4 Басқалар

ISO/IEC 15408 ТОЕ –ның IT қауіпсіздік бағалау құралдарына және спецификацияға бағытталған,сондай-ақ ол IT қауіпсіздігіне мүдделі немесе оған жауапты барлық тұлғаларға анықтама материалы ретінде пайдалы болуы мүмкін. ISO/IEC 15408 құрамындағы ақпарат кейбір қосымша мүдделі топтарға пайдалы болып шығуы мүмкін:

a) IT қауіпсіздігі талаптары мен ұйымдасқан саясатты сақтауға және анықтауға жауапты жүйе қауіпсіздігін қамтамасыз ететін ұйымдардың сақтаушылары мен қызметкерлері;

b) IT –шешімі қауіпсіздік деңгейіне жататын бағалауға жауапты ішкі және сыртқы қызмет аудиторлары;

c) IT қауіпсіздік құралдарының спецификациясына жауапты қауіпсіздік жобалаушылары мен сәулетшілер;

d) анықталған ортада қолдануға арналған IT-шешім қабылдауға жауапты аккредиттелген тұлғалар;

e) бағаны қолдау мен сұранысқа жауапты бағалау демеушілері; сондай-ақ

f) IT қауіпсізідігі бағдарламасын бақылау мен басқаруға жауапты бағалаудың өкілетті органдары.

### 5.4 ISO/IEC 15408 әртүрлі бөлімдері

ISO/IEC 15408 төменде көрсетілген бір-бірімен байланысты бөлек жиынтық түрінде ұсынылған.Бөлімдерді сипаттауда қолданылатын терминдердің мәні 6 бөлімде түсіндіріледі.

a) 1-бөлім. ISO/IEC 15408 кіріспесі кіріспе және жалпы модель болып табылады, олар IT қауіпсіздігін бағалау принциптері мен жалпы концепциясын анықтайды және бағалаудың жалпы моделін ұсынады.

b) 2-бөлім. Қауіпсіздіктің функционалдық компоненттері функционалдық компоненттер жиынтығын құрайды,олар стандартты шаблон ретінде қызмет атқарады,оларға ТОЕ-ның функционалдық талаптары негізделген. ISO/IEC 15408 функционалдық компоненттер жиынтығын каталогизрлейді және оларды класс және тұқымдастар түрінде ұйымдастырады.

c) 3-бөлім. Қауіпсіздікті қамтамасыз ету компоненттері сапаны қамтамасыз ететін компоненттер жиынтығын құрайды,олар стандартты шаблондар түрінде қызмет атқарады, оларға ТОЕ үшін кепілдік талаптары негізделеді. ISO/IEC 15408 қамтамасыз ету компоненттерінің жиынтығын каталогтайды, оларды тұқымдастар мен кластарға ұйымдастырады. ISO/IEC 15408 PP мен ST үшін бағалау өлшемдерін анықтайды және алдын ала анықталған жеті қамтамасыз ету топтамаларін ұсынады,олар бағалау

кепілдігінің деңгейі деп аталады (EAL).

Жоғарыда көрсетілген ISO/IEC 15408-дің үш бөліміне қосымша басқа да құжаттар жарияланды. Мысалы, ISO/IEC 18045 негіз ретінде ISO/IEC 15408-ді қолдана отырып, IT қауіпсіздігінің бағалау методологиясын /әдіснамасын/ ұсынады. Басқарушылық құжаттар мен техникалық негіздеме материалдарын қоскқанда басқа да құжаттар жариялануы мүмкін.

1-кестеде ISO/IEC 15408-тің бөлімдеріне қызығушылық тудыратын мақсатты аудиторияның үш тобы ұсынылған.

**1-кесте - «IT қауіпсіздігін қамтамасыз етуді бағалаудың критерийлеріне» жұмыс жоспары**

| Бөлімдер | Тұтынушылар | Әзірлеушілер | Бағалаушылар |
|---|---|---|---|
| 1-бөлім | Негізгі ақпарат ретінде қолданылады және анықтамалық мақсаттарға міндетті. PP басқарушылық құрылымы. | Анықтамалық мақсаттарға жәнеақпараттық анықтамалық үшін қолданылады. TOE үшін қауіпсіздік | PP және ST құрылымына басшылық ретінде және анықтамалық мақсаттарға міндетті түрде |
| 2-бөлім | TOE талаптарын реттеуде анықтама және басшылыққа алуда қолданылады. . | TOE үшін функционалдық спецификацияны реттеу және функционалдық талаптар туралы өтініштерін интерпретациялауда анықтама ретінде міндетті түрде қолданылады. | Функционалдық талаптар өтініштерін интерпретациялауда анықтама үшін міндетті түрде қолданылады. |
| 3-бөлім | Кепілдіктің талап етілетін деңгейін анықтауда басшылық негізінде қолданылады. | TOE-ны бағалауға тәсілдерді анықтауға және кепілдік талаптары туралы өтінішіті интерпретациялауда анықтама ретінде қолданылады. | Кепілдік талаптары туралы өтініштерді интерпретациялауда анықтама ретінде қолданылады.. |

### 5.5 Бағалау мәнмәтіні

Бағалау нәтижелерін көптеп салыстыруға қол жеткізу үшін бағалау беделді сызбалар аясында өткізіледі,бұл стандарттарды белгілейді,бағалау сапасын бақылайды және нормативтік құжаттарды басқарады және оларда бағалау мен бағалаушының құралдары сәйкес болуы тиіс.

ISO/IEC 15408 нормативтік базаға талаптарды белгілей алмайды.Алайда бұндай бағалау нәтижелерін өзара тану мақсатына жету үшін түрлі бағалау органдарының нормативтік-құқықтық базасы арасында келісім талап етіледі.

Бағалау нәтижелерінің басым салыстырмалылығына қол жеткізудің екінші тәсілі бұл нәтижеге жетуге арналған жалпы әдіснаманы пайдалану болып табылады. ISO/IEC 15408үшін бұл әдіснама ISO/IEC 18045-те келтірілген.

Бағалаудың жалпы әдіснамасын пайдалану нәтижелердің объективтілігіне және қайталануына ықпал етеді,бірақ бұл жеткілікті болып табылмайды.Бағалаудың көптеген өлшемдері сараптамалық бағалау мен базалық білімді қолдануды талап етеді,олар үшін келісімге келу оңай емес.Бағалау нәтижелерінің келісімділігін арттыру мақсатында соңғы бағалау нәтижелері сертификаттау процесіне ұсынылуы мүмкін.

Сертификаттау процесі - бұл тәуелсіз тексеру нәтижелерін бағалау,ол әдетте жалпыға бірдей қолжетімді болып табылады.

Сертификаттау процесі IT қауіпсіздік өлшемдерін қолданудағы басым келісімділікке қол жеткізу құралы болып табылады.

Сертификаттаудың процестері мен бағалау сызбалары бағалау жөніндегі органдардың қарамағында болады, олар ISO/IEC 15408 қызметі шеңберіне кірмейді және осындай сызбалар мен процестерді басқарады.

## 6 Жалпы модель

### 6.1 Жалпы модельге кіріспе

Бұл бөлімде осы тұжырымдамалар қолданылуы тиіс мәнмәтінді қоса, ISO/IEC 15408 қолданылатын жалпы тұжырымдамалар және осы тұжырымдамаларды қолдануға ISO/IEC 15408 тәсілімі ұсынылған. ISO/IEC 15408 осы бөлімін пайдаланушыларынан кеңес алуға міндетті ISO/IEC 15408-2 және ISO/IEC 15408-3 осы тұжырымдамалардың қолдануын кеңейтеді және сипатталған тәсілім қолданғанын болжайды. Сонымен қатар, бағалау әрекеттерін жасауға ниетті ISO/IEC 15408 пайдаланушылары үшін ISO/IEC 18045 қолданылады. Бұл бөлім ақпараттық қауіпсіздік туралы біршама білімді талап етеді және осы саладағы оқу құралы ретінде пайдалануға арналмаған.

ISO/IEC 15408 тұжырымдамалар мен қауіпсіздік терминдерін қолдана отырып, қауіпсіздікті қарастырады. Осы тұжырымдамалар мен терминологияны түсіну ISO/IEC 15408 тиімді пайдалану үшін қажетті шарт болып табылады. Алайда, тұжырымдамалар жалпылама болып келеді және ISO/IEC 15408 қолданылатын IT қауіпсіздігі мәселелерінің санатын шектеу үшін арналмаған.

### 6.2 Активтер және контрмерлер

Қауіпсіздік активтерді қорғаумен байланысты. Активтер – әлдекім құндылықтар мәнін беретін объектілер. Активтер мысалдары:

- файл немесе сервер ішіндегісі;
- дауыс беру кезіндегі дауыстардың шынайылылығы;
- электрондық сауда процесіне қол жеткізу;
- қымбат принтерді пайдалану мүмкіндігі;
- құпия нысанға қолжетімділік.

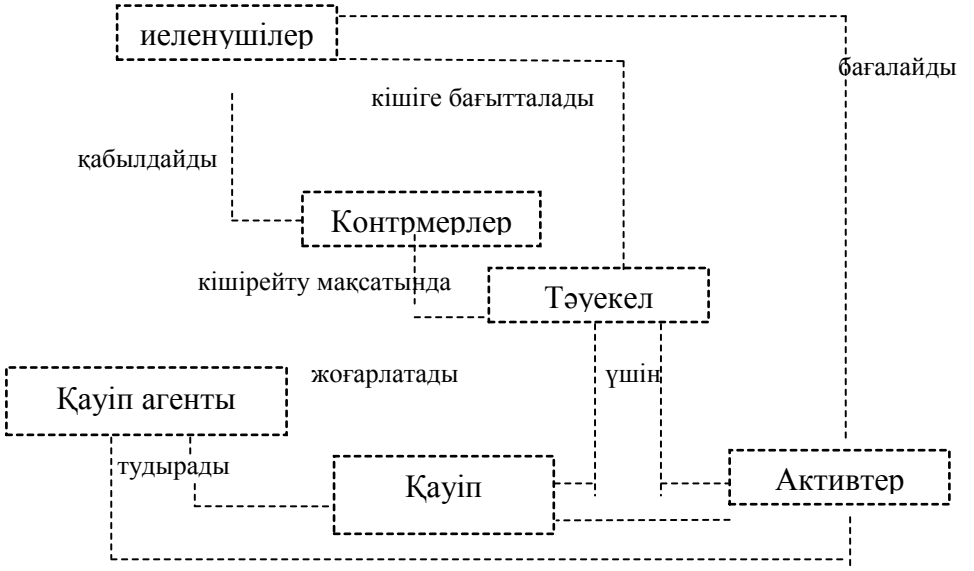
Бірақ, құн – субъективті түсінік екендігін ескерсек, барлық дерлік актив болуы мүмкін.

Осы активтер орналасқан қоршаған орта жұмыс ортасы деп аталады. Жұмыс ортасының мысалдары (аспектілері):

- банктегі компьютер бөлмесі;
- Ғаламторға қосылған компьютерлер желісі;
- LAN;
- жалпы кеңселік орта болып табылады.

Көптеген активтер ақпарат иелерімен белгіленген талаптарға сәйкес сақталатын,

өңделетін және IT-өнімдермен жеткізілетін ақпарат түрінде ұсынылған. Ақпараттар иелері кез келген осындай ақпараттың қолжетімділігі, таратылуы мен өзгеруін қатаң бақыланғанын және активтер қатерлерден қарсы іс-қимыл шараларымен қорғалғанын талап етуі мүмкін. 2 сурет осы жоғарғы деңгей мен байланыс тұжырымдамаларын суреттейді.




**2 сурет – Қауіпсіздік пен байланысты қамтамасыз ету тұжырымдамалары**

Қызығушылық тудыратын активтерді сақтау осы активтердің құнын белгілейтін иелердің міндеті болып табылады. Қатерлердің нақты немесе болжамды агенттері де активтердің құнын белгілей алады және ие мүдделеріне қайшы келетін тәсілмен активтерді теріс пайдалануға ұмтылуы мүмкін. Қатерлер агенттерінің мысалдары: хакерлер, арам ниетті пайдаланушылар, арам ниетсіз пайдаланушылар (кейде қателіктер жасайтын), компьютерлік процестер мен жазатайым жағдайлар.

Активтер иелері осындай қатерлерді активтердің құнсыздану мүмкіндігі деп қабылдайтын болады, сондықтан иелер үшін активтердің құны төмендетілетін болады. Қауіпсіздікпен байланысты құнсыздану әдетте активтердің құпиялылығын жоғалтуды, активтердің тұтастығын жоғалтуды және активтердің қолжетімділігін жоғалтуды қамтиды, бірақ олармен шектелмейді.

Бұл қатерлер қатерлердің іске асу ықтималдығы мен осы қатер іске асқан кездегі активтерге әсерін негізге ала отырып, активтер үшін тәуекелдерді туғызады. Кейіннен активтер үшін тәуекелдерді төмендету үшін қарсы іс-қимыл шаралары қолданылады. Осы қарсы шаралар IT қарсы шараларынан (брандмауэрлар мен смарт-карталар сияқты) және техникалық емес (күзет және рәсімдер сияқты) қарсы шаралардан тұруы мүмкін. Қауіпсіздіктің (бақылаудың) қарсы іс-қимыл шараларын және оларды енгізу мен басқару әдістерін неғұрлым жалпы талқылау үшін сондай-ақ ISO/IEC 27001 және ISO/IEC 27002 қараңыз.

Активтер иелері осы активтер үшін жауапты болуы мүмкін немесе жауапты болады, сондықтан өзінің активтердің қатерлерге ұшырау тәукелдерін қабылдау шешімін қорғау мүмкіндігіне ие болуы тиіс.

Осы шешімді қорғаудағы екі маңызды элемент – ол

- қарсы іс-қимыл шаралары жеткілікті: егер қарсы шаралар өз функцияларын орындаса, онда олар активтер үшін қатерлерге қарсы тұра алады;

- қарсы іс-қимыл шаралары дұрыс: қарсы шаралар мәлімделгенді орындайды

дегенді көрсету мүмкіндігі.

Активтер иелерінің көпшілігіне қарсы шаралардың жеткіліктілігі мен дұрыстығын бағалау үшін қажетті білім, тәжірибе немесе ресурстар жетпейді, және олар тек қарсы шараларды әзірлеушілердің пайымдауларына сүйенгілері келмеуі мүмкін. Сондықтан бұл тұтынушылар осы қарсы шаралардың бағалауына тапсырыс беріп, өздерінің бірнеше немесе барлық қарсы шараларының жеткіліктілігі мен дұрыстығына өзінің сенімділігін арттыруды дұрысырақ көруі мүмкін.


**3 сурет – Бағалау, олардың өзара қарым-қатынастары кезінде қолданылатын түсінік**

### 6.2.1 Контрметр жеткіліктілігі

Бағалау барысында қарсы шаралардың жеткіліктілігі «қауіпсіздік тапсырмасы» деп аталатын құрастырылым көмегімен талданады. Осы тармақшада бұл құрастырылымға қысқартылған көзқарас келтірілген: егжей-тегжейлі және толық сипаттауды А қосымшасында көруге болады.

Қауіпсіздік тапсырмасы активтер мен осы активтерге қатерлерді сипаттаудан басталады. Сосын қауіпсіздік тапсырмасы қарсы шараларды сипаттайды (қауіпсіздік мақсаттары нысанында) және бұл қатерлерге қарсы тұруға осы қарсы шаралар жеткілікті екендігін көрсетеді: егер қарсы шаралар бекітілгенді орындаса, онда қатерлерге қарсылық көрсетіледі.

Кейін қауіпсіздік тапсырмасы осы қарсы шараларды екі топқа бөледі:

a) ТОЕ үшін қауіпсіздік мақсаттары: олар дұрыстығы бағалау кезінде айқындалатын қарсы шараларды сипаттайды;

b) жұмыс ортасы үшін қауіпсіздік мақсатары: олар дұрыстығы бағалау кезінде айқындалмайтын қарсы шараларды сипаттайды;

Осындай бөліністің себептері:

- ISO/IEC 15408 IT қарсы шараларының дұрыстығын сипаттау үшін ғана жарайды. Ал IT жатпайтын қарсы шаралар (мысалы, күзетші-адамдар, рәсімдер) әрдайым жұмыс ортасында болады;

- қарсы шаралардың дұрыстығын бағалау уақытты және ақшалай шығындарды талап

етеді, бұл IT барлық қарсы шараларының дұрыстығын бағалауды мүмкін емес етуі мүмкін;

- IT тарапынан кейбір қарсы іс-қимылдар ықтималдығы басқа бағалау барысында бағаланып қойды. Сондықтан осы дұрыстықты қайта бағалау орынсыз.

TOE үшін (дұрыстығы бағалау кезінде бағаланатын IT қарсы шаралары), қауіпсіздіктің функционалдық талаптарында (SFR) қауіпсіздік мақсаты TOE үшін қауіпсіздік мақсаттарының қосымша егжей-тегжейлілігін талап етеді. Бұл SFR дәлдікті қамтамасыз ету мен салыстырмалықты жеңілдету үшін стандартталған тілде (ISO/IEC 15408-2 сипатталған) тұжырымдалады.

Сонымен, қауіпсіздік тапсырмасы:

- SFR TOE үшін қауіпсіздік мақсаттарына жауап беретіндігін;
- TOE үшін қауіпсіздік мақсаттары мен операциялық орта үшін қауіпсіздік мақсаттары қатерлерге қарсы тұратындығын;
- SFR мен операциялық орта үшін қауіпсіздік мақсаттары қатерлерге қарсы тұратындығын көрсетеді.

Жоғарғылардағыдан мынадай қорытынды шығару керек, дұрыс TOE (SFR талаптарына жауап беретін) дұрыс жұмыс ортасымен үйлестікте (операциялық орта үшін қауіпсіздік мақсаттарына жауап беретін) қатерлерге қарсы тұратын болады. Келесі екі тармақшаларда TOE дұрыстығы мен жұмыс ортасы дұрыстығы туралы мәселе бөлек талқыланатын болады.

### 6.2.2 БО дұрыстығы

Бағалау объектісі қате жобаланып іске асырылуы мүмкін, сондықтан осалдықтарға әкелетін қателіктері болуы мүмкін. Осы осалдықтарды пайдаланып зиянкестер бұрынғыша шығын келтіре және/немесе активтерді теріс пайдалана алады.

Бұл осалдықтар әзірлеу кезінде жіберілген кездейсоқ қателерден, әлсіз дизайннан, зиянды кодтың әдейі қосуынан, сапасыз тестілеуден және т.б. туындауы мүмкін.

БО дұрыстығын анықтау үшін

- БОтестілеу;
- әр түрлі БО жобалық ұсынымдарын зерделеу;
- БО әзірлеу ортасының физикалық қауіпсіздігін зерделеу сияқты әрекеттердің әр түрлі түрлері орындалуы мүмкін.

Қауіпсіздік тапсырмасы қауіпсіздікті қамтамасыз ету талаптары түрінде (SAR) дұрыстығын анықтау үшін осы әрекеттердің құрылымданған сипаттауын қамтамасыз етеді. Бұл SAR дәлдікті қамтамасыз ету мен салыстырмалықты жеңілдету үшін стандартталған тілде (ISO/IEC 15408-3 сипатталған) тұжырымдалған.

Егер SAR сақталса, онда БО дұрыстығына сенімділік орын алады, сондықтан БО-да зиянкестер пайдаланулары мүмкін осалдықтардың болу ықтималдығы аз. БО дұрыстығына кепілдік көлемі SAR өздерімен анықталады: бірнеше «әлсіз» SAR шағын кепілдікке әкелсе, көп «күшті» SAR үлкен кепілдікті қамтамасыз етеді.

### 6.2.3 Жұмыс атқарылу ортасының дұрыстығы

Операциялық орта да қате жобаланып енгізілуі мүмкін, сондықтан осалдықтарға әкелетін қателіктері болуы мүмкін. Осы осалдықтарды пайдаланып зиянкестер бұрынғыша шығын келтіре және/немесе активтерді теріс пайдалана алады.

Бірақ ISO/IEC 15408 жұмыс ортасының дұрыстығына қатысты ешқандай кепілдіктер келтірілмеген. Немесе, басқаша айтқанда, операциялық орта бағаланбайды (келесі бөлікті қараңыз).

Бағалауға қатысты келер болсақ, операциялық орта қауіпсіздік мақсаттарының операциялық орта үшін 100% дұрыс іске асырылуын білдіреді деп тұжырылымдалады.

Бұл БО тұтынушысы өзінің операциялық ортасының дұрыстығын анықтау үшін

- егер БО OS үшін жұмыс ортаның жай-күйі үшін қауіпсіздік мақсаттары «жұмыс ортасы сенімсіз желідегі объектілердің (мысалы, Ғаламтор) БО-ға қолжетімділігін тек ftp арқылы алуды қамтамасыз етуі тиіс» десе, тұтынушы бағаланған желі аралық экранды таңдап, онда тек ftp үшін БО-ға қол жеткізуді баптау;

- егер жұмыс ортасы үшін қауіпсіздік мақсаттары «пайдалану жағдайларымен қамтамасыз етіледі, әкімшілік қызметкерлер тарапынан зиянды әрекеттерге жол берілмейді» десе, тұтынушы зиянды тәртіп үшін айыппұл санкцияларын қосу үшін өзінің байланыстарын әкімшілік қызметкерлермен бейімдеу сияқты басқа әдістерді пайдалану мүмкін дегенді жоққа шығармайды, бірақ бұл анықтама ISO/IEC 15408 бөлігі болып табылмайды.

### 6.3 Бағалау

ISO/IEC 15408 бағалаудың екі түрін мойындайды: төменде сипатталған ST/БО бағалауы, және ISO/IEC 15408-3 айқындалған РР бағалауы. Көп жерлерде ISO/IEC 15408 ST/БО бағалауына сілтеме жасап, «бағалау» терминін (дәрежелеусіз) қолданады.

ISO/IEC 15408 ST/БО бағалау екі кезеңде жүргізіледі:

a) ST бағалауы: БО және жұмыс ортасының жеткіліктілігімен анықталады;

b) БО бағалауы: БО дұрыстығы анықталады. Бұрын айтылғандай, БО бағалауы жұмыс ортасының дұрыстығын бағаламайды.

ST бағалауы қауіпсіздік мақсатына мақсатты қауіпсіздікті бағалау өлшемдерін (ISO/IEC 15408-3 айқындалған) қолдану арқылы жүргізіледі. ASE өлшемдерін қолданудың нақты әдісі бағалаудың қолданыстағы әдіснамасымен анықталады.

БО бағалауы қиынырақ. БО бағалау үшін негізгі бастапқы деректер БО мен ST қамтитын бағалау деректер болып табылады, сондай-ақ әдетте жобалық құжаттар немесе әзірлеушіні тестілеу нәтижелері сияқты әзірлеу ортасының деректерін де қамтиды.

БО бағалауы SAR қолданудан (қауіпсіздік тапсырмасы бойынша) бағалау дәлелдеріне дейін қамтиды. Нақты SAR қолданудың нақты әдісі бағалаудың қолданыстағы әдіснамасымен анықталады.

SAR қолдану нәтижелерін құжаттамалық тіркеу, құрылуы тиіс құжаттар және қандай егжей-тегжейліліктері – қолданыстағы бағалау әдіснамасымен, сонымен қатар жүргізіліп отырған бағалау кестесімен де айқындалады.

БО бағалау процесінің нәтижесі мынадай болуы мүмкін:

- барлық SAR сақталмаған деген пікір, сондықтан ST белгіленгендей БО SFR сәйкес келетіндігіне белгілі кепілдік деңгейі жоқ;

- барлық SAR орындалды деген пайымдау, сондықтан ST белгіленгендей БО SFR барлық талаптарына жауап береді дегенге сенімділіктің белгілі деңгейі бар.

БО бағалау ТОЕ әзірлеуді аяқтағаннан кейін немесе оның әзірленуімен қатар орындалуы мүмкін.

ST/БО бағалау нәтижелерін анықтау әдісі 9 бөлімде сипатталған. Бұл нәтижелер ТОЕ сәйкестігі мәлімделген РР (ларды) және топтаманы (терді) сәйкестендіреді, және бұл құрастырылымдар келесі бөлімде сипатталған.

## 7. Нақты қолдану үшін қауіпсіздік талаптарын оңтайландыру

### 7.1 Операциялар

ISO/IEC 15408 функционалдық қамтамасыз ету мен сапасын қамтамасыз ету Компоненттеры ISO/IEC 15408-2 және ISO/IEC 15408-3 анықтамаларымен дәл сәйкестікте қолданылуы мүмкін, немесе рұқсат етілген операцияларды қолданумен бейімделулері мүмкін. Операцияларды қолданған кезде PP/ST авторына қажеттіліктер осы талапқа байланысты басқа талаптарға байланысты қанағаттандырылуын қадағалау керек. Рұқсат етілген операцияларды келесі жиынтықтан таңдайды:

- итерация: құрауышқа әр түрлі операциялармен бір реттен көп пайдаланылуға рұқсат етеді;
- иелену: өлшемдерді айырықшалауды рұқсат етеді;
- таңдау: тізімдегі бір немесе одан көп тармақты айырықшалауды рұқсат етеді;
- нақтылау: бөлшектерді қосуды рұқсат етеді.

Иелену мен таңдау операцияларына құрауышта көрсетілгенде ғана рұқсат етіледі. Итерация мен нақтылау барлық Компоненттер үшін рұқсат етілген. Операциялар егжей-тегжейлі төмен сипатталған.

ISO/IEC 15408-2 қосымшаларында таңдау мен иеленуді нақты орындалуына қатысты нұсқаулар келтірілген. Бұл басшылық операцияларды қалай аяқтау керектігі туралы нормативтік нұсқауларды қамтиды, және ауытқушылықтар PP/ST авторымен негізделмесе, осы нұсқаулар сақталуы тиіс:

a) «Жоқ» таңдауды аяқтау үшін таңдау ретінде ғана қолжетімді, егер анық көрсетілсе.

Таңдауды аяқтау үшін ұсынылған тізімдер бос болмаулары тиіс. Егер «Жоқ» опциясы таңдалса, таңдаудың қосымша өлшемдері таңдалынбайды. Егер опция ретінде таңдауда нұсқа ретінде «Жоқ» көрсетілмесе, «және» мен «немесе» таңдауда нұсқаларды біріктіруге жол беріледі, егер таңдауда анық «нұсқаның бірін таңдаңыз» делінбесе.

b) Таңдау операциялары қажет болған жерде итерация арқылы бірігуі мүмкін. Бұл жағдайда әрбір итерация үшін таңдалған нұсқаның қолданылуы басқа қайта іріктеудің затымен қиылыспауы тиіс, себебі олар алынып тастауға арналған.

#### 7.1.1 «Итерация» операциясы

Итерация операциясы әр құрауышпен орындалуы мүмкін. PP/ST авторы итерация операциясын бір құрауышқа негізделген бірнеше талаптарды қосу жолымен орындайды. Құрауыштың әр итерациясы иелену мен таңдауды басқа әдіспен орындау арқылы немесе оған басқа әдіспен нақтылауларды қолдану жолымен іске асатын осы құрауыштың барлық басқа итерацияларынан ерекшеленуі тиіс.

Әр түрлі итерациялар анық негіздеме мен осы талаптардың қадағалануын беру үшін ерекше сәйкестендіруге ие болулары тиіс.

Итерация операциясын кейде Компоненттермен пайдалануға болатындығын атай кету керек, сонымен қатар мұнда оларды қайталаудың орнына мәндердің диапазоны немесе тізімімен бірге иелену операциясын да орындауға болады. Бұл жағдайда автор мәндер диапазонының толық негіздемесін қамтамасыз ету қажеттілігін немесе олардың әрқайсысы үшін бөлек қажеттілікті ескере отырып, лайықты баламаны таңдай алады. Автор бұл мәндер үшін жеке хаттамалар талап етілетіндігін естен шығармауы тиіс.

### 7.1.2 Иелену операциясы

Иелену операциясы құрауышта PP/ST авторымен орнатылған өлшемі бар элемент болған кезде орын алады. Өлшем шектелмеген тұрақсыз шама немесе тұрақсыз шаманы белгілі бір мән диапазонына дейін тарылтатын ереже болуы мүмкін.

PP-дағы элемент иеленуді қамтыған кез келген кезде PP авторы төрт әрекеттің бірін орындайды:

a) иеленуді аяқсыз қалдыру. PP авторы PP-да «Сәйкестендірудің сәтсіз талпыныстардың белгілі саны орындалса немесе асырылса, TSF [иелену: әрекеттер тізімі] тиіс» FIA_AFL.1.2 қоса алады.

b) иеленуді орындау. Мысалы, PP авторы PP-да «Сәйкестендірудің сәтсіз талпыныстардың белгілі саны орындалса немесе асырылса, TSF келешекте кез келген затқа сыртқы объектінің байланысу мүмкіндігін болдырмауы тиіс» FIA_AFL.1.2 қоса алады.

c) рұқсат етілген мәндер диапазонын қосымша шектеу үшін иеленуді тарылту. Мысал ретінде PP авторы PP-да «TSF сәйкестендірудің сәтсіз әрекеттерін [иелену: 4 пен 9 арасындағы оң бүтін сан] табуы тиіс» FIA_AFL.1.1 қоса алады.

d) иеленуді таңдауға түрлендіру, осылайша иеленуді тарылту. Мысалы PP авторы PP-да «Сәйкестендірудің сәтсіз талпыныстардың белгілі саны орындалса немесе асырылса, TSF [таңдау жасау: осы пайдаланушыға келешекте кез келген затқа байлануға тыйым салу, әкімшіні хабардар ету] тиіс» FIA_AFL.1.2 қоса алады.

ST-дағы элемент иеленуді қамтыған кезде ST авторы жоғарыда b) көрсетілгендей иеленуді аяқтауы тиіс. ST үшін a), c) және d) нұсқаларына рұқсат етілмейді.

b), c) және d) нұсқаларында таңдалған мәндер иеленумен талап етілген түрге сәйкес болуы керек.

Иелену жиынтықпен (мысалы, субъектілердің) аяқталуға тиіс болса, субъектілер жиынтығын көрсетуге болады, сонымен қатар

- барлық субъектілер;
- X түріндегі барлық субъектілер;
- a субъектісінен басқа барлық субъектілер;
- қандай субъектілер ескерілгендігі белгілі болған уақыт ішінде

сияқты жиынтық элементтері алынуы мүмкін жиынтықтың біршама сипаттамасын.

### 7.1.3 Таңдау операциясы

Таңдау операциясы осы құрауышты бірнеше элементтерден таңдау PP/ST авторымен жасалуы тиіс элементті қамтыған кезде орын алады.

PP-дағы элемент іріктеуді қамтығанда, PP авторы үш әрекеттердің бірін орындай алады:

a) таңдауды орындамай қалдыру;

b) бір немесе одан көп элементтерді бөлу арқылы таңдауды аяқтау;

c) нұсқалардың кейбіреуін жойып, екі немесе одан көбін қалдырып, таңдауды шектеу.

ST-дағы элемент таңдауды қамтыса, ST авторы b) тармағында көрсетілгендей осы таңдауды жасау керек. ST үшін a) және c) нұсқаларына рұқсат етілмейді.

b) және c) тармақшаларында таңдалған зат немесе заттар таңдауға ұсынылған заттардан алынуы тиіс.

### 7.1.4 «Нақтылау» операциясы

Нақтылау операциясын әр талап ету бойынша орындауға болады. PP/ST авторы осы талапты өзгерте отырып, нақтылауды орындайды. Нақтылау үшін бірінші ереже: нақтыланған талапқа жауап беретін TOE PP/ST мәнмәтінінде жалпыланбаған талапқа да қанағат етеді (яғни, нақтыланған талап бастапқы талаптан «қаталдау» болуы тиіс). Егер нақтылау осы талапқа сәйкес келмесе, алынған нақтыланған талап кеңейтілген талап ретінде қарастырылады және тап мұндай болып қарастырылады.

Бұл ережеден жалғыз ерекшелік - PP/ST авторына субъектілердің, объектілердің, операциялардың, қауіпіздік атрибуттарының және/немесе сыртқы объектілердің барлығына емес, бірнешеуіне қолдану үшін SFR нақтылауға рұқсат ету болып табылады.

Алайда бұл ерекшелік сәйкестік мәлімделген PP-дан алынатын SFR тазалауға қолданылмайды; Бұл SFR PP-дағы SFR қарағанда заттардың, объектілердің, операциялардың, қауіпсіздік атрибуттарының және/немесе сыртқы объектілердің азғантай санына қолдану үшін нақтылана алмайды.

Нақтылаудың екінші ережесі: нақтылау бастапқы құрауышпен байланысты болуы тиіс.

Нақтылаудың жеке жағдайы талапқа азғантай өзгерту енгізілгендегі редакторлық пысықтау болып табылады, яғни ағылшын тілінің дұрыс грамматикасына бейілділік себебінен немесе оқырман үшін оны түсініктілеу ету үшін сөйлемді басқаша айту. Бұл өзгерту талаптың мәнін өзгертуге қандай да бір мүмкіндік бермейді.

## 8 Қорғау профильдері мен топтамалары

### 8.1 Кіріспе

Тұтынушылардың мүдделі топтары мен қауымдастықтарға өздерінің қауіпсіздікке мұқтаждықтарын білдіруге мүмкіндік беру мен ST жазылуын жеңілдету үшін ISO/IEC 15408 осы бөлімі екі арнайы кескіндемелерді: топтамалар мен қорғау профильдерін (PP) қамтиды. Келесі екі тармақтарда осы кескіндемелер егжей-тегжейлі сипатталған, содан кейін осы кескіндемелердің қолданылуы туралы бөлім болады.

### 8.2 Топтамалар

Топтама дегеніміз қауіпсіздік талаптарының атаулы жиынтығы. Топтама:

- SFR ғана қамтитын функционалдық топтама, немесе
- SAR ғана қамтитын кепілдіктер топтамасы болуы мүмкін.

SFR және SAR қамтитын аралас топтамаларға жол берілмейді.

Топтама кез келген жақпен анықталуы және қайта қолдану үшін арналуы мүмкін. Осы мақсат үшін ол үйлесімдікте пайдалы және тиімді болатын талаптарды қамтуы тиіс. Топтамалар ірілеу топтамалардың кескіндемесінде, PP мен ST пайдаланылуы мүмкін. Қазіргі кезде топтамаларды бағалау өлшемдері жоқ, сондықтан SFR немесе SAR кез келген жиынтығы топтама бола алады.

Қамтамасыз ету топтамаларының мысалдары ретінде ISO/IEC 15408-3 айқындалған бағалауды қамтамасыз ету деңгейлері (EAL) болып табылады. Осы мақала жазылу сәтіне ISO/IEC 15408 осы нұсқасы үшін функционалдық топтамалар жоқ.

### 8.3 Қорғау профильдері

ST әрдайым нақты БО сипаттаған кезде (мысалы, MinuteGap v18.5 Firewall), PP БО

түрін сипаттауға арналған (мысалы, брандмауэрлердің). Бір РР әр түрлі бағалауларда қолданылатын көптеген әртүрлі ПТ үшін шаблон ретінде пайдаланылуы мүмкін. РР егжей-тегжейлі сипаттамасы В қосымшасында келтірілген.

Жалпы, ST БО-ге талаптарды сипаттайды және осы БО әзірлеушісімен жазылған, ал РР БО түріне жалпы талаптарды сипаттайды, сондықтан әдетте

- БО осы түріне арналған талаптарға қатысты келісімге келуге тырысатын пайдаланушылар қауымдастығымен;
- осы БО үшін минималды базалық деңгейді орнатуды қалайтын БО әзірлеушісі немесе ұқсас БО әзірлеушілерінің тобымен;
- сатып алу процесі шеңберінде өз талаптарын айқындайтын үкімет немесе ірі корпорациямен жазылады.

РР РР-ға ST-нің рұқсат етілген сәйкестік түрін анықтайды. Яғни, РР жай-күйлері (РР сәйкестігін пайымдауда, В.5 қараңыз), ST үшін рұқсат етілген сәйкестік түрлері:

- егер РР қатаң сәйкестікті талап етсе, ST қатаң түрде РР сәйкес болуы керек;
- егер РР дәлелденуші сәйкестік талап етілуі керек деп мәлімдесе, ST қатаң немесе дәлелденуші түрде РР сәйкес келуі тиіс.

Қайталай отыра, басқаша айтқанда, егер РР анық түрде рұқсат етсе, ST РР-ға көрнекілік түрде сәйкес болуына жол беріледі.

Егер ST бірнеше РР-ға сәйкестігі туралы мәлімдесе, ол осы РР бекіткен тәртіпте әр РР-ға сәйкес болуы тиіс (жоғарыда сипатталғандай). Бұл ST бірнеше РР қатаң сәйкестендіріледі және басқа РР бұл айқын дегенді білдіреді.

ST қарастырылып отырған РР не сәйкес келеді, не сәйкес келмейтіндігіне назар аударыңыз. ISO/IEC 15408 «ішінара» сәйкестікті мойындамайды. Осыған байланысты РР авторы РР сәйкестігі туралы РР/ST авторларына тыйым сала отырып, РР аса ауыртпалықты болмауын қамтамасыз етуіне жауапты болады.

Егер:

- ST жауап беретін барлық БО РР-ға да сәйкес болса, және
- РР сәйкес келетін барлық операциялық орталар ST сәйкес келетін болса,

ST баламалы немесе РР-ға қарағанда шектеулі болып келеді.

Немесе, ресми түрде емес, ST БО-ға бірдей немесе артық шектеулер қояды және сол немесе одан кем шектеулерді БО операциялық ортасына қояды.

Бұл ортақ пайымдауды ST әр түрлі тармақшалары үшін нақтырақ етіп жасауға болады:

a) қауіпсіздік мәселелерін анықтау: ST сәйкестік негіздемесі ST қауіпсіздік мәселесін анықтау РР қауіпсіздік мәселесін анықтауға қарағанда баламалы (немесе шектеулі) екендігін көрсетуі тиіс. Бұл:

- ST қауіпсіздік мәселесін анықтауды қанағаттандыратын барлық БО РР қауіпсіздік мәселесін анықтауға да жауап беретіндігін;
- РР қауіпсіздік мәселесін анықтауды қанағаттандыратын барлық операциялық орталар ST қауіпсіздік мәселесін анықтауға да жауап беретіндігін білдіреді.

b) қауіпсіздік мақсаттары: ST сәйкестік негіздемесі ST қауіпсіздік мақсаттары РР қауіпсіздік мақсаттарына қарағанда баламалы (немесе шектеулі) екендігін көрсетуі тиіс. Бұл:

- ST қауіпсіздік мақсаттарына жауап беретін барлық БО РР қауіпсіздік мақсаттарына да жауап беретіндігін;
- РР қауіпсіздік мақсаттарына жауап беретін барлық операциялық орталар ST операциялық жүйелері үшін де қауіпсіздік мақсаттарына жауап беретіндігін білдіреді.

Егер қорғау профильдеріне қатаң сәйкестік көрсетілсе, онда келесі талаптар қолданылады:

a) қауіпсіздік мәселесін анықтау:

- ST PP қауіпсіздік мәселесін анықтауды қамтуы тиіс және қосымша қатерлер мен OSP көрсете алады; Ол PP-да анықталған келесі екі маркада түсіндірілгендей екі ықтимал ерекшеліктермен барлық болжамдарды қамтуы тиіс,

- егер PP-да анықталған осы жорамалды (немесе болжамның бөлігін) жолдайтын жұмыс ортасы үшін барлық қауіпсіздік мақсаттары ST-да БО үшін қауіпсіздік мақсаттарымем ауыстырылса, PP-да көрсетілген жорамал (немесе болжамның бөлігі) ПБ-дан алынып тасталуы мүмкін,

- егер жаңа жорамал PP-да БО үшін қауіпсіздік мақсаттарын шешуге арналған қатерді (немесе қатердің бөлігін) азайтпаса, және егер Бұл жорамал PP-да БО үшін қауіпсіздік міндеттерін шешуге арналған OSP (немесе OSP бөліктеріне) сәйкес келмесе, жаңа жорамал PP-да айқындалған ST-дағы жорамалдар жиынтығына қосылуы мүмкін;

b) қауіпсіздік мақсаттары: ST:

- PP БО-сі үшін барлық қауіпсіздік мақсаттарын қамтуы тиіс, бірақ БО үшін қосымша қауіпсіздік мақсаттарын көрсетуі мүмкін;

- келесі екі тармақта түсіндірілгендей, екі ерекшеліктерді қоспағанда, PP-да анықталғандай, операциялық орта үшін барлық қауіпсіздік мақсаттарын қамтуы тиіс;

- PP-дағы операциялық орта үшін анықталған мақсаттар ST-да БО үшін қауіпсіздік мақсаттары болып табылатындығын көрсетуі мүмкін. Бұл қауіпсіздік мақсаттарын қайта тағайындау деп аталады. Егер қауіпсіздік мақсаты БО-да қайта орнатылса, қауіпсіздік мақсаттарының негіздемесі жорамал немесе болжамның қандай бөлігі енді қажет еместігін анық көрсетуі тиіс;

- егер жаңа мақсаттар PP-да БО қауіпсіздік міндеттерін шешуге арналған қатерді (немесе қатердің бөлігін) азайтпаса, және егер жаңа мақсаттар PP-да ТОЕ қауіпсіздік міндеттерін шешуге арналған ПБП (немесе ПБП бөлігін) орындамаса, операциялық орта үшін қосымша мақсаттар көрсетуі мүмкін;

c) қауіпсіздік талаптары: ST PP-да барлық SFR және SAR қамтуы тиіс, бірақ қосымша немесе иерархиялық тұрғыда әлділеу SFR мен SAR талап етуі мүмкін. ST операцияны аяқтау PP-дағы әрекеттермен келісілген болуы тиіс; Немесе бір аяқтау ST мен PP қолданылатын болады, өз кезегінде бұл талапты шек қоятын етеді (нақтылау ережелері қолданылады).

Егер қорғау профильдеріне айқын сәйкестік көрсетілсе, онда келесі талаптар қолданылады:

- ST неліктен ST PP-ға қарағанда «баламалы немесе одан гөрі шектеулі» болып саналатындығына негіздемені қамтуы тиіс;

- көрсетілген сәйкестік PP авторына шешілуі тиіс жалпы қауіпсіздік мәселесін сипаттауға, және рұқсат етуді анықтаудың бірден көп тәсілі барын біле тұра оны рұқсат ету үшін қажетті талаптарға ұсыныстар беруге мүмкіндік береді.

PP бағалауы міндетте болып табылмайды. Бағалау оларға ISO/IEC 15408-3 тізілген APE өлшемдерін қолдану арқылы жүргізіледі. Осындай бағалаудың мақсаты: PP толық, бірізді және техникалық негізделгендігін және басқа PP немесе PP жасау үшін үлгі ретінде қолдану үшін жарайтындығын көрсету.

Бағаланатын PP-дағы PP/ST негізделе отырып, екі артықшылықты көруге болады:

- PP қателер, екі ұштылықтар мен ақтаңдақтар болуының аз тәуекелділігі бар. Егер жаңа ST жазу немесе бағалау кезінде анықталған PP байланысты қандай да бір мәселелер (осы PP бағалау кезінде анықталуы ықтимал) табылып жатса, PP түзетуге дейін едәуір уақыт өтуі мүмкін.

- жаңа PP/ST бағалау бағаланған PP бағалауының нәтижелерін қайта қолданыла алады, өз кезегінде бұл жаңа PP/ST бағалау үшін аз құш салуға әкеледі.

### 8.4 PP және топтамаларды пайдалану

Егер ST өзінің бір немесе бірнеше топтамаларға және/немесе қорғау профильдеріне сәйкестігін мәлімдесе, осы ST бағалау (осы ST басқа қасиеттері ішінде) ST шынымен осы ST сәйкес олар мәлімдеген топтамаларға және/немесе PP сәйкес екендігін көрсетеді. Осы сәйкестікті анықтау туралы егжей-тегжейлі ақпарат А қосымшасында келтірілген.

Бұл келесі процесті шешуге мүмкіндік береді:

a) ақпараттық қауіпсіздік өнімінің белгілі түрін сатып алуға тырысатын ұйым PP-да қауіпсіздік қажеттілігін дамытады, сосын оны бағалап, жариялайды;

b) әзірлеуші осы PP алып, PP сәйкестігі туралы мәлімдейтін ST жазады және осы ST бағаға ие болады;

c) сосын әзірлеуші БО құрады (немесе барын пайдаланады) және оның ЗБ байланысты бағалайды.

Нәтижесінде әзірлеуші оның БО ұйымның қауіпсіздік талаптарына сай екендігін дәлелдей алады: сондықтан ұйым БО сатып ала алады. Мұндай ойлау желісі топтамаларға қолданылады.

### 8.5 Көп нұсқалы қорғау профильдерін қолдану

ISO/IEC 15408 сондай-ақ PP-ға басқа PP сәйкес болуына, әрқайсысы алдыңғысына (ларға) негізделген PP тізбегін құруға мүмкіндік береді.

Мысалы, интеграл сұлбасы үшін PP мен смарт-карталардың ОЖ үшін PP алып, оларды екеуіне де сәйкес келетіндігін пайымдайтын смарт-картаның PP (ИС мен ОЖ) құру үшін пайдалануға болады. Сосын Smart Card PP мен аппретті жүктеу PP негізінде қоғамдық көлік үшін смарт-карталарда PP жазуға болады. Ең соңында, әзірлеуші осы қоғамдық көліктің PP үшін смарт-карталар негізінде ST құра алады.

## 9 Бағалау нәтижелері

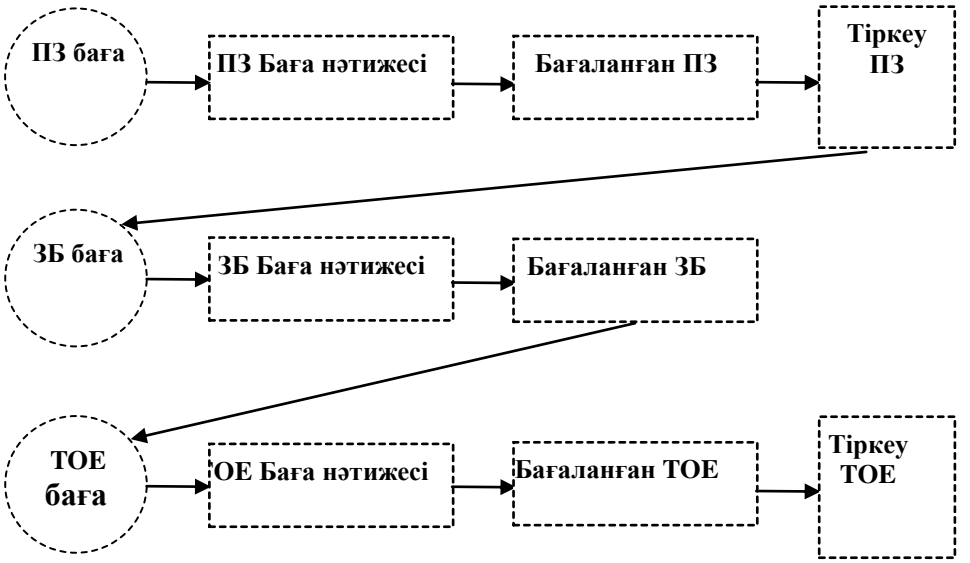
### 9.1 Кіріспе

Бұл бөлімде ISO/IEC 18045 сәйкес орындалған PP және ST/TOE бағалауларының болжалды нәтижелері келтірілген.

PP бағалаулары бағаланған PP тізімдемесіне әкеледі.

ST бағалауы БО бағалау шеңберінде қолданылатын аралық нәтижелерге әкеледі.

ST/TOE бағалаулары бағаланған БО тізімдемесіне әкеледі. Көп жағдайларда осы тізімдемелер нақты БО-ға емес, БО-дан өндірілетін IT-өнімдерге жатқызылады. Сондықтан тізімдемеде IT-өнімнің болуы барлық IT-өнім бағаланған дегенді білдіреді деп түсіндірілмеуі тиіс; Оның орнына ST/БО бағалауының нақты дәрежесі ST анықталады. Кітапханалар мысалдары библиографияда келтірілген.




**4 сурет – Бағалау нәтижелері**

ST бағаланған РР немесе бағаланбаған РР топтамаларіне негізделген болуы мүмкін – алайда ол міндетті емес, себебі ST бір нәрсеге мүлдем негізделмеуі тиіс.

Қауіпсіздікті бағалау нәтижелерін ұсыну үшін абсолюттік объективті шкала болмаса да, бағалау дәлелдеме ретінде келтірілуі мүмкін объективті және қайталанатын нәтижелерге әкелуі тиіс. Бағалау өлшемдерінің жиынтығының болуы мәнді нәтижеге әкелу үшін бағалауға қажетті алдын ала шарт болып табылады және бағалау органдары арасында бағалау нәтижелерін өзара мойындау үшін техникалық негізді қамтамасыз етеді.

Бағалау нәтижесі БО қауіпсіздігінің қасиеттерін зерттеудің белгілі түрінің нәтижелерін ұсынады. Мұндай нәтиже қосымшаның қандай да бір нақты ортасында пайдалану үшін автоматты жарамдылығына кепілдік бермейді. БО-ні нақты қолданбалы ортада пайдалану үшін шешімді қабылдау бағалау нәтижелерін қоса отырып, қауіпсіздіктің көптеген мәселелерін қарауға негізделген.

### 9.2 РР бағалауының нәтижелері

ISO/IEC 15408-3 бағалаушы РР толық, бірізді және техникалық негізделгендігін және ST әзірлеу кезінде пайдалану үшін қолайлы екендігін көрсету үшін кеңес беруге міндетті бағалау өлшемдерін қамтиды.

Бағалау нәтижелері сондай-ақ «Сәйкестік талаптарын» қамтуы тиіс (9.4 қараңыз).

### 9.3 ST/ТОЕ бағалауының нәтижелері

ISO/IEC 15408-3 бағалаушы ST-да ТОЕ SFR-ды қанағаттандыратындығына жеткілікті сенімділік бар болуын анықтау үшін кеңес беруге міндетті бағалау өлшемдерін қамтиды. Сондықтан ТОЕ бағалауы ЗБ үшін өту/жоқтығы туралы пайымдауға әкелуі тиіс. Егер ST бағалау да, ТОЕ бағалау да өткелді жасауға әкелсе, онда негізгі өнім тізілімге қосыла алады. Сондай-ақ бағалау нәтижелері келесі тармақшада айқындалғандай «Сәйкестік талаптарын» қамтуы тиіс.

Бағалау нәтижелері кейіннен сертификаттау процесінде пайдаланылады, бірақ бұл сертификаттау процесі ISO/IEC 15408 шеңберіне кірмейді.

### 9.4 Сәйкестікті бекіту

Сәйкестік талаптары оның бағалауынан өткен PP немесе ST қанағаттандырылатын талаптарды жинау көздерін көрсетеді. Бұл сәйкестіктер шағымы ISO/IEC 15408 сәйкестік талаптарын қамтиды:

a) PP немесе ST шағымдары қойылатын ISO/IEC 15408 нұсқасын сипаттайтын;

b) ISO/IEC 15408-2 (қауіпсіздіктің функционалдық талаптары) талаптарына сәйкестікті сипаттайтын:

- ISO/IEC 15408-2 сәйкестігі. PP немесе ST ISO/IEC 15408-2 сәйкес, егер осы PP немесе ST барлық SFR ISO/IEC 15408-2 функционалдық Компоненттерына негізделген болса, немесе

- ISO/IEC 15408-2 кеңейтілген – PP немесе ST ISO/IEC 15408-2 сәйкес кеңейтілген болса, егер осы PP немесе ST кем дегенде бір SFR ISO/IEC 15408-2 функционалдық Компоненттерына негізделген болмаса

c) ISO/IEC 15408-3 (қауіпсіздікті қамтамасыз ету талаптары) талаптарына сәйкестікті сипаттайтын:

- ISO/IEC 15408-3 сәйкес. Егер осы PP немесе ST барлық SAR ISO/IEC 15408-3 тек қамтамасыз ету компоненттерына негізделген болса, PP немесе ST ISO/IEC 15408-3 сәйкес немесе

- ISO/IEC 15408-3 кеңейтілген. – PP немесе ST ISO/IEC 15408-3 сәйкес кеңейтілген, егер осы PP немесе ST кем дегенде бір SAR ISO/IEC 15408-3 кепілдік Компоненттерына негізделмесе.

Сәйкестік туралы талап топтамаларға қатысты өтінішті қамтуы мүмкін, мұндай жағдайда ол келесілерден тұрады:

- топтаманың аты Conformant. PP немесе ST алдын ала анықталған топтамаға сәйкес келеді (мысалы, EAL), егер:

- осы PP немесе ST SFR топтамасындағы SFR бірдей немесе

- осы PP немесе ST SAR топтамасындағы SAR бірдей.

- топтаманың аты Augmented - PP немесе ST – бұл алдын ала анықталған топтаманың кеңейтуі, егер:

- осы PP немесе ST SFR топтамасындағы барлық SFR қамтыса, бірақ кем дегенде бір қосымша SFR немесе иерархиялық тұрғыдан алғанда топтамасындағы SFR-дан жоғары бір SFR болса.

Осы PP немесе ST SAR топтамасындағы барлық SAR қамтыса, бірақ кем дегенде бір қосымша SAR немесе иерархиялық тұрғыдан алғанда топтамасындағы SAR-дан жоғары бір SAR болса.

TOE осы ST үшін сәтті бағаланған жағдайда ST сәйкестігінің кез келген пайымдаулары сондай-ақ TOE үшін де орынды екендігін атай кету керек. TOE, мысалы, ISO/IEC 15408-2 сәйкес болуы мүмкін.

Сәйкестік туралы шағым сондай-ақ қорғау профильдеріне қатысты екі өтінішті қосуы мүмкін:

a) PP Conformant - PP немесе TOE сәйкестік нәтижесінің бөлігі ретінде тізімделген белгілі PP сәйкес келеді.

b) сәйкестік туралы өтініш (тек PP үшін). Бұл пайымдау PP немесе ST осы PP сәйкес болуы тиіс тәсілді сипаттайды: қатаң немесе дәлелденуші. Осы Сәйкестік туралы келісім жайында қосымша ақпаратты алу үшін В қосымшасын қараңыз.

### 9.5 ST/БО бағалау нәтижелерін пайдалану

ST және БО бағалағаннан кейін активтердің иелері БО жұмыс ортасымен бірге

қатерлерді есептейтіндігіне кепілдікке ие бола алады (ST айқындалғандай). Бағалау нәтижелері қатерлерге активтерді ашу тәуекелді қабылдау туралы шешімді қабылдау кезінде активтердің иелерімен қолданылуы мүмкін.

Актив иесі:

a) ST қауіпсіздік мәселесінің анықтауы актив иесінің қауіпсіздік мәселесімен сәйкес келетіндігін;

b) актив иесінің операциялық ортасы ST сипатталған Операциялық орта үшін қауіпсіздік мақсаттарымен сәйкес келетіндігін (немесе келісу мүмкіндігін) мұқият тексеру қажет.

Егер олай болмаса, БО актив иесінің мақсаттары үшін жарамсыз болып қалуы мүмкін.

БО бағаланғаннан кейін БО-да бұрын белгісіз болған қателердің немесе осалдықтардың пайда болуы мүскін. Бұл жағдайда әзірлеуші БО түзете алады (осалдықтарды жою үшін) немесе осалдықты бағалау облысынан шығару үшін ST өзгерте алады. Қандай да болсын жағдайда бағалаудың ескі нәтижелері жарамсыз болып қалуы мүмкін.

Егер сенімді қалпына келтіру қажетті деп саналса, қайта бағалау қажет. ISO/IEC 15408 осы қайта бағалау үшін қолданылуы мүмкін, бірақ қайта бағалаудың егжей-тегжей рәсімдері ISO/IEC 15408 осы бөлімінің шегінен шығуда.

**А қосымшасы**
(*ақпараттық*)

## Қауіпсіздік тапсырмаларының спецификациясы

### А.1 Осы қосымшаның мақсаты мен құрылымы

Осы қосымшаның мақсаты – қауіпсіздік тұжырымдамасын (ST) түсіндіру. Бұл қосымшада ASE өлшемдері айқындалмаған; Бұл анықтаманы ISO/IEC 15408-3 табуға болады және библиографияда келтірілген құжаттармен расталады.

Бұл қосымша төрт негізгі бөліктен тұрады:

a) ST қамтуы тиіс. Бұл А.2-де жинақталып, одан әрі егжей-тегжейлі А.4 – А.10-да сипатталған. Бұл тармақшалар ST міндетті мазмұнын, осы құрамдас арасындағы өзара байланысты сипаттайды және мысалдар келтіреді.

b) ST-ді пайдалану. Бұл А.3-те жинақталып, одан әрі егжей-тегжейлі А.11-де сипатталған. Бұл тармақшалары сипаттайды, қалай пайдалану керек ST, және кейбір мәселелер болады жауап беру арқылы ST.

c) сенімінің төмен деңгейі. Сенімі төмен дәрежелі ST – бұл мазмұны төмендетіл ST. Олар А. 12-де егжей-тегжейлі сипатталған.

d) стандарттарға сәйкес келген бекіту. ST авторының БО белгілі бір стандартқа сәйкес келеді деп айтуы мүмкіндігі А.13-те сипатталған.

### А.2 ST міндетті мазмұны

А.1 суретте ISO/IEC 15408-3-те келтірілген ST міндетті мазмұны бейнеленген. А.1 суреті сондай-ақ ST құрылымдық жоспары ретінде пайдаланылуы мүмкін балама құрылымдар жіберіледі. Мысалы, егер қауіпсіздік талаптарының негіздемесі ерекше үлкен болса, ол қауіпсіздік талаптарының тақырыпшасына емес, ST қосымшасына енгізілуі мүмкін. Жеке ST тақырыпшалар және осы тармақшалардың құрамы төменде баяндалып, одан әрі егжей-тегжейлі А.4 - А.10-да түсіндіріледі. Әдетте ST құрамында келесілер қамтылады:

a) абстракцияның әртүрлі деңгейіндегі БО үш сипаттамалық сипаттау қамтитын ST жүргізу;

b) талап сәйкестікті көрсету, сәйкес келеді ме, ST талаптарына сәйкес кез-келген PP және/немесе топтамалар, егер қандай PP және/немесе топтамасына;

c) қауіпсіздік проблемасын айқындау, қауіп, OSP мен жорамалдарды көрсету;

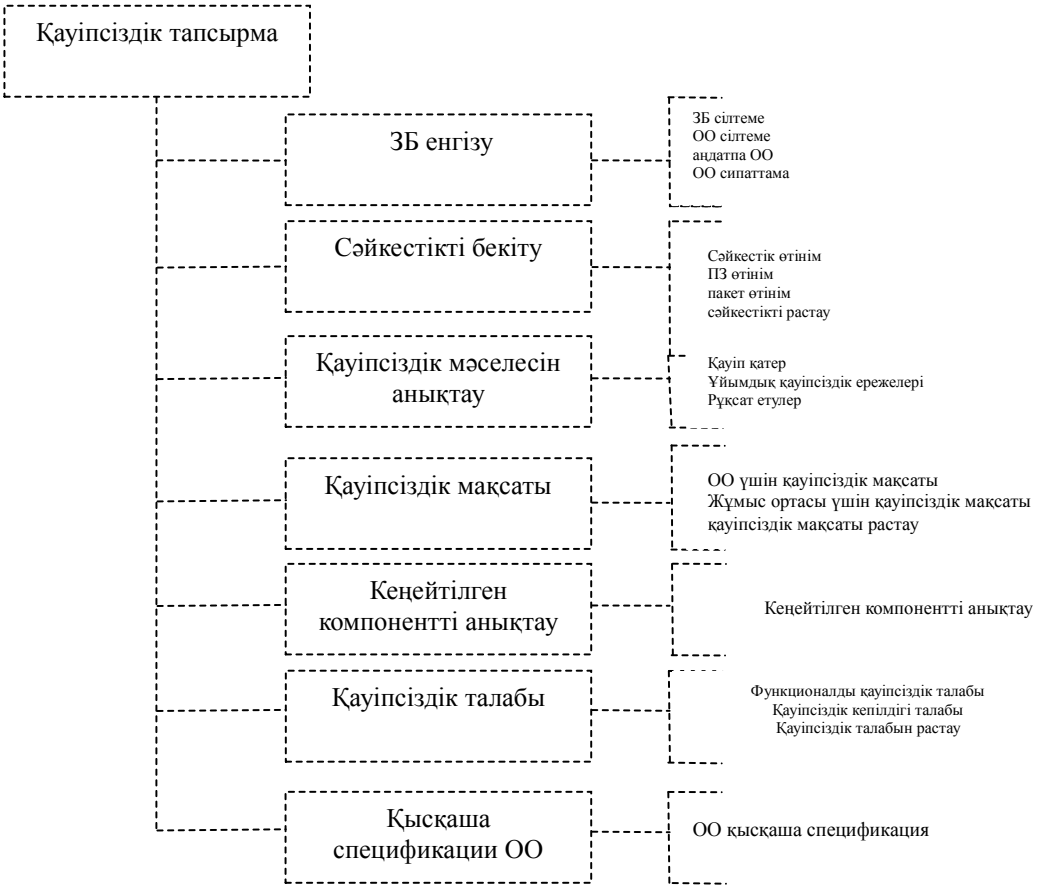
d) қауіпсіздік мақсатына көрсететін шешімі қауіпсіздік мәселелері арасында бөлінеді мақсаттары үшін қауіпсіздік БО және қауіпсіздік мақсаттары үшін операциялық ортаны БО;

e) компоненттерін (міндетті емес) кеңейтілген анықтамасы, онда жаңа компоненттері (яғни ISO/IEC 15408-2 немесе ISO/IEC 15408-3 енгізілмеген) болуы мүмкін. Бұл жаңа компоненттер дұрыстығын қамтамасыз етудің кеңейтілген функционалдық және кеңейтілген талаптарын анықтау үшін қажет;

f) қауіпсіздік талаптары, олар БО-ге арналған қауіпсіздік мақсаттарын стандартталған тілге аударуды қамтамасыз етеді. Бұл стандарт тілі SFR нысанына ие. Сонымен қатар, бұл тармақшада SAR анықталады;

q) SFR –дың БО-де іске асырылуын көрсететін БО жиынтық ерекшелігі.

Сондай-ақ, төмен мазмұнға ие сенімділігі төмен дәрежелі ST болады; Олар А.12-де егжей-тегжейлі сипатталған. Осы қосымшаның барлық қалған бөліктері толық мазмұнды ST-ді көздейді.




**А.1 суреті – Қауіпсіздік тапсырмасының мазмұны**
**Қауіпсіздік тапсырмасы**

## А.3 ST-ді пайдалану

### А.3.1 ST қалай пайдаланылуы тиіс

Типтік ST мынадай екі рөлді атқарады:

- бағалауға дейін және кезінде ST «бағалануға тиістіні» анықтайды. Бұл рөлін ST әзірлеуші мен бағалаушы арасында келісу үшін БО қауіпсіздіктің нақты қасиеттеріне және бағалаудың нақты көлеміне қатысты негіз болып табылады. Техникалық дұрыстығы мен толықтығы маңызды мәселелері болып табылады рөлі үшін. А.7 ST осы рөлде пайдаланылуы тиіс екенін сипаттайды.

- ST бағалаудан кейін «бағаланғанды» көрсетеді. Бұл рөлде ST БО әзірлеуші немесе қайта сатушы және БО әлеуетті тұтынушы арасындағы келісім үшін негіз болып табылады. ST БО нақты қорғаудың абстрактілі қасиеттерін сипаттайды, және әлеуетті тұтынушы бұл сипаттамаға арқа сүйей алады, өйткені БО ST сәйкестігі үшін бағаланды. Пайдаланудың қарапайымдылығы мен түсініктілігі – осы рөл үшін негізгі проблема. А.11 ST осы рөлде қалай пайдаланылуы тиістігін сипаттайды.

### А.3.2 ST қалайша пайдаланылмауы тиіс

ST мынадай екі рөлді (көптің арасында) орындауы тиіс емес:

- егжей-тегжейлі ерекшелігі: ST - бұл абстракцияның салыстырмалы түрде жоғары деңгейдегі қауіпсіздік ерекшелігі. ST, әдетте, хаттаманың егжей-тегжейлі ерекшеліктерін, алгоритмдер және/немесе механизмдердің егжей-тегжейлі сипаттамасын, егжей-тегжейлі операциялардың егжей-тегжейлі сипаттамасын және т. б.қамтуы тиіс емес.

- толық ерекшелігі: ST - бұл жалпы сипаттама емес, қауіпсіздік ерекшелігі. Егер қауіпсіздікке қатысы болмаса, интероперабельділік, физикалық өлшемдері мен салмағы, талап етілетін кернеу және т. б сияқты қасиеттер ST бөлігі болуы тиіс. Бұл, жалпы жағдайда ST толық ерекшеліктің өзі емес, толық ерекшеліктің бөлігі болуы мүмкін.

### А.4 ST жүргізу (ASE_INT)

ST жүргізу БО-ді нарративнті нысанда абстракцияның үш деңгейде сипаттайды:

a) ST жататын ST және БО үшін сәйкестендіру материалды қамтамасыз ететін ST сілтемесі және БО сілтемесі;

b) БО қысқаша сипатталатын БО шолу;

c) БО-ді егжей-тегжейлі сипаттайттын БО сипаттамасы.

### А.4.1 ST анықтамасы және TOE анықтамасы

ST бұл нақты ST сәйкестендіретін ST-дің нақты сілтемесін қамтиды. ST-дің типтік сілтемесі баспа атауынан, нұсқадан, авторларынан және жарияланған күннен тұрады. «MauveRAM ST деректер базасы, 1.3 нұсқа, MauveCorp Specification Team, 2002 жылғы 11 қазан» ST сілтемесінің үлгісі болып табылады.

ST сондай-ақ ST сәйкестігі туралы хабарлайтын БО сәйкестендіретін БО сілтемесін қамтиды. БО типтік сілтемесі әзірлеуші атынан, БО атауынан және БО нұсқасы нөмірінен тұрады. «MauveCorp MauveRAM Database v2.11» БО сілтемесінің үлгісі болып табылады. Өйткені бір БО бірнеше рет бағалануы мүмкін, мысалы, бұл БО-нің әр түрлі тұтынушыларымен, сондықтан бірнеше ST-ге ие, бұл сілтеме бірегей болып табылмайды.

Егер БО бір немесе бірнеше жақсы танымал өнімдерден құралса, өнім атауына (атауларына) сілтеме жасай отырып, оған бұны БО сілтемесінде көрсетуге рұқсат берілген. Алайда, бұл тұтынушыларды адастыру үшін пайдаланылмауы тиіс: ахуалдың қауіпсіздіктің негізгі компоненттері немесе қызметтері бағалау кезінде ескерілмеген, бірақ БО сілтемесі бұны көрсетпеген жағдайға осы жол берілмейді.

ST сілтемесі және БО сілтемесі ST және БО индексациясы мен байлауын және оларды БО/өнім бағаланатын тізімі ақпарына қосуды жеңілдетеді.

### А.4.2 БО-ге аннотация

БО-ге аннотация БО-дің әлеуетті тұтынушылардың бағытталған, олар қауіпсіздікте олардың қажеттіліктерін қанағаттандыруы мүмкін БО табу үшін бағаланған БО/Өнімдердің тізімін қарайды және олардың аппараттық қамтамасыз ету, бағдарламалық қамтамасыз етумен және микробағдарламамен қолдаунат алады. Әдеттегі ұзындығы шолу БО – бірнеше абзацтарын.

Осы мақсатта БО аннотациясында БО және оның негізгі қауіпсіздік функцияларын пайдалану қысқаша сипатталады, БО түрі анықталады және БО талап етілетін БО қатысы жоқ кез келген негізгі аппараттық/бағдарламалық/бағдарламалық/аппараттық құралдар анықталады.

### А.4.2.1 БО қауіпсіздік бөлігінде негізгі сипаттамалар және пайдалану

БО қауіпсіздігін пайдалану және негізгі функцияларды сипаттамасы қауіпсіздік тұрғысынан БО қамтамасыз ете алатыны және оның қауіпсіздік мағынасында пайдаланылуы мүмкіндігі туралы жалпы түсінік беру үшін арналған. Бұл тарауша БО пайдалануды және БО тұтынушылар түсінетін тілді пайдалана отырып, қауіпсіздіктің негізгі функцияларын бизнес-операциялар тұрғысынан сипаттайтын БО (потенциалды) тұтынушылар үшін жазылуы тиіс.

«MauveCorp MauveRAM Database v2.11» бұның мысалы болып табылады – бұл желілік ортада пайдалануға арналған бірнеше рет пайдаланылатын деректер базасы. Ол бір мезгілде белсенді пайдаланушыларға 1024 мүмкіндік береді. Ол құпия сөзді/токен және биометрикалық аутентификацияны пайдалануға мүмкіндік береді, деректердің кездейсоқ бүлінуінен қорғайды және он мың транзакцияны домалатуы мүмкін. Оның аудит функциялары оңай реттеледі, бұл басқа пайдаланушылар мен транзакцияның құпиялылығын қорғай отырып, кейбір пайдаланушылардың және транзакция үшін егжей-тегжейлі аудит жүргізуге мүмкіндік береді .

### А.4.2.2 БО түрі

БО шолуда: брандмауэр, VPN-брандмауэр, смарт-карта, криптомодем, интранет, веб-сервер, дерекқор, веб-сервер және деректер базасы, ЖЕЖ, ЖЕЖ веб-сервер және мәліметтер базасын және т. б. сияқты БО жалпы түрі анықталады

Мүмкін, бұл БО оңай қол жетімді түрі болып табылмайды, және бұл жағдайда «жоқ» қолайлы болар еді.

Кейбір жағдайларда БО түрі тұтынушыларды жаңылыстыруы мүмкін. Мысалдар мыналарды қамтиды:

- БО-ден оның БО түрі үшін белгілі бір функционалдық мүмкіндіктерді күтуге болады, бірақ БО осы функционалдылығына ие емес. Мысалдар мыналарды қамтиды:

- сәйкестендіру/аутентификацияның ешқандай функцияларын қолдамайтын банкоматтық картаның БО түрі;
- дерлік барлық жерде қолданылатын хаттамаларды қолдамайтын БО түрінің брандмауэрі;
- сертификаттың күші жойылған функционалдығы жоқ PKI үлгідегі БО.
- БО белгілі бір операциялық орталарда оның БО түрі үшін жұмыс істейді деп күтуге болады, бірақ ол жасай алмайды. Мысалдар мыналарды қамтиды:
- егер компьютерде желілік қуат, флоппи-дисковод, CD/DVD-плеер болмаса, сенімді жұмыс істей алмайтын ДК операциялық жүйе түрі;
- бұл брандмауэр арқылы қосыла алатын барлық пайдаланушылар болса, сенімді жұмыс істей алмайтын брандмауэр жоғары сапалы болып табылады.

### А.4.2.3 БО құрамына кірмейтін қажетті аппараттық құралдар/бағдарламалық жасақтама/бағдарламалық-аппараттық құралдар

Кейбір БО басқа IT-ге сенім артпайды, көптеген БО (әсіресе бағдарламалық БО) қосымша, БО емес, аппараттық құралдарға, бағдарламалық қамтамасыз етуге және/немесе тігуге сенім артады. Соңғы жағдайда БО шолу БО жатпайтын бағдарламалық қамтамасыз етудің және/немесе тігудің осындай жабдықты сәйкестендіру үшін қажет. қосымша аппараттық қамтамасыз етудің, бағдарламалық қамтамасыз етудің және/немесе тігудің толық және егжей-тегжейлі сәйкестендіруі талап етілмейді, бірақ БО пайдалану үшін

қажетті негізгі аппараттық қамтамасыз ету, бағдарламалық қамтамасыз ету және/немесе тігуді анықтау үшін, сәйкестендіру әлеуетті тұтынушылар үшін толық және жеткілікті толық болуы тиіс.

Аппараттық/бағдарламалық қамтамасыз ету/тігуді сәйкестендіру мысалы:

- 1 ГГц немесе одан жоғары процессор стандартты ДК және Yaiza операциялық жүйесінің 3.0 Update 6b, с немесе 7 немесе версия 4.0512 басқаруындағы жұмыс істейтін МБ немесе одан көп көлемді ОЗУ;
- 1 ГГц немесе одан жоғары нұсқасы процессорлы стандартты ДК және Yaiza операциялық жүйесінің 3.0 Update 6d басқаруындағы жұмыс істейтін 512 МБ немесе одан көп көлемді ОЗУжәне WonderMagic 1.0 1.0- WM драйверлі видеокарта;
- 3.0 ОС (немесе одан жоғары) Yaiza ДК нұсқасы стандартты;
- интегралды схема CleverCard SB2067;
- QuickOS v2.0операциялық жүйесінің басқаруымен жұмыс істейтін CleverCard SB2067;
- 2002 жылдың желтоқсанында Жол қозғалысы департаментінің бас директорының LAN Кеңсесін орнату.

### А.4.3 БО сипаттамасы

БО сипаттамасы - бірнеше бетте жұмыс істей алатын БО суреттемелік сипаттамасы. БО сипаттамасы бағалаушыларға және әлеуетті тұтынушыларға БО қауіпсіздік мүмкіндіктері туралы жалпы түсінік БО шолуда ұсынылғанына қарағанда, егжей-тегжейлі беруі тиіс. БО сипаттамасы БО орналысатын қосымшалардың одан әрі кең тұрғыда сипаттау үшін пайдаланылуы мүмкін.

БО сипаттамада БО физикалық саласы: БО құрайтын аппараттық құралдар, тігу, бағдарламалық қамтамасыз ету мен басшылық бөлімдерінің барлық тізімі талқыланады. Бұл тізім нақтылау деңгейінде сипатталған болуы тиіс, оның сол бөліктер туралы оқырманға жалпы түсінік беруге жеткілікті.

БО сипаттамада сонымен қатар, БО логикалық саласын талқылау керек: БО талдап тексеру деңгейінде ұсынылатын қауіпсіздіктің логикалық функциялары, оның оқырманға осы функциялар туралы жалпы түсінік беруге жеткілікті. Бұл сипаттамасы БО шолуда сипатталған қауіпсіздіктің негізгі функцияларына қарағанда егжей-тегжейлеу болады деп күтіледі.

Физикалық және логикалық салалардың БО-ді сипаттайтыны, БО белгілі бір бөлігі немесе функциясы орналасқаны немесе БО-ге жатпайтын бұл бөлігі немесе функциясы олардың маңызды қасиеті болып табылады. Бұл БО байланысып, БО жатпайтын объектілерден оңай бөлектенуі мүмкін кезде әсіресе маңызды.

Мысалдар БО қатысы жоқ объектілерімен БО байланысады:

- БО IC смарт-карталар криптографиялық сопроцессоры, бүкіл АЖ емес болып табылады;
- БО - бұл IC смарт-карта, криптографиялық процессорды қоспағанда;
- БО MinuteGap Firewall v18.5 желілік мекенжайлардың трансляция бөлігі болып табылады тарату.

### А.5 Сәйкестікті бекіту (ASE_CCL)

Бұл ST тармақшасында ST сәйкес келетіні сипатталады:

- осы стандарттың 2-бөлім мен 3-бөлім;

- қорғау бейіндері (егер бар болса);
- топтамалар (егер бар болса).

ST-дің ISO/IEC 15408 сәйкес келетінің сипаттамасы екі тармақтан тұрады: ISO/IEC 15408 нұсқасы, ол ST қауіпсіздіктің кеңейтілген талаптарын қамтып, пайдаланыла ма немесе жоқ па (қараңыз: А. 8).

ST-дің қорғау бейініне сәйкестіктігін сипаттау ST сәйкестігі мәлімделген топтамаларды аударатынын білдіреді. Бұны түсіндіру үшін 9.4-ті қараңыз.

ST топтамаға сәйкестіктін сипаттау ST сәйкестігі мәлімделген топтамаларды аударатынын білдіреді. Бұны түсіндіру үшін 9.4-ті қараңыз.

### А.6 Қауіпсіздік мәселелерін анықтау (ASE_SPD)

#### А.6.1 Кіріспе

Қауіпсіздіктің мәселелерін анықтау жойылатын қауіпсіздік мәселесін анықтайды. ISO/IEC 15408 қатысты қауіпсіздіктің мәселелерін анықтау аксиоматикалық болып табылады. Яғни, кауіпсіздіктің мәселелерін анықтау процесі ISO/IEC 15408 стандартының шегінен шығады.

Дегенмен, бағалау нәтижелерінің тиімділігі ST-ға өте бағынышты, ал ST тиімділігі қауіпсіздік мәселелерін анықтау сапсына өте бағынышты екенін атап өту қажет. Сондықтан, қауіпсіздік мәселелеріне жақсы анықтама алу үшін бірқатар ресурстарды жиі жұмсап, дұрыс анықталған процестер мен талдауларды пайдалану керек.

ISO/IEC 15408-3 сәйкес, барлық тармақшаларда бекітулердің болуы міндетті емес, қауіпі бар ST-нің OSP және керісінше болуы міндетті емес екеніне назар аударыңыздар. Бұдан басқа, кез келген ST болжамды болуы мүмкін.

Сондай-ақ, БО физикалық түрде бөлінген кезде, БО операциялық ортасының жеке салалары үшін тиісті қауіптерді, ОСП және болжамдарды талқылау дұрыс болатын шығар.

#### А.6.2 Қауіп-қатерлер

Бұл тармақшада қаупсіздік мәселелері анықталған, қауіп-қатерлер көрсетілген, БО қарсы тұруға тиіс, оның жұмыс ортасы немесе екеуінің комбинациясы.

Қауіп-қатер - бұл активке қауіп-қатердің агентінің қолайсыз әрекетінде болып тұр

Қолайсыз әрекеттер - бұл активтердің қауіп-қатеріне қарсы агенті жасаған әрекеттер.

Бұл әрекеттер актив құндылығын алатын активтің бір немесе бірнеше қасиеттеріне әсер етеді.

Қауіптер агенттері бөлек нысандар ретінде сипатталуы мүмкін, бірақ кейбір жағдайларда оларды объектілердің түрі, объектілер тобы және т.б. сипаттауы мүмкін.

Қауіпті агенттердің мысалдары хакерлер, пайдаланушылар, компьютерлік үрдістер және апаттар болып саналады.

Қауіпті агенттерді тәжірибе, ресурстар, мүмкіндіктер және мотивация сияқты аспектілермен сипаттауға болады.

Қауіптердің мысалдары:

- Хакер (тәжірибесі мол, стандартты жабдықтары бар және бұл үшін төленеді) компания желісінен құпия файлдарды қашықтан көшіреді;
- Құрт ғаламдық желінің өнімділігін айтарлықтай төмендетеді;
- Жүйелік администратор пайдаланушы құпиялылығын бұзады;
- Интернеттегі біреу құпия электрондық хабарламаларды тыңдайды.

### А.6.3 (OSP) қауіпсіздікті ұйымдастыру саясаты

Бұл тармақшада OSP қауіпсіздік мәселелері анықтамасы көрсетілген, БО-ны әрекетке әкелетін, оның операциялық ортасы немесе екеуінің комбинациясы.

OSP – бұл қауіпсіздік ережесі, процедура немесе нұсқаулық, қазір мәжбүр етілген (немесе мүмкін мәжбүр етілген ) немесе болашақта жұмыс ортасындағы нақты немесе гипотетикалық ұйым. БО операциялық ортаны бақылайтын ОСП-ны ұйымы белгілейді, немесе олар заңнамамен белгіленеді немесе органдар реттейді. БО-ға OSP-ны немесе БО жұмыс ортасына қолдануға болады.

OSP мысалдары:

- Үкіметтің барлық өнімдері парольдерді генерациялау және шифрлаудың ұлттық стандартына сәйкес келуі тиіс;
- Бөлімнің файлдық сервері тек жүйелік администратордың артықшылықтарымен және бөлімнің құпиялылығымен пайдаланушылар үшін ғана басқарылуы мүмкін.

### А.6.4 Болжам

Қауіпсіздік мәселесінің анықтамасының осы тармағы қауіпсіздік жұмысын қамтамасыз ету үшін жұмыс ортасында жасалған жорамалды көрсетеді. Егер БО осы жорамалдарға сәйкес келмейтін операциялық ортада орналастырылса, БО өзінің барлық қауіпсіздігін қамтамасыз ете алмауы мүмкін.

Функционалдар. Болжамдар физикалық, кадрлық және операциялық өзара әрекеттесуге негізделуі мүмкін.

Жорамалдар мысалдары:

- Жұмыс ортасының физикалық аспектілеріне қатысты болжамдар:
- БО электромагниттік сәулеленуді барынша азайтуға арналған бөлмеде орналастырылатын болады деп болжануда;

БО әкімшісінің консольдері шектелген қатынас аймағында орналасатын болады деп болжануда.

- Жұмыс ортасының штаттық аспектілері туралы болжам:
- БО пайдаланушылары БО-ны басқару үшін жеткілікті дайындықтан өтеді деп болжануда;
- БО пайдаланушылары Ұлттық құпия ретінде жіктелген ақпарат үшін бекітілген деп болжануда;
- БО қолданушылары өздерінің құпия сөздерін жазбайды деп болжануда.

Жұмыс ортасының аспектілері туралы болжам:

- БО-ны іске қосу үшін кем дегенде 10 ГБ дискілік кеңістігі бар ПК жұмыс станциясы қол жетімді деп болжануда;
- БО - бұл жұмыс станциясында жұмыс істейтін операциялық жүйе жоқ жалғыз қосымшалар деп болжануда;
- БО сенімді емес желіге қосылмайды деп болжануда.

Бағалау кезінде бұл жорамалдар шынайы болып саналады: олар қандай да бір жолмен сыналмайды.

Осы себептерге байланысты жорамалдар өндіріс ортасында ғана жасалуы мүмкін.

БО-ға қатысты болжамдар ешқашан қабылданбайды, себебі, бағалау БО-ға қатысты жасалған мәлімдемелерді бағалаудан тұрады және БО-дағы мәлімдемелердің шын екендігін болжайды.

### А.7 (ASE_OBJ) Қауіпсіздік мақсаттары

Қауіпсіздік мақсаттары - қауіпсіздік проблемасын анықтаумен анықталған мәселеге бағытталған шешімнің қысқаша және дерексіз нұсқауы.

Қауіпсіздік мақсаттарының рөлі үш есе:

- мәселені жоғары деңгейде және табиғи тілде шешуді қамтамасыз ету;
- бұл шешімді екі бөлек шешімдерге бөлу, бұл әртүрлі субъектілер мәселенің бір бөлігін шешуге тиіс екендігін көрсетеді;
- бұлны жартылай шешу мәселені толық шешетінін көрсетіңіз.

#### А.7.1 Жоғары деңгейдегі шешім

Қауіпсіздік мақсаттары шамадан тыс қысқа және айқын анықтамалар жиынтығынан тұрады, олар қауіпсіздік мәселесі бойынша жоғары деңгейдегі шешім болып табылады.

Қауіпсіздік мақсаттарына қол жеткізу деңгейі ТОЕ-ны жақсы білетін әлеуетті пайдаланушылар үшін түсінікті және түсінікті болуға бағытталған. Қауіпсіздік мақсаттары табиғи тілде ұсынылады.

#### А.7.2 Жартылай шешімдер

ST-де қауіпсіздікті қамтамасыз ету мақсатында, қауіпсіздік себептері бойынша сипатталғандай шешімі екі бөлікке бөлінеді.

Қаіпсздік мақсатында сипатталып көрсетілгендей, ST-де жоғары деңгейдегі қауіпсіздік шешімі екі бөлікке бөлінген. Бұл жартылай шешімдер ТОЕ үшін қауіпсіздік мақсаттары және операциялық орта үшін қауіпсіздік мақсаттары деп аталады.

Бұл дегеніміз, бұл жартылай шешімдер екі түрлі ұйымдармен қамтамасыз етілуі тиіс: ТОЕ және операциялық ортасы.

#### А.7.2.1 БО үшін қауіпсіздік мақсаттары

Қауіпсіздік мәселесінің анықтамасымен анықталатын, БО мәселесінің белгілі бір бөлігін шешу үшін қауіпсіздік функцияларын қамтамасыз етеді.

Бұл жартылай шешім БО үшін қауіпсіздік мақсаттары деп аталады және бірқатар тапсырмалардан тұрады

БО үшін қауіпсіздік мақсаттарының мысалдары:

- БО өзі мен сервер арасында берілетін барлық файлдардың мазмұнын құпия сақтауыға тиіс;
- БО ұсынатын Қызметке кіруге рұқсат беру үшін, БО барлық пайдаланушыларды анықтап, түпнұсқалығын растауы керек:

ST-ның 3-қосымшсында сипатталғандай, деректерге қол жеткізу саясатына сәйкес БО пайдаланушылардың деректерге қол жеткізуін шектеуі керек;

Егер БО физикалық түрде таратылса, мұны көрсету үшін БО қауіпсіздік мақсаттары бар СТ тармақшаларын бірнеше тармақшаларға бөлуге болады.

#### А.7.2.2 Жұмыс ортасы үшін қауіпсіздік мақсаттары

БО-ға оның қауіпсіздік мүмкіндіктерін дұрыс қамтамасыз етуге көмектесу үшін (олар БО-ның қауіпсіздік мақсаттарымен болып анықталады), БО жұмыс істеу ортасы техникалық және іс жүргізу шараларын қамтиды.

Бұл жартылай шешім операциялық орта үшін қауіпсіздік тапсырмалары деп аталады

және операциялық орта жететін мақсаттарды сипаттайтын пікірлер жиынтығынан тұрады.

Жұмыс ортасы үшін қауіпсіздік мақсаттарының мысалдары:

- Операциялық жүйе БО-ны орындау үшін Linux 3.01b нұсқасымен жұмыс станциясын қамтамасыз етуі керек;

- БО-мен жұмыс істеуге рұқсат берместен бұрын, БО-ның барлық пайдаланушылары тиісті оқытудан өтуіне пайдалану шарттары кепілдік беруі тиіс;

- БО-ның пайдалану шарттары БО-ға, әкімшілік персонал мен қызмет көрсетуші персоналға, бірге жүретін әкімшілік персоналға физикалық қол жеткізуді шектейді;

- БО генерацияланған, оларды орталық аудит серверіне жібермес бұрын, операциялық орта аудит журналдарының құпиялылығын қамтамасыз етеді,

- Егер олардың әрқайсысы әр түрлі қасиеттерге ие БО операциялық жүйесі бірнеше сайттардан тұрса, мұны көрсету үшін операциялық ортаның қауіпсіздік мақсаттары бар СТ тармақшаларын бірнеше тармақшаларға бөлуге болады.

### А.7.3 Қауіпсіздік мақсаттары мен қауіпсіздік мәселелерінің анықтамалары арасындағы байланыс

ST сонымен қатар, екі тармақшасы бар қауіпсіздік мақсаттарының негіздемесін қамтиды:

- қандай қауіпсіздік мақсаттарына назар аударатындығын, қандай қауіптерді, OSP-ді және жорамалдарды көрсететінін қадағалау;

- барлық қауіп-қатерлерді, OSP және болжамдарды қауіпсіздік мақсаттарымен тиімді түрде шешетінін көрсететін негіздемелер жиынтығы.

#### А.7.3.1 Қауіпсіздік мақсаттары мен проблемаларды анықтауды қадағалау

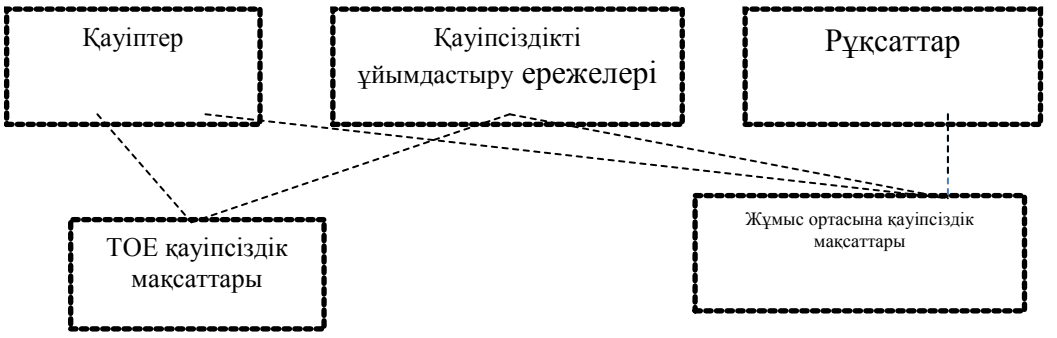
Қауіпсіздік мәселесінің анықтамасында сипатталғандай OSP және рұқсаттамаларға, қадағалау қауіпсіздік мақсаттарының қауіптерге қалай жіберілетінін көрсетеді.

Тексеру қауіпсіздікті қамтамасыз ету міндеттерін қауіпсіздік мәселесінің анықтамасында сипатталғандай қауіптерге, OSP және жорамалдарға қалай жіберілетінін көрсетеді.

a) Жанама мақсаттары жоқ: әрбір қауіпсіздік мақсаты кем дегенде бір қауіппен, ПБП немесе рұқсаттамамен бақыланады

b) Қауіпсіздік мәселесінің анықтауға толық қатысты: әрбір қауіп, OSP және шешімдерде кемінде бір қауіпсіздік мақсаты бар7

c) Түзете жол тарту: жоспарлар әрдайым жасалғандықтан, операциялық ортада БО кем дегенде бір қауіпсіздік мақсатын көздейді, БО болжамды ескермейді. ISO/IEC 15408-3, рұқсат етілген жол тартулар А.2 суретте көрсетілген.




**А.2-сурет – Қауіпсіздік мақсаттары мен қауіпсіздік проблемаларын анықтауды қадағалау**

Қауіпсіздіктің бірнеше мақсаттарын бірдей қауіппен бақылауға болады, осы қауіпсіздік мақсаттарының тіркесімі осы қауіпке қарсы тұратынын көрсетеді.Осындай дәлел OSP және жорамалдар үшін жарамды.

### А.7.3.2 Іргелестіруге логикалық негіздеме беру

Қауіпсіздік мақсаттарының негіздемесі сондай-ақ қадағалаудың тиімді екендігін көрсетеді: егер белгілі бір қауіпті қадағалайтын барлық қауіпсіздік мақсаттары болса, ПБ немесежорамалға қол жеткізілсе, барлық көрсетілген қауіптер, ПБП және болжамдар қарастырылады (яғни қарсы тұрады, тиісінше сақталады және қолдау көрсетіледі),

Бұл демонстрация қатерлерге қарсы тұрудың тиісті қауіпсіздік мақсаттарына қол жеткізудің әсерін талдайды, ПБП талаптарының сақталуын қамтамасыз ету және жорамалдарды қолдау және бұл шынымен де осылай деген қорытындыға әкеледі.

Кейбір жағдайларда, қауіпсіздік проблемаларын анықтау бөліктері қауіпсіздік мақсаттарының кейбіріне өте жақын болғанда, демонстрация өте қарапайым болуы мүмкін. Қауіп мысалы:

«Т17: Х қауіп агенті А және В арасындағы көшу кезінде құпия ақпаратты оқиды, БО үшін қауіпсіздік мақсаттары: «ОТ 12: БО А және В арасында жіберілген барлық ақпараттың құпия екенін қамтамасыз етуі керек», А демонстрациялау «Т17 ОТ-12-мен тікелей қарама-қарсы»

### А.7.3.3 Қатерлерге қарсы тұру туралы

Қауіп-қатерге қарсы тұру, бұл қауіпті жоюды білдірмейді, бұл сондай-ақ осы қауіптің жеткілікті азайту дегенді білдіреді.

Қауіптерді жоюдың мысалдары:

- қауіпті агентті қолайсыз әрекет ету мүмкіндігін болдырмау;
- осылайша активті ауыстыру, өзгерту немесе қорғау, осы қолайсыз әрекеттер оған қолданылмайтын ету;
- қауіпті агентті жою (мысалы: көбінесе желіде ақаулық әкелетін компьютерлерді желіден алып тастау).

Қауіпті төмендету мысалдары:

- қауіп-қатердің агентінің қолайсыз әрекеттер жасауға қабілеттілігін шектеу;
- қауіпті агентті қолайсыз әрекет ету мүмкіндігі шектеу;
- қолайсыз әсерлерді табысты орындау мүмкіндігін азайту;
- қауіпті агентті қолайсыз әрекет ету үшін ынталығын төмендету;
- қауіпті агенттерден көп тәжірибе немесе үлкен ресурстарды талап ету.

Қауіптің салдарын төмендету ммысалдары::

- активтіңрезервты көшірмесінің жиілігі;
- активтің резервтік көшірмелерін алу;
- мүлікті сақтандыру;
- тиісті шараларды қабылдау үшін табысты қолайсыз әрекеттерді уақтылы анықтауды қамтамасыз ету.

### А.7.4 Қауіпсіздік мақсаттары: қорытынды

Қауіпсіздік мақсаттарына негізделген және қауіпсіздік мақсаттарына негіздеме ретінде келесі қорытынды жасауға болады: егер барлық қауіпсіздік мақсаттарына қол жеткізілсе қауіпсіздік проблемасын анықтауда анықталған қауіпсіздік проблемасы (ASE_SPD) шешіледі: барлық қауіп-қатерлерге қарсы шығады, барлық барлық ПБО

сақталады және барлық жорамалдар расталды.

### А.8 (ASE_ECD) кеңейтілген компоненттерді анықтау

Көптеген жағдайларда ST -ға қойылатын қауіпсіздік талаптары (келесі бөлімшені қараңыз) ISO / IEC 15408-2 компоненттеріне немесе ISO/IEC 15408-3 негізделген. Алайда, кейбір жағдайларда ISO / IEC 15408-2 немесе ISO/ IEC 15408-3 компоненттеріне негізделмеген ST талаптар болуы мүмкін. Бұл жағдайда жаңа компоненттерді (кеңейтілген компоненттерді) анықтау керек және бұл анықтаманы Extended Components анықтамасында жасау керек. Осы мәселе бойынша қосымша ақпарат алу үшін С.4 қосымшасын қараңыз.

Назар аударыңыз, кеңейтілген талаптарға емес (алдыңғы құрамдас бөліктерге негізделген талаптар), бұл бөлім тек кеңейтілген құрамдастарға ғана арналған.

Жетілдірілген талаптар қауіпсіздік талаптарына енгізілуі керек (төмендегі кіші бөлімнен қараңыз) және барлық мақсаттарда ISO / IEC 15408-2 немесе ISO / IEC 15408-3 компоненттеріне негізделген талаптарға сәйкес келеді.

### А.9 Қауіпсіздік талаптары (ASE_REQ)

Қауіпсіздік талаптары екі топтық талаптардан тұрады:

а) функционалдық қауіпсіздік талаптары (SFR): БО үшін қауіпсіздік мақсаттарын стандартталған тілге аудару;

b) (SAR) қауіпсіздік қамтамасыз ету талаптары: БО-ның SFR талаптарына сай екендігі туралы растауды қалай алуға болатынын сипаттау.

Бұл екі топ келесі екі тармақпен талқыланады:

#### А.9.1 Қауіпсіздік функционалына қойылатын талаптар (SFR)

SF - БО үшін қауіпсіздік мақсаттарының аудармасы болып табылады. Олар әдетте абстракцияның толық деңгейінде болады, бірақ олар толық аударма болуы керек(қауіпсіздік мақсаттары толығымен жойылуы керек) және кез-келген нақты техникалық шешімдерге тәуелді болмау (іске асыруға). ISO / IEC 15408 стандарты тілге бірнеше себептер бойынша аударуды талап етеді:

- бағалануы керек нәрсесінің нақты сипаттамасын беру. ТОЕ үшін қауіпсіздік мақсаттары әдеттегі тілде тұжырымдалғандықтан, стандартталған тілге аудару ТОЕ функциясының неғұрлым нақты сипаттамасын береді.

- екі ST арасындағы салыстыру мүмкіндігін беру. СТ-ның әртүрлі авторлары өздерінің қауіпсіздік мақсаттарын сипаттау кезінде әр түрлі терминологияны пайдалана алатындықтан, стандартталған тіл бірдей терминология мен ұғымдарды қолдануды қамтамасыз етеді. Бұл салыстыруға оңай.

ISO/IEC 15408 стандартында қауіпсіздік мақсаттарын операциялық орта үшін аудару көзделмеген, себебі жұмыс ортасы бағаланбайды және сондықтан оны бағалауға арналған сипаттама талап етілмейді. Операциялық жүйенің қауіпсіздігін бағалауға қатысты баптар бойынша библиографияны қарау.

Бір есепте операциялық орта бөліктері бағаланады, бірақ бұл ағымдағы бағалаудың шеңберінен тыс. Мысалы: ОС БО оның жұмыс ортасында брандмауэр болуын талап етуі мүмкін. Кейінгі бағалау тағы да брандмауэрді бағалауы мүмкін, бірақ бұл бағалау ОС БО бағалауына ешқандай қатысы жоқ.

### А.9.1.1 ISO / IEC 15408 қолдаушы, қауіпсіздікті талап етуде қауіпсіздік мақсаттарын түрлендіру тәсілдері

ISO / IEC 15408 осы аударманы үш тәсілмен қолдайды:

a) алдын-ала нақты анықталған «тіл» арқылы, не бағалануы керек екенін нақты сипаттауға. Бұл тіл ISO / IEC 15408-2 стандартында анықталған компоненттер жиынтығы ретінде анықталады. Бұл тілді SFR-гі БО үшін қауіпсіздік мақсаттарының айқын анықтамасы ретінде пайдалану міндетті болып табылады, кейбір ерекшеліктер бар (7.3 қараңыз).

b) операцияларды ұсыну арқылы: ST авторына БО үшін қауіпсіздік мақсаттарын неғұрлым нақты аударуды қамтамасыз ету үшін SFR-ді өзгертуге мүмкіндік беретін механизмдер. ISO/IEC 15408-нің осы бөлігінде төрт жарамды операциялар анықталды: : тағайындау, іріктеу, итерация және нақтылау. Олар 7.1-де сипатталған.

c) тәуелділікті қамтамасыз ету арқылы: SFR-ге неғұрлым толық аударманы қолдайтын механизм. ISO / IEC 15408-2 тілінде SFR басқа SFR -қа байланысты болуы мүмкін. Бұл ST осы SFR-ды қолданса, ол басқа SFR-ды әдетте пайдалануы керек. Бұл сценарий жазушысының ST-ның өтуін қиындатады, соның ішінде SFR -ны қолдана отырып, ST толықтығын жақсартады. Тәуелділіктер бұдан әрі 7.2-де келтірілген.

### А.9.1.2 SFR мен қауіпсіздік мақсаттарының өзара байланысы

Сондай-ақ, SFR екі тармақшадан тұратын ST қауіпсіздік талаптарын негіздемесі бар:

- жол тарту көрсеткендей, SFR- мекен жайлары БО-ға қауіпсіздік мақсаттарын анықтайды;
- БО үшін барлық қауіпсіздік мақсаттары SFR тиімді шешетінін көрсететін негіздемелер жиынтығы.

#### А.9.1.2.1 SFR және TOE үшін қауіпсіздік мақсаттары

Жол тарту көрсеткендей, SFR қауіпсіздік мақсатында TOE үшін келесідей бақыланады:

a) Жалған SFR-дың болмауы: әрбір SFR кем дегенде бір қауіпсіздік мақсатын бақылайды.

b) TOE үшін қауіпсіздік мақсаттарына толық қатысты. TOE үшін әрбір қауіпсіздік мақсаты кем дегенде бір SFR ізі болады.

TOE үшін бірдей қауіпсіздік мақсаттары үшін бірнеше SFR бақылануы мүмкін, осы қауіпсіздік талаптарының үйлесімі TOE үшін қауіпсіздік мақсаттарына сай келетіндігін көрсетеді.

#### А.9.1.2.2 Іргелестіру үшін логикалық негіздеме беру

Қауіпсіздік талаптарына негіздеме ізнің тиімді екендігін көрсетеді: егер БО үшін арнайы қауіпсіздік мақсатын бақылайтын барлық SFR орындалса, БО үшін осы қауіпсіздік мақсаты қол жеткізіледі

Бұл демонстрациялау тиісті SFR -ны қанағаттандырудың салдарын талдауға тиіс БО үшін қауіпсіздік мақсаттарына қол жеткізу және қорытынды жасауға мүмкіндік береді, бұл шын мәнінде осылай.

SFR БО үшін қауіпсіздік міндеттеріне өте ұқсас болған жағдайда, демонстрациялау

өте қарапайым болуы мүмкін.

### А.9.2 Қауіпсіздікке сенім талаптары (SARs)

SAR – бұл БО қалай бағаланғаны туралы сипаттама. Бұл сипаттама екі себеп бойынша стандартталған тілді қолданады:

- БО қалай бағалайтынын нақты сипаттау
- стандартталған тілді қолдану дәл сипаттама жасауға көмектеседі және белгісіздікті болдырмайды.
- ST екі арасындағы салыстыру мүмкіндігін беру. СТ-ның әртүрлі авторлары бағалауды сипаттау кезінде әр түрлі терминологияны пайдалана алады, стандартталған тіл бір терминология мен тұжырымдаманы қолданады. Бұл салыстыруға оңай.

Бұл стандартталған тіл ISO / IEC 15408-3 стандартында анықталған компоненттер жиынтығы ретінде анықталады. Бұл тілді пайдалану міндетті болып табылады, кейбір ерекшеліктер бар.

ISO / IEC 15408 осы тілді екі жолмен кеңейтеді:

a) операцияларды қамтамасыз ету арқылы: ST авторына SAR-ді өзгертуге мүмкіндік беретін механизмдер. ISO / IEC 15408-де төрт операция бар: тағайындау, іріктеу, итерация және нақтылау. Олар 7.1-де сипатталған

b) тәуелділікті қамтамасыз ету арқылы: SAR-ге неғұрлым толық аударманы қолдайтын механизм. ISO / IEC 15408-3 тілінде SAR басқа SAR-лерге байланысты болуы мүмкін. Бұл дегеніміз, егер ST осы SAR-ды қолданса, әдетте басқа SAR-ді пайдалану қажет. Бұл ST автордың жұмысын айтарлықтай қиындатады, соның ішінде қажетті SAR-ді және сол арқылы ST толықтығын жақсартады. Тәуелділіктер бұдан әрі 7.2-де келтірілген.

### А.9.3 SAR және қауіпсіздік талаптарын негіздеу

ST қауіпсіздік талаптарын негіздейді, сондай-ақ, SAR -ның осы нақты жиынтығы сәйкес деп саналды. Бұл үшін түсінік жоқ. Осы түсіндірменің мақсаты ST оқырмандарға осы нақты жиынтығын таңдау себептерін түсінуге мүмкіндік беру болып табылады. Сәйкессіздіктің мысалы - бұл қатерлердегі қауіпсіздік мәселесінің сипаттамасы, онда қауіпті агент өте тиімді және SAR құрамында төмен (немесе жоқ) осалдығы бар осалдылықты талдау (AVA_VAN) бар.

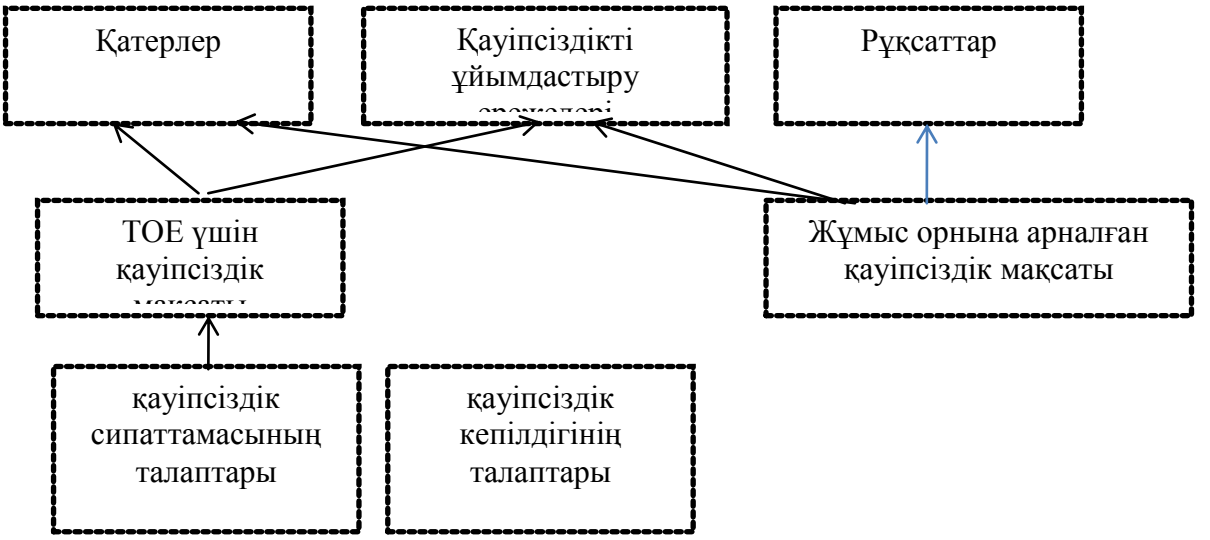
### А.9.4 Қауіпсіздік талаптары: қорытынды

ST қауіпсіздік проблемасын анықтау кезінде қауіпсіздік проблемасы қатерлерден, OSP және жорамалдан тұрады.

ST қауіпсіздік мақсаттарының шешім екі қосалқы түрінде беріледі:

- TOE үшін қауіпсіздік мақсаттары;
- жұмыс ортасының қауіпсіздік мақсаттары.

Сонымен қатар, қауіпсіздік мақсаттарына негіздеме беріледі, егер барлық қауіпсіздік мақсаттарына қол жеткізілсе, қауіпсіздік мәселесі шешіледі: барлық қауіптер жойылып, барлық ПБО орындалды және барлық болжамдар күшінде қалады.




**А.3-сурет - Қауіпсіздік проблемасын анықтау, қауіпсіздік мақсаттары мен қауіпсіздік талаптары арасындағы өзара байланыс**

### А.10 БО қысқаша спецификация (ASE_TSS)

БО-ның қысқаша спецификациясы мақсаты БО-ның барлық SFR -на қалай жауап беретінін сипаттау, БО тұтынушыларын қамтамасыз ету болып табылады.

БО қорытынды ерекшелігі, БО осы мақсат үшін пайдаланатын жалпы техникалық механизмдерді қамтуы тиіс. Осы сипаттаманың нақты әлеуетті тұтынушыларға БО жалпы пішінін және іске асырылуын түсінуге мүмкіндік беру үшін жеткілікті болуы керек.

Мысалы, егер БО интернеттегі компьютер болса және SFR аутентификациялау үшін FIA_UAU.1 болса, онда осы түпнұсқалық растама қалай орындалатындығын анықтайды: құпия сөз, белгі, көздің сыртқы мөлдір қабығы сканерлеу және т.б. Қосымша ақпарат, мысалы, БО пайдаланатын стандарттар. SFR-ті қанағаттандыру үшін немесе қосымша сипаттамалармен қамтамасыз етілуі мүмкін.

### А.11 ST көмегімен жауап беруге болатын сұрақтар

Бағалаудан кейін ST «бағаланған» дегенді көрсетеді. Осы рөлде ST, БО әзірлеушісі немесе сатушысы мен БО тұтынушысы арасындағы келісімнің негізі болып табылады. ST келесі сұрақтарға жауап бере алады (және басқалары):

a) Көптеген ST / БО-ні ескере отырып, маған қажет ST / БО қалай табуға болады? Бұл мәселе ТОЕ қорытындысында келтірілген, БО қорытындысының қысқаша (бірнеше абзацта) береді.

b) Менің қазіргі IT- инфрақұрылымыммен БО үйлесімді ме? Бұл мәселе БН шолуында қарастырылады, ол БО-ны іске қосу үшін қажетті негізгі аппараттық / бағдарламалық-аппараттық / бағдарламалық қамтамасыз ету элементтерін анықтайды;

c) Осы БО жұмыс істеп тұрған жұмыс ортасына кіреді ме? Бұл мәселе операциялық орта үшін қауіпсіздік тапсырмалары арқылы шешіледі, ол ТОЕ операциялық ортада қолданылатын барлық шектеулерді анықтайды;

d) БН (мүдделі оқырман) не істейді? Бұл мәселе БО қорытындысында келтірілген, бұл БО қысқаша қорытындыы (бірнеше абзацтар);

e) БН (мүдделі тұтынушы) не істейді? Бұл мәселе БО сипаттамасымен шешіледі, ол

қысқаша (бірнеше беттік) БО қорытындысын береді;

f) БО (техникалық) не істейді? Бұл мәселе БО-ны қолданатын механизмдердің жоғары деңгейлі сипаттамасын қамтамасыз ететін БО-ны біріктіретін спецификациясы арқылы шешіледі;

q) БО (сарапшы) не істейді? Бұл мәселені жоғары технологиялық сипаттаманың дерексіз сипаттамасын және қосымша мәліметтерді беретін ТОЕ-ны біріктіруді қамтамасыз ететін SFR қарастырады;

h) БО менің үкімет / ұйыммен анықталған мәселені анықтай ма? Егер сіздің үкіметіңіз / ұйымдарыңыз топтамаларды анықтаған болса және / немесе осы шешімді анықтау үшін РР, онда жауаптың барлық бөлімшелері мен РР-дың тізімін көрсететін ST талаптарының сәйкестігі бөлімінде табуға болады, оған ST сәйкес

i) БО қауіпсіздік мәселесін (сарапшыны) білдіре ме? БО үшін қандай қауіп бар? Ұйым қауіпсіздігінің қандай саясаты қолданылады? Операциялық орта туралы қандай болжамдар жасайды? Бұл мәселелер қауіпсіздік проблемасын анықтау арқылы шешіледі;

j) БО-ға қаншалықты сенім арта аламын? Бұны SAR бағалау үшін пайдаланылған сенімділік деңгейін қамтамасыз ететін қауіпсіздік талаптары бөлімінде және ТОЕ дұрыс болуын бағалауды қамтамасыз ететін сенімде табуға болады.

### А.12 Кепілдіктің төмен деңгейі бар қауіпсіздік тапсырмалары

ST-ті жазуы тривалды емес тапсырма және әсіресе төмен сенімділік бағалауларымен, әзірлеуші мен бағалағыштың барлық бағалауға жұмсаған күш-жігерінің негізгі бөлігі болуы мүмкін. Осы себепті сіз ST-ті төмен сенім деңгейімен жаза аласыз.

ИСО / МЭК 15408 EAL 2-ні бағалауға сенімсіздігі төмен, бірақ EAL 2 және одан жоғары емес үшін ST ST-ды пайдалануға мүмкіндік береді. Сенімділігінің төмен деңгейі бар ST тек РР-дың төмен дәрежеде сенімділікке сәйкестігін талап етеді (В қосымшасын қараңыз). Кәдімгі ST (яғни, толық мазмұнмен) РР-ны төмен деңгейде сенімділікпен талап ете алады.

ST сенімділігінің төмен деңгейі әдеттегі ST -мен салыстырғанда анағұрлым төмен мазмұнға ие:

- Қауіпсіздік проблемасының анықтамасын сипаттаудың қажеті жоқ; ТОЕ үшін қауіпсіздік мақсаттарын сипаттаудың қажеті жоқ. Жұмыс ортасының қауіпсіздік мақсаттары әлі де сипатталуы керек;
- Қауіпсіздік мақсаттары үшін негізді сипаттаудың қажеті жоқ, себебі ST -де қауіпсіздік мәселесі анықталмаған;
- Қауіпсіздік талаптарын негіздеу талап етілмейтін тәуелділіктерді негіздеу үшін қажет, өйткені ST-де ТОЕ үшін қауіпсіздік мақсаттары жоқ.

Осының барлығы:

a) ТОЕ мен ST сілтемелері;

b) Сәйкестік өтініші;

c) әртүрлі нормативтік сипаттама;

1) БО шолу;

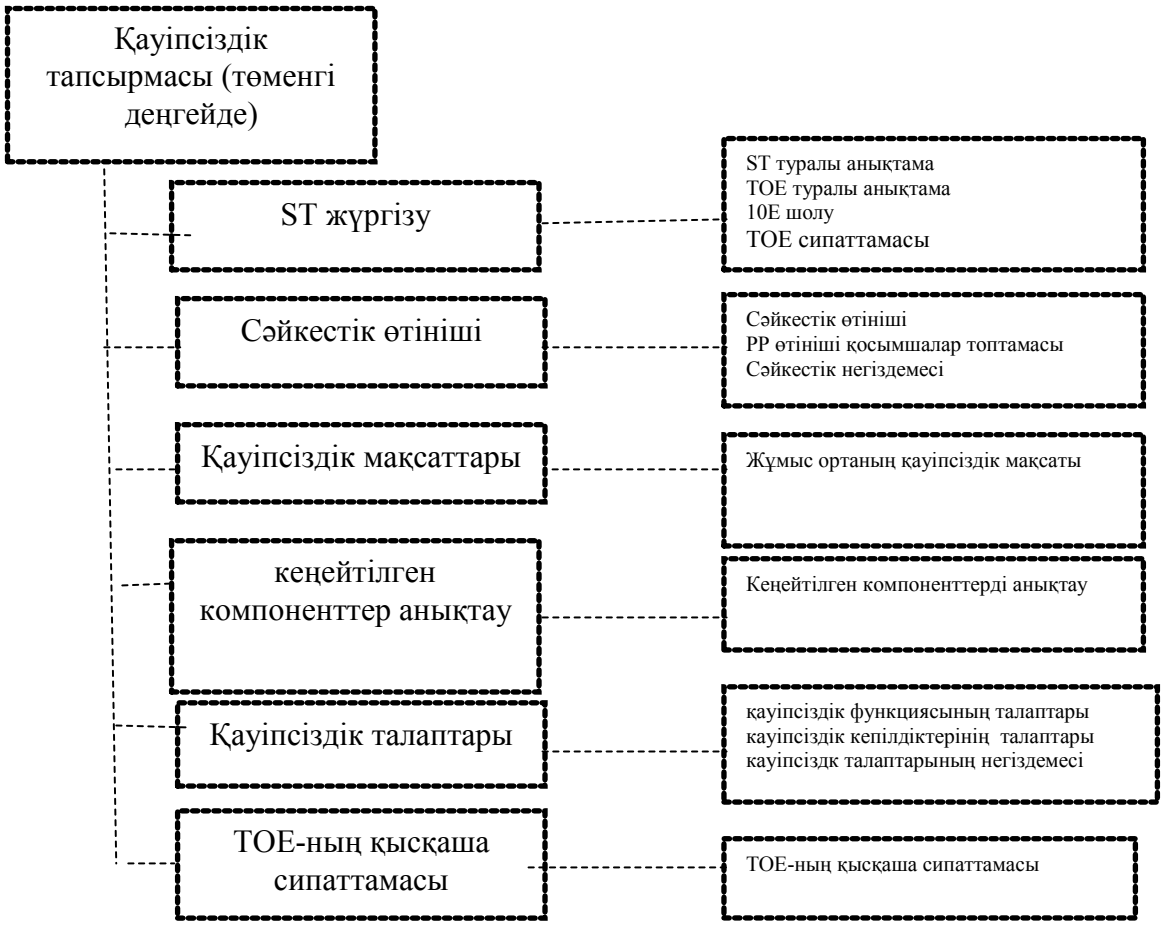
2) БО сипаттамасы;

3) БО-ның қысқаша спецификасы.

d) операциялық орта үшін қауіпсіздік мақсаттары;

e) SFR және SAR (кеңейтілген компоненттерді анықтауды қоса алғанда) және қауіпсіздік талаптарын негіздеу (егер тәуелділік сақталмаса ғана).

Төменгі деңгейдегі сенімділік деңгейі төмен ST ST мазмұны А.4-суретте көрсетілген.




**А.4-сурет - Кепілдік деңгейі төмен қауіпсіздік тапсырмасының мазмұны**

### А.13 Басқа ST стандарттарына сілтеме

Кейбір жағдайларда ST әзірлеушісі сыртқы стандартқа сілтеме жасай алады, мысалы, нақты криптографиялық стандарт немесе хаттама. ISO / IEC15408 бұл үш жолды жасауға мүмкіндік береді:

а) Ұйымның (немесе оның бір бөлігінің) қауіпсіздік саясаты.

Егер, мысалы, құпия сөздердің қалай таңдалатындығын анықтайтын мемлекеттік стандарт болса, бұл ST-де ұйымның қауіпсіздік саясаты ретінде көрсетілуі мүмкін. Бұл қоршаған ортаны қорғау мақсаттарына қол жеткізуге әкелуі мүмкін (мысалы, егер TOE пайдаланушылары парольдерді тиісінше таңдау керек болса) немесе ол TOE үшін қауіпсіздік мақсаттарына алып келуі мүмкін, содан кейін TOE парольдерді генерациялайтын болса, сәйкес SFR-ге (ең алдымен FIA класына) қатысты. Екі жағдайда да, әзірлеушінің негіздемесі ақылға қонымды болуы керек, себебі TOE және SFR қауіпсіздік мақсаттары OSP орындау үшін жарамды. Бағалаушы, егер бұл OSP төменде сипатталғандай, SFR арқылы жүзеге асырылса, бұл дұрыс болып табылатынын тексереді (және бұл үшін стандартты зерделеуді шешуі мүмкін).

b) SFR.-ны нақтылау кезінде қолданылатын техникалық стандарттар (мысалы, криптографиялық стандарттар) ретінде.

Бұл жағдайда стандартқа сәйкестік SFR TOE жүзеге асырудың бөлігі болып табылады және стандарттың толық мәтіні SFR құрамына кіреді.

SFR-қа кез –келген сәйкестіктей, сәйкестігі кейіннен анықталады: ADV уақытында: Development және ATE: тесттер талдаудың және талдаудың көмегімен, SFR БО-да толығымен және толығымен орындалады. Егер стандартты белгілі бір бөлігіне ғана

сілтеме талап етілсе, бұл бөлік SFR - да нақты көрсетілуі керек.

c) Техникалық стандарт ретінде (мысалы, криптографиялық стандарт), БО құрамдас ерекшеліктерінде көрсетілген.

БО қысқаша сипаттамасы тек SFR қалай жүзеге асырылғаны туралы түсініктеме ретінде қарастырылады және SFR немесе ADV: Development үшін ұсынылған құжаттар секілді қатаң орындау талаптары ретінде қатаң түрде пайдаланылмайды. Бағалаушы TSS техникалық стандартқа сілтеме жасайтын болса, сәйкессіздікті анықтай алады және бұл ADV-да көрсетілмейді: Даму құжаттары, бірақ стандарттың орындалуын тексеру үшін күнделікті қызмет жоқ.

**В қосымшасы**
(*ақпараттық*)

## Қорғаныс профильдерінің спецификациясы

### В.1 Осы қосымшаның мақсаты мен құрылымы

Осы қосымшаның мақсаты Қорғаушы профиль тұжырымдамасын түсіндіру болып табылады (PP). APE өлшемдері осы қосымшада анықталмаған; Бұл анықтаманы ISO / IEC 15408-3-де табуға болады және библиографияда көрсетілген құжаттармен расталады.

PP және ST -ны айтарлықтай әйкестігі болғандықтан, осы қолданба PP және ST арасындағы айырмашылықтарға баса назар аударады. PP мен ST арасында бірдей болатын материал А қосымшасында сипатталған.

Бұл қосымша төрт негізгі бөлімнен тұрады:

a) Қандай PP болуы керек. Бұл В.2-де жазылған және В.4-В.9-да толығырақ сипатталған. Бұл бөлімдерде PP-ның міндетті мазмұны, осы мазмұн мен мысалдар арасындағы байланыс сипатталады.

b) PP-ды қалай пайдалануға болады. Бұл В.3-де жазылған.

c) PP сенімділігінің төмен деңгейі. Төмен деңгейлі PP - төмендетілген мазмұнмен PP. Олар В.11-егжей-тегжейлі сипатталған.

d) стандарттарға сәйкестікті талап ету. Q.12-де автордың PP-ны белгілі бір стандартты қанағаттандыруы туралы талап етуі мүмкін.

### В.2 PP-ның міндетті мазмұны

В.1-сурет ISO / IEC 15408-3-де көрсетілген PP үшін міндетті мазмұнды бейнелейді. В.1-сурет PP құрылымдық құрылымы ретінде де қолданылуы мүмкін, балама құрылымдарға рұқсат етіледі. Мысалы, егер қауіпсіздік талаптарын негіздеу қиын болса, онда ол PP-ға қосымшаға қосылуы мүмкін, бірақ қауіпсіздік талаптары бөлімінде емес. PP-ның жекелеген тармақшалары және осы тармақшалардың мазмұны төменде келтірілген және В.4-В.9-нақты түрде түсіндірілген. PP құрамында:

a) БО түрін сипаттама сипаттайтын PP-ны енгізу;

b) ҚБ-ның кез келген ҚБ және / немесе қаптамалардың талаптарын қанағаттандыратындығын көрсететін сәйкестік талаптары және егер болса, ҚБ және / немесе қаптамалары

c) Қауіпсіздік мәселесін, дисплей қауіптерін, OSP және болжамдарды анықтау;

d) Қауіпсіздік шешімі БО үшін қауіпсіздік мақсаттары мен БО жұмыс ортасы үшін қауіпсіздік мақсаттары арасында бөлінгенін көрсететін қауіпсіздік мақсаттары;

e) жаңа компоненттерді анықтауға болатын кеңейтілген компоненттер (яғни ISO / IEC 15408-2 немесе ISO / IEC 15408-3-ге енгізілмеген). Бұл жаңа компоненттер кеңейтілген функционалдық және кеңейтілген сенімділік талаптарын анықтау үшін қажет;

f) қауіпсіздік мақсаттарын БО үшін стандартталған тілге аударатын қауіпсіздік талаптары. Бұл стандартталған тіл SFR формасына ие. Бұдан басқа, осы тармақша SAR-ды анықтайды;

Сондай-ақ төмендетілген PP бар, олар мазмұнды төмендетеді; Олар В.11-де нақты сипатталған. Бұдан басқа, осы қосымшаның барлық басқа бөліктері толық мазмұны бар PP бар деп есептейді.


**В.1-сурет - Қорғау профилінің мазмұны**

Сонымен қатар қысқартылған мазмұны бар кепілдіктің төмен деңгейіне РР (оңайлатылған РР), мұндай РР В.11-де толық сипатталған. Осы тұрғыда осы қосымшаның қалған барлық бөлімдері толық мазмұны бар РР-ды болжамдайды.

### В.3 ҚБ қолдану

#### В.3.1 РР-ды қалай пайдалануға болады

РР әдетте, пайдаланушы қауымдастығы, реттеуші орган немесе даму тобы қауіпсіздіктің қажеттіліктерінің жалпы жиынтығын анықтаған кезде қажеттіліктің анықтамасы болып табылады.

Сондықтан РР көбінесе:

- белгілі бір тұтынушыға немесе тұтынушылар тобына қойылатын талаптарды нақтылаудың бөлігі, егер олар РР-ге сәйкес келсе, белгілі бір ІТ-ны сатып алуды қарастырады;
- нормативтік актінің белгілі бір реттеуші органнан бөлімі, ол тек ІТ-ның нақты түрін ғана пайдалануға мүмкіндік береді;
- ІТ әзірлеушілер тобымен анықталған, содан кейін олар осы типтегі барлық ІТ-дың осы негізге сәйкес келетініне келіседі.

Бұл басқа пайдалануды жоққа шығармайды.

### В.3.2 РР қалай пайдаланбау қажет

РП орындауға болмайтын үш (көпшілік арасында) рөлдер:

- техникалық сипаттамалары: РР жоғары деңгейде абстракцияның қауіпсіздік ерекшелігі ретінде жасалған. Тұтастай алғанда, ПП- нақты хаттама сипаттамалары, алгоритмдердің және / немесе механизмдердің толық сипаттамалары, нақты операциялар туралы нақты сипаттама болуы керек және т.б.

- толық спецификация: РР жалпы сипаттаманы емес, қауіпсіздік ерекшелігі ретінде жасалған. Қауіпсіздік орынды болмаса, интероперабельділік, физикалық өлшемдер және салмақ сияқты қажетті сипаттар, қажетті кернеу және т.б. РР бөлігі болмауы керек. Бұл дегеніміз, ST.- әдетте толық спецификация емес, толық сипаттаманың бөлігі.

-бір өнімнің ерекшелігі: ST-тан айырмашылығы жоқ, бір өнімді емес, IT-ның нақты түрін сипаттауға арналған РР. Бір ғана өнім сипатталған кезде, осы мақсат үшін ST-ні пайдалану керек.

### В.4 ПП-ны енгізу (APE_INT)

Кіріспе РР екі деңгейдегі абстракцияның баяндалған түрінде сипаттайды:

a) РР сәйкестендіру материалын ұсынатын РР-ға сілтеме;

b) TOE қысқаша сипаттайтын TOE шолу.

### В.4.1 РР-ге сілтеме

РР осы РР-ны анықтайтын РР-ға анық сілтемеден тұрады. РР-ға типтік сілтеме тақырыптан, нұсқасынан, авторларынан және жариялау күнінен тұрады. РР-ға сілтеме жасалған мысал - «Atlanta Navy CablePhone Encryptor PP, 2b нұсқасы, Atlantean Navy Procurement Office, 7 сәуір 2003». Сілтеме әртүрлі РР және сол РР әртүрлі нұсқаларын ажырату үшін бірегей болуы керек.

РР сілтемесі РР-ны индекстеп, байланыстыруға және оны РР тізімдеріне қосуды жеңілдетеді.

### В.4.2 БО аннотация

БО зерттеуі қауіпсіздіктің қажеттіліктерін қанағаттандыра алатын және олардың аппараттық құралдарымен, бағдарламалық жасақтамаларымен және микробағдарламаларымен қамтамасыз етілген БО табу үшін бағаланатын өнім тізімдерін сканерлейтін әлеуетті БО тұтынушыларына бағытталған.

БО-ға шолу, сондай-ақ, БО жобалау кезінде немесе қолданыстағы өнімдерді бейімдеу кезінде РР-ды пайдалануға болатын әзірлеушілерге арналған.

БО шолу типтік ұзындығы бірнеше абзац.

Осы мақсатта БО шолу БО пайдалану және оның негізгі қауіпсіздік функцияларын қысқаша сипаттайды, БО түрін анықтайды және БО үшін қол жетімді кез-келген негізгі аппараттық-бағдарламалық / бағдарламалық қамтамасыз етуді / БО-лық емес бағдарламалық қамтамасыз етуді анықтайды.

#### В.4.2.1 БО-ны пайдалану мен негізгі қауіпсіздік ерекшеліктері

БО пайдалану мен негізгі қауіпсіздік функцияларының сипаттамасы БО-ның қабілетті болуы туралы жалпы түсінік беруге және оныне үшін қолдануға болады.

Бұл бөлім БО пайдаланушылары түсінетін тілді пайдалану арқылы БО

пайдалануды және негізгі қауіпсіздік функцияларын бизнес операциялары тұрғысынан сипаттайтын (әлеуетті) БО пайдаланушыларына жазылуы тиіс.

Мысалы, «Atlantean Navy CablePhone Encryptor» - бұл шифрлау құрылғысы, ол кемелер арасындағы құпия байланыспен қамтамасыз етуі тиіс Атлантлы Navy CablePhone кабельдік теледидар жүйесі. Ол үшін кемінде 32 түрлі қолданушыға рұқсат беруі және кемінде 100 Мбит / с шифрлау жылдамдығын қамтамасыз етуі керек. Ол соттар арасындағы екі жақты қарым-қатынасты да, желі бойынша хабар таратуды да қамтамасыз етуі керек».

### В.4.2.2 БО типі

БО аннотациясы: Брандмауэр, VPN брандмауэр, смарт-карта, криптомодем, интранет, веб-сервер, деректер базасы, веб-сервер және деректер базасы, LAN, веб-сервер мен LAN деректер базасымен және т.б.

### В.4.2.3 БО болып табылмайтын қол жетімді жабдық, бағдарламалық жасақтама және енгізілген бағдарламалық жасақтама

Кейбір БО басқа IT-ға сүйенбейді, көптеген БО (әсіресе бағдарламалық жасақтамаға негізделген БН) қосымша, БО-ны, аппараттық қамтамасыз етуді, бағдарламалық қамсыздандыруды және / немесе микробағдарламаны қолданады. Соңғы жағдайда БО-сыз аппараттық-бағдарламалық қамтамасыз етуді / бағдарламалық қамсыздандыруды анықтау үшін БО шолу қажет.

Қауіпсіздік профилі белгілі бір өнім үшін жазылмағандықтан, көптеген жағдайларда тек қол жетімді жабдық / бағдарламалық жасақтама / микробағдарлама туралы жалпы түсінік бере аласыз. Кейбір басқа жағдайларда, мысалы: Платформа бұрыннан белгілі бір тапсырыс берушіге қойылатын талаптарды нақтылау, нақты ақпарат берілуі мүмкін.

Аппараттық / бағдарламалық қамтамасыз ету / енгізілген қауіпсіздік мысалдары:

- Ешқандай. (Толық автономды БО үшін);
- Yaiza операциялық жүйесі 3.0 ортақ компьютерде жұмыс істейді;
- CleverCard SB2067 интегралдық схемасы;
- QuickOS нұсқасы 2.0 операциялық жүйесі арқылы жұмыс істейтін микропроцессорлық CleverCard SB2067;
- Желілер Департаменті Бас директорының LAN басқармасына орнату, желтоқсан 2002 ж.

## В.5 Сәйкестік өтініші (APE_CCL)

Осы PP тарауда PP басқа PP және топтамаларға сәйкестікте сипатталады. ST үшін сәйкестік талаптарының тармақшасымен бірдей (А.5 қараңыз), бір ерекшелігі: сәйкестік туралы мәлімдеме.

ҚС-дағы сәйкестік туралы мәлімдеме PP және / немесе басқа ST -лардың осы PP-ға сәйкестігін анықтайды. PP-ның авторы «қатаң» немесе «дәлелденген» сәйкестікті қажет етеді. Осы тақырып бойынша қосымша ақпарат алу үшін D қосымшасын қараңыз.

## В.6 Қауіпсіздік проблемасын анықтау (APE_SPD)

Бұл кіші бөлім А.6-да түсіндірілгендей, ST қауіпсіздік проблемасын анықтаудың

тармақшасымен бірдей

### В.7 Қауіпсіздік мақсаттары (APE_OBJ)

Бұл субтитр А.7-де түсіндірілгендей, ST қауіпсіздік мақсаттарының тармақшасымен бірдей.

### В.8 Кеңейтілген құрамдас бөліктерді анықтау (APE_ECD)

Осы тармақ А.8-тармағында сипатталғандай, кеңейтілген ST компоненттерінің қосалқы тармағына ұқсас.

### В.9 Қауіпсіздік талаптары (APE_REQ)

Осы тармақ А.9-тармағында түсіндірілгендей, ST қауіпсіздік талаптары секциясына ұқсас. Дегенмен, PP-да операцияларды жүргізу ережелері ST бойынша операцияларды жүргізу ережелерінен біршама ерекшеленетінін ескеріңіз. Бұл 7.1-де толығырақ сипатталған.

### В.10 БО қысқаша спецификациясы

PP-дың қысқаша сипаттамасы жоқ.

### В.11 Сенімнің төмен деңгейіне арналған қорғау профилдері

Кішігірім сенімділік деңгейі төмен PP-мен (яғни, толық мазмұнымен) осындай сенімділік деңгейі төмен сенімділік дәрежесімен тұрақты ST -ға жатады. Бұл сенімділік деңгейі төмен PP төмендегілерді білдіреді:

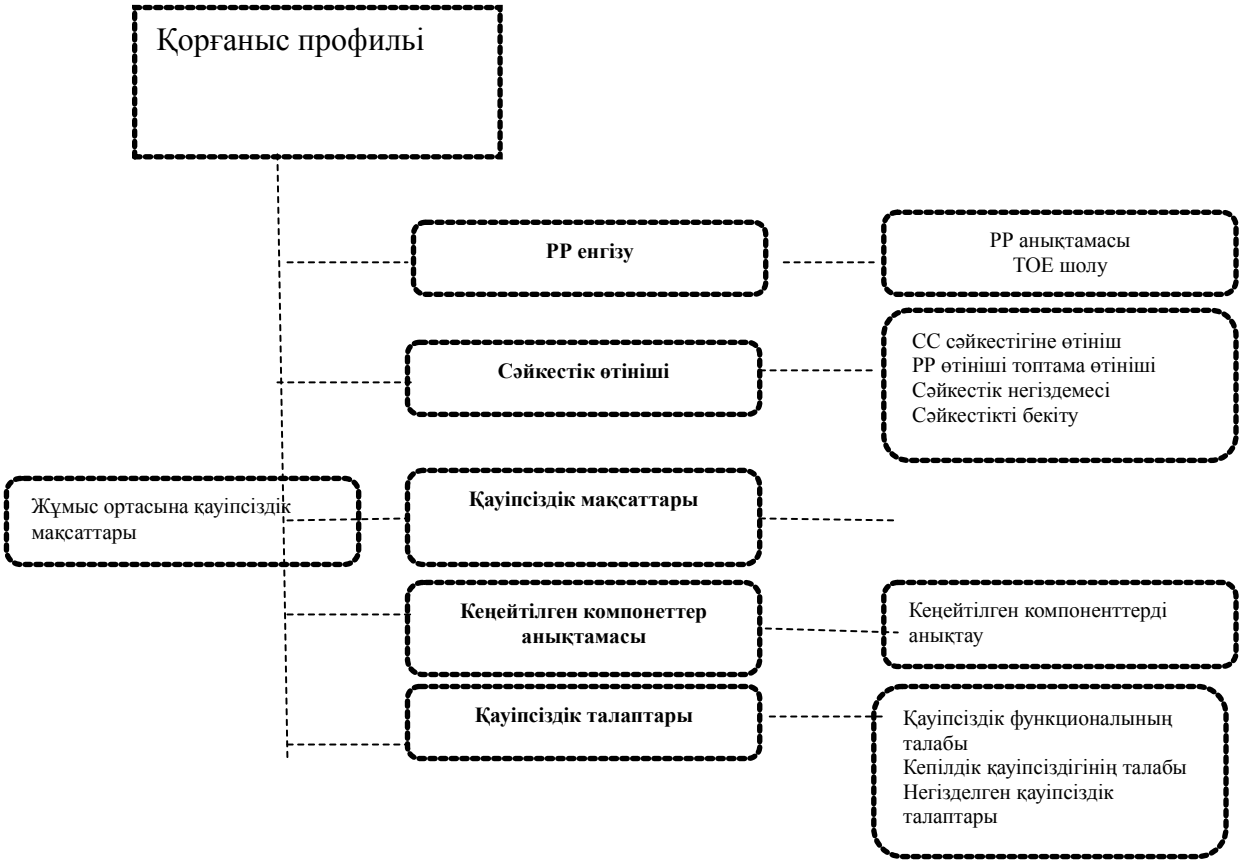
б) сәйкестік талаптары;

c) операциялық ортасының қауіпсіздік мақсаттары;

d) SFR және SAR (кеңейтілген компоненттерді анықтауды қоса алғанда) және қауіпсіздік талаптарын негіздеу (егер тәуелділік сақталмаса ғана).

Кепілдік деңгейі төмен PP тек қана PP-дың сенімділігінің төмен деңгейіне сәйкестігін талап етеді (В.5-ні қараңыз). Регламенттелген PP, PP сенімділіктің төмен дәрежеде болуын талап ете алады.

В.2-суретте төмен сенім деңгейі төмен ПП төмендегені көрсетілген.




**В.2-сурет - Кепілдік деңгейі төмен қорғаныс профилінің мазмұны**

### В.12 Басқа РР стандарттарына сілтеме

Бұл тармақ А13-де сипатталғандай, ST стандартының тармақшасымен бірдей, тек қана ерекшелік бар: егер РР-де шоғырландырылған БО ерекшелігі болмаса, үшінші нұсқа РР үшін жарамсыз болып табылады.

РР-ның авторы SFR -дағы стандартқа сілтеме БО-ны әзірлеушіге осы РР-ға (стандарттың мөлшеріне және күрделілігіне және кепілдік талап етілетін деңгейіне байланысты) елеулі жүктеме жүктей алады деп еске салады және ол баламалы болуы мүмкін осы Стандартқа сәйкестікті бағалау.

## С қосымшасы
*(ақпараттық)*

## Операцияларды орындау бойынша басшылық

### С.1 Кіріспе

ISO / IEC 15408, 1-бөлімде сипатталғандай, қауіпсіздік профилдері мен қауіпсіздік мақсаттары алдын ала анықталған қауіпсіздік талаптарын қамтиды, сондай-ақ PP және ST авторларын кейбір жағдайларда компоненттік тізімдерді кеңейтуге мүмкіндік береді.

### С.2 Операциялардың мысалдары

Операциялардың төрт түрі 7.1-де берілген. Әр түрлі операциялар мысалдары төменде сипатталған:

### С.2.1 «Итерация» операциясы

7.1.1-де сипатталғандай, әр компонент үшін Итерация операциясы орындалуы мүмкін. PP/ST авторы бір құрамдасқа негізделген бірнеше талаптарды қосу арқылы иерация жұмысын орындайды. Компоненттің әрбір итерация осы компоненттің барлық басқа итерацияларынан ерекшеленеді, ол тапсырмаларды және таңдауларды орындау арқылы немесе оны өзгеше түрде нақтылау арқылы жүзеге асырылады. Бұл талаптардың нақты негіздемесі мен қадағалауы үшін әртүрлі итерациялар бірегейлендірілуі керек.

Итерацияның типтік мысалы - FCS_COP.1. Криптографиялық операциялар екі рет қайталанып, екі түрлі криптографиялық алгоритмді енгізуді талап етеді. Әрбір Итерацияның бірегей мысалы:

Криптографиялық операциялар (RSA және DSA қолтаңбалары) (FCS_COP.1 (1))

Криптографиялық операциялар (TLS / SSL: симметриялық операциялар) (FCS_COP.1 (2))

### С.2.2 «Тағайындау» операциясы

7.1.2-де сипатталғандай, бұл құрамдас бөлік құрамында PP/ST авторы белгілейтін параметр бар элемент болған жағдайда тапсырма операциясы орын алады. Параметр айнымалы мәндерді белгілі бір ауқымға дейін шектейтін шексіз айнымалы немесе ереже болуы мүмкін.

Мақсаты бар элементтің үлгісі болып табылатын: FIA_AFL.1.2 «Нақты аутентификация әрекеттерінің белгілі бір саны орындалды немесе асқаннан кейін, TSF [тағайындады: әрекеттер тізімі].»

### С.2.3 «Таңдау» операциясы

7.1.3-де сипатталғандай, іріктеу операциясы компонент құрамында PP/ST авторы бірнеше элементтерден таңдауға тиісті элемент болғанда орын алады.

FPT_TST.1.1 «TSF өзін-өзі сынаудың [таңдау: бастапқы іске қосу кезінде, қалыпты жұмыс кезінде кезеңді түрде, уәкілетті қолданушының сұрауы бойынша, [тағайындауы: өздігінен сынау жүзеге асырылатын жағдайлар]] астында орындалуы керек», дұрыс жұмысын көрсету ...»

### С.2.4 «Нақтылау» операциясы

7.1.4-де сипатталғандай, әрбір талап бойынша нақтылау операциясы жүргізілуі мүмкін. ҚБ / ҚТ авторы бұл талапты өзгерту арқылы нақтылауды орындайды.

Тиісті нақтылау мысалы: FIA_UAU.2.1 «НҚҚ-ны осы пайдаланушының атынан басқа TSF -ның әрекеттеріне рұқсат бермес бұрын әрбір пайдаланушы аутентификациядан өтуін талап етуі керек». «TSF -ға түсініктеме беру үшін, әрбір пайдаланушы осы қолданушының атынан басқа TSF -ның әрекеттеріне рұқсат беруден бұрын пайдаланушы атын / паролімен сәйкестендірілуі тиіс».

Түсіндіруге арналған бірінші ереже БО-ның көрсетілген талапты қанағаттандыратыны PP/ST тұрғысындағы агрегаттық емес талапты қанағаттандырады (яғни, нақтыланған талаптар бастапқы талапқа қарағанда «қатаң» болуы керек).

Бұл ережеге тек қана PP/ST авторы SFR -ны кейбіреулеріне емес, субъектілерге, объектілерге, операцияларға, қауіпсіздік атрибуттарына және / немесе сыртқы нысандарға қолдану үшін нақтылауға мүмкіндік береді.

Мұндай ерекше жағдайдың мысалы FIA_UAU.2.1 «TSF -ны осы пайдаланушының атынан кез-келген басқа TSF -ның әрекеттеріне рұқсат бермес бұрын әрбір пайдаланушы түпнұсқалығын растауды талап етуі керек». «TSF-дан шыққан әрбір пайдаланушының сол пайдаланушының атынан басқа TSF -ның әрекеттеріне рұқсат беруден бұрын түпнұсқалығын растауды талап етуі тиіс».

Деректерді нақтылаудың екінші ережесі, нақтылау бастапқы компонентке қатысты болуы керек. Мысалы, электромагниттік сәулеленудің алдын алу үшін қосымша элементпен аудит компонентін тазалауға жол берілмейді.

Анықтаудың жеке жағдайы - сұрауда шағын өзгерістер болғанда, яғни ағылшын тілінің дұрыс грамматикасына байланысты немесе оқырман үшін түсінікті болғандықтан, сөйлемді қайта топтастыру кезінде редакциялық қайта қарау. Бұл өзгеріс талаптың мәнін қандай да бір түрде өзгертуге мүмкіндік бермейді. Редакциялық түсініктеме мысалдары:

- SFR FPT_FLS.1 «TSF мынадай қателіктер үшін қауіпсіз жағдайды сақтауды жалғастыруы керек: бір процессордың бөлінуі» FPT_FLS.1 «TSF мынадай қате орын алған жағдайда қауіпсіз жағдайды сақтауды жалғастыруы керек: бір процессордың бөлінуі немесе тіпті FPT_FLS.1. TSF бір процессор бұзылғанда қауіпсіздікті сақтауды жалғастыруы керек».

### С.3 Компоненттерді ұйымдастыру

ISO / IEC 15408 ISO / IEC 15408-2 және ISO / IEC 15408-3 компоненттерін иерархиялық құрылымдарға ұйымдастырды:

- класстар, олардан тұратын
- отбасылар, олардан тұратын
- құрамдас бөліктер, олардан тұратын
- элементтер.

Бұл ұйым иерархиясында классынан - отбасы - құрамдас бөлік - құрамдас бөліктерді іздестіруде тұтынушыларға, әзірлеушілерге және бағалаушыларға көмектесетін элемент.

ISO/IEC 15408 бірыңғай иерархиялы стилде функционалды және кепілдендіретін компоненттерді білдіреді және олар үшін сол ұйымды және терминологияны пайдаланады.

### С.3.1 Класс

Класстың мысалы FIA класы: сәйкестендіру және түпнұсқалық растау, пайдаланушыны идентификациялауға, пайдаланушылардың аутентификациясына және пайдаланушылар мен субъектілердің байланысына бағытталған.

### С.3.2 Отбасы

Отбасының мысалы FIA_UAU болып табылады, ол аутентификация және аутентификация. Бұл отбасы пайдаланушының аутентификациясына баса назар аударады.

### С.3.3 Құрамдас бөлік

Компоненттің мысалы - FIA_UAU.3. Түпнұсқалық растамаға түпнұсқаландырылмаған түпнұсқалық аутентификация.

### С.3.4 Элемент

FIA_UAU.3.2 элементтің мысалы көшірілген түпнұсқалық деректерді пайдаланудың алдын алуға бағытталған.

## С.4 Кеңейтілген компоненттер

### С.4.1 Кеңейтілген компоненттерді қалай анықтауға болады

PP/ST авторы кеңейтілген құрамдас бөлікті анықтаған кезде, ол қолданыстағы ISO / IEC 15408 құрамдас бөліктеріне ұқсас: нақты, біржақты және бағаланатын (осы компонент бойынша талаптардың БО үшін қанағаттандырылатынын жүйелі түрде көрсете алуы мүмкін). Кеңейтілген компоненттер қолданыстағы ISO / IEC 15408 компоненттеріне сәйкес бірдей таңбалауды, экспрессиялау әдісін және дәреженің деңгейін пайдаланады.

PP/ST авторы кеңейтілген компоненттің барлық қолданылатын тәуелділіктері осы кеңейтілген компоненттің анықтамасына қосылғанын қамтамасыз етуі керек. Ықтимал тәуелділіктердің мысалдары:

а) егер кеңейтілген компонент FAU компоненттеріне байланысты аудитке қатысты болса: қауіпсіздік аудит классын қосу қажет болуы мүмкін;

б) егер кеңейтілген құрамдас деректерді өзгертсе немесе қол жеткізсе, онда кіруді бақылау саясатын құрайтын компоненттеріне (FDP_ACC) байланысты болуы мүмкін;

с) егер кеңейтілген компонент нақты жобаның сипаттамасын қолдана отырып, тиісті ADV-ға тәуелділікті қамтуы мүмкін: дамушы отбасы (мысалы, функционалдық ерекшелігі).

Кеңейтілген функционалдық компонент болған жағдайда PP/ST авторы осы компоненттің анықтамасына ISO / IEC 15408-2 құрамдас бөліктеріне ұқсас кез-келген қолданыстағы инспекция мен байланысты операцияларды қосу керек. Кеңейтілген сенімділік компоненті болған жағдайда PP/ST авторы ISO / IEC 18045 стандартында көрсетілген әдістемеге ұқсас компонент үшін тиісті бағалау әдістемесін қамтамасыз етуі тиіс.

Кеңейтілген компоненттер бар отбасыларға орналастырылуы мүмкін, бұл жағдайда PP / ST әзірлеушісі осы отбасылардың қалай өзгеретінін көрсетуі керек. Егер олар қазіргі отбасына сәйкес келмесе, олар жаңа отбасына орналастырылуы тиіс. Жаңа отбасыларды ISO/IEC 15408-ге ұқсас белгілеу керек.

Жаңа отбасылар бар класстарға орналастырылуы мүмкін, бұл жағдайда PP/ST

әзірлеушісі осы класстардың қалай өзгеретінін көрсетуі керек. Егер олар қолданыстағы классқа сай болмаса, олар жаңа классқа қойылуы керек. Жаңа класстар ISO / IEC 15408 стандартына ұқсас болуы керек.

**D қосымшасы**
*(ақпараттық)*

**PP сәйкестігі**

### D.1 Кіріспе

PP ST үшін «шаблон» ретінде пайдалануға арналған. Яғни PP қолданушы қажеттіліктерінің жиынтығын сипаттайды, ал осы PP-ға сәйкес келетін ST осы қажеттіліктерге жауап беретін БО-ды сипаттайды.

PP-ді басқа ПП үшін үлгі ретінде қолдануға болатындығын атап өту керек, яғни PP басқа PP-мен сәйкестікті талап етуі мүмкін. Бұл оқиға PP және ПП туралы толығымен қайталанады. Түсінікті болу үшін, бұл қосымша тек ST/PP жағдайын сипаттайды, бірақ ол PP / PP жағдайларында да орын алады.

ISO/IEC 15408 жартылай келісімнің кез-келген түріне жол бермейді, сондықтан, егер PP, PP немесе ST талап етілсе, көрсетілген PP-не немесе PP-ге толығымен сәйкес келуі тиіс. Дегенмен, корреспонденцияның екі түрі бар (қатаң және дәлелденген), хат алмасудың рұқсат етілген түрі PP арқылы анықталады. Яғни PP (PP-ге сәйкестігі туралы мәлімдемесінде, B.5-ні қараңыз), ST үшін түрлерінің қайсысы рұқсат етілуін көрсетеді.

Қатаң және көрнекілендірілген келісу арасындағы бұл айырмашылық әрбір PP-ға қолданылады, оған ST жеке негізде сәйкестікті талап етуі мүмкін. Бұл дегеніміз, ST кейбір PP-на қатаң сәйкес келеді және дәлелденген - басқа PP. ST тек қана дәлелденген PP-да ғана рұқсат етіледі, егер PP оны бірден қабылдайды, ал ST әрдайым PP-ға қатаң сәйкес келеді.

Басқаша айтқанда, ST PP-ге бірден-бірі түзетсе ғана, PP-ға дәлелденген жолмен сәйкес келуге рұқсат етіледі.

PP-дың сәйкестігі PP немесе ST (және егер ST болжамды өнім болса, онда өнім) осы PP-ның барлық талаптарын қанағаттандырады.

Жарияланған PP, әдетте, дәлелді сәйкестікті талап етеді. Бұл дегеніміз, PP-лерге сәйкестікті растайтын ST-лар PP-да сипатталған жалпы қауіпсіздік проблемасын шешуді ұсынуы керек, бірақ олар PP-да сипатталғанға қарағанда кез-келген баламалы немесе неғұрлым шектеулі болуы мүмкін.

ISO / IEC 15408 стандартындағы «баламалы, бірақ одан да шектеулерсіз» жеткілікті түрде анықталған, бірақ, негізінен, PP және ST түрлі объектілерді талқылайтын, түрлі түсініктерді және т.б. қолданатын толықтай әртүрлі қосымшаларды қамтуы мүмкін екенін білдіреді. Жалпы алғанда, ST -да бірдей немесе үлкен шектеулерді, ал сол немесе аз болса - БО жұмыс ортасына енгізеді.

### D.2 Қатаң сәйкестік

Қатаң сәйкестік PP-ға қойылатын талаптардың орындалғанын дәлелдеуге мұқтаж болған PP-дың авторына жіберіледі, ал ST - PP-ны құру, ST PP-ге қарағанда кеңірек болуы мүмкін.

Іс жүзінде, ТОЕ, кем дегенде, ST -да бірдей жұмыс істейтіндігін көрсетеді, ал операциялық орта негізінен PP-мен бірдей.

Қатаң сәйкестікті пайдаланудың типтік мысалы - өнімнің қауіпсіздігіне қойылатын талаптар PP-да көрсетілген талаптарға дәл сәйкестік күткенде сатып алу негізінде таңдау болып табылады.

PP-ны қатаң сәйкестікте жүзеге асыратын ST -да PP-да көрсетілгендерге қосымша шектеулер енгізілуі мүмкін.

### D.3 Дәлелденетін сәйкестік

Тиісті сәйкестік PP авторы болып табылады, ол ST PP-да сипатталған жалпы қауіпсіздік проблемасына қолайлы шешім екенін дәлелдеуге мұқтаж.

PP және ST арасындағы қатаң сәйкестік жағдайында, ішкі және жоғары деңгей арасындағы айқын байланыс бар, егер бұл репрезентативті хат-хабарлар болса, онда бұл қатынас анық болмайды. PP-ны сәйкестендіру туралы ST -ны PP-да сипатталған жалпы қауіпсіздік проблемасына шешу ұсынылады.

Дегенмен, сәйкестікті растау БО мен оның жұмыс ортасына бірдей немесе үлкен шектеулер енгізген жағдайда ғана рұқсат етіледі.

**В.А. қосымшасы**
*(ақпараттық)*

**Стандарттардың сілтемелік халықаралық, аймақтық стандарттарға, шет мемлекеттерінің стандарына сәйкестігі туралы мәліметтер**

**В.А.1-кесте - Стандарттардың сілтемелік халықаралық, аймақтық стандарттарға, шет мемлекеттерінің стандарына сәйкестігі туралы мәліметтер**

| Аймақтық стандарттарды белгілеу және атау | Дәрежесі сәйкестік | Ұлттық стандарт, мемлекетаралық стандарт белгілеу және атауы |
|---|---|---|
| ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components (Ақпараттық технологиялар - Қауіпсіздік техникасы - IT қауіпсіздігін бағалау өлшемдері - 2-бөлім: Қауіпсіздіктің функционалдық компоненттері) | IDT | ҚР СТ ГОСТ Р ИСО/МЭК 15408-2-2006 (ГОСТ Р ИСО/МЭК 15408-2-2002, IDT) Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемдері 2-бөлім. Функционалдық қауіпсіздік талаптары. Мазмұны |
| ISO/IEC 15408-3:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components (Ақпараттық технологиялар - Қауіпсіздік әдістері - АТ қауіпсіздігін бағалау өлшемдері - 3-бөлім: Қауіпсіздікті қамтамасыз ету компоненттері) | IDT | ҚР СТ ГОСТ Р ИСО/МЭК 15408-3-2006 (ГОСТ Р ИСО/МЭК 15408-3-2002,) Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемдері 3-бөлім. Қауіпсіздікке деген сенім талаптары. |
| ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security evaluation (Ақпараттық технологиялар, қауіпсіздік техникасы, IT қауіпсіздігін бағалау әдістемесі) | IDT | ҚР СТ ИСО/МЭК 18045-2009 «Ақпараттық технологиялар. Қорғаныс әдістері. Ақпараттық технологияларды қорғау әдіснамасы» |

## Библиография

[1] (ISO/IEC 15292, Information technology – Security techniques – Protection Profile registration procedures) ISO/IEC 15292, Ақпараттық технологиялар - Қауіпсіздік әдістері - Қауіпсіздік профилін тіркеу рәсімдері.

[2] (ISO/IEC 15443 (all parts), Information technology – Security techniques – A framework for IT security assurance) ISO/IEC 15443 (барлық бөліктер), Ақпараттық технологиялар - Қауіпсіздік әдістері - IT қауіпсіздігінің жұмыс ортасы

[3] (ISO/IEC 15446, Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets) ISO/IEC 15446, Ақпараттық технологиялар - Қауіпсіздік техникасы - Қауіпсіздік профилдерін және қауіпсіздікті қамтамасыз ету бойынша тапсырмаларды дайындау бойынша нұсқаулық.

[4] (ISO/IEC 19790, Information technology – Security techniques – Security requirements for cryptographic modules) ISO/IEC 19790, Ақпараттық технологиялар - қауіпсіздік әдістері - криптографиялық модульдерге арналған қауіпсіздік талаптары

[5] (ISO/IEC 19791, Information technology – Security techniques – Security assessment of operational systems) ISO/IEC 19791, Ақпараттық технологиялар - Қауіпсіздік әдістері - Операциялық жүйелердің қауіпсіздігін бағалау

[6] (ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements) ISO/IEC 27001, Ақпараттық технологиялар - Қауіпсіздік техникасы - Ақпараттық қауіпсіздікті басқару жүйесі - Талаптар

[7] (ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management) ISO/IEC 27002, Ақпараттық технологиялар - Қауіпсіздік әдістері - Ақпараттық қауіпсіздікті басқарудың практикалық ережелері

[8] (IEEE Std 610.12-1990, Institute of Electrical Engineers, Standard Glossary of Software Engineering Terminology) IEEE Std 610.12-1990, Электротехника және электроника инженерлері институты, бағдарламалық қамтамасыз етуді әзірлеу технологиясы саласындағы терминологияның стандартты глоссарийі

[9] (Common Criteria portal, February 2009. CCRA, www.commoncriteriaportal.org) Жалпы өлшемдер порталы, ақпан, 2009 ж. CCRA, www.commoncriteriaportal.org

**ӘОЖ 681.324:006.354** **МКЖ 35.040**

**Түйін сөздер:** ақпараттық технологиялар, қауіпсіздік бағалау критерийлері, қауіпсіздік тапсырмалары, қорғау профилі, бағалау объектісі, қауіпсіздіктің функциялық мүмкіндіктері, қауіпсіздікке деген сенімділік

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

# Информационные технологии

# Методы и средства обеспечения безопасности

# Критерии оценки безопасности информационных технологий

# Часть 1

# ВВЕДЕНИЕ И ОБЩАЯ МОДЕЛЬ

**СТ РК ISO/IEC 15408-1-2017**

*(ISO/IEC 15408-1:2009 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model, IDT)*

**Издание официальное**

**Комитет технического регулирования и метрологии
Министерства по инвестициям и развитию Республики Казахстан
(Госстандарт)**

**Астана**

## Предисловие

**1 ПОДГОТОВЛЕН И ВНЕСЕН** АО «Национальный инфокоммуникационный Холдинг «Зерде»

**2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ** Приказом Председателя Комитета технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан от «24» ноября 2017 года № 334-од.

**3** Настоящий стандарт идентичен международному стандарту ISO/IEC 15408-1:2009 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель)

Официальной версией является текст на государственном и русском языке

Международный стандарт разработан техническим комитетом ISO/IEC JTC 1 Информационные технологии, SC 31, Технологии автоматической идентификации и сбора данных.

Перевод с английского языка (en).

Официальный экземпляр стандарта, на основе которого подготовлен настоящий национальный стандарт и на которые даны ссылки, имеются в Едином государственном фонде нормативных технических документов.

Сведения о соответствии стандартов (межгосударственных) ссылочным международным стандартам приведены в дополнительном приложении В.А.

Степень соответствия - идентичная (IDT).

**4** В настоящем стандарте реализованы положения Законов Республики Казахстан «О техническом регулировании» от 09 ноября 2004 года № 603-II и «Об информатизации» от 24 ноября 2015 года № 418-V.

**5 СРОК ПЕРВОЙ ПРОВЕРКИ** 2024 год
**ПЕРИОДИЧНОСТЬ ПРОВЕРКИ** 5 лет

**6 ВВЕДЕН ВЗАМЕН С**Т РК ГОСТ Р ИСО/МЭК 15408-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

*Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Нормативные документы по стандартизации», а текст изменений – в ежемесячных информационных указателях «Национальные стандарты». В случае пересмотра (отмены) или замены настоящего стандарта соответствующая информация будет опубликована в информационном указателе «Национальные стандарты».*

## Введение

ISO/IEC 15408 под общим названием Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в ИТ состоит из следующих частей:

- Часть 1: Введение и общая модель
- Часть 2: Функциональные компоненты обеспечения безопасности
- Часть 3: Компоненты обеспечения гарантии безопасности

ISO/IEC 15408 допускает сопоставимость результатов независимых оценок безопасности. ISO/IEC 15408 делает это путем предоставления общего набора требований к функциональным возможностям безопасности ИТ-продуктов и мер доверия, применяемых к этим IT-продуктам в ходе оценки безопасности. Данные ИТ-продукты могут быть реализованы в аппаратных средствах, прошивке или программном обеспечении.

Процесс оценки устанавливает уровень уверенности в том, что функциональные возможности безопасности этих ИТ-продуктов и меры доверия, применяемые к этим ИТ-продуктам, соответствуют этим требованиям. Результаты оценки могут помочь потребителям определить, удовлетворяют ли эти IT-продукты их потребностям в безопасности.

ISO/IEC 15408 подходит в качестве руководства по разработке, оценке и/или закупкам IT-продуктов с функциями безопасности.

ISO/IEC 15408 является гибким, позволяющим применять ряд методов оценки для ряда свойств безопасности целого ряда ИТ-продуктов. В связи с этим пользователям стандарта рекомендуется следить за тем, чтобы эта гибкость не использовалась неправильно. Например, использование ISO/IEC 15408 в сочетании с неподходящими методами оценки, нерелевантными свойствами безопасности или несоответствующими IT-продуктами может привести к бессмысленным результатам оценки.

Факт проведения оценки ИТ-продукта имеет значение только в контексте свойств безопасности, которые были оценены, и использованных методов оценки. Оценивающим органам рекомендуется проверять продукты, свойства и методы в целях определения смыслового значения результатов, которые даст оценка. Кроме того, покупателям оцененных продуктов рекомендуется рассмотреть этот контекст для определения пригодности и применимости оцененного продукта к их конкретной ситуации и потребностям.

ISO/IEC 15408 затрагивает вопросы защиты от несанкционированного раскрытия, изменения или потери использования активов. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно соответственно называются конфиденциальностью, целостностью и доступностью. ISO/IEC 15408 также может быть применим к аспектам безопасности ИТ за пределами этих трех свойств. ISO/IEC 15408 применим к рискам, связанным с деятельностью человека (злонамеренным или иным), а также к рискам, сопряженным с деятельностью, не связанной с человеком. Помимо безопасности ИТ, ISO/IEC 15408 может применяться в других областях ИТ, но не заявляет требований на применимость в этих областях.

Некоторые темы, поскольку являются связанными со специализированными технологиями или относятся к безопасности ИТ скорее косвенным образом, считаются выходящими за рамки стандарта ISO/IEC 15408. Некоторые из них указаны ниже.

a) ISO/IEC 15408 не содержит критериев оценки безопасности, относящихся к административным мерам безопасности, не связанным непосредственно с функциональностью безопасности ИТ. Вместе с тем признается, что административными мерами, такими как организационный, кадровый, физический и процедурный контроль, может часто достигаться или поддерживаться значительная степень безопасности.

b) Оценка некоторых технических физических аспектов безопасности ИТ, таких как управление электромагнитным излучением, конкретно не рассматривается, однако многие из рассмотренных концепций являются применимыми к этой области.

c) В ISO/IEC 15408 не рассматривается методология оценки, в соответствии с которой критерии должны применяться. Данная методология приведена в ISO/IEC 18045.

d) В ISO/IEC 15408 не рассматриваются административные и правовые рамки, в соответствии с которыми критерии могут применяться органами оценки. Однако ожидается, что ISO/IEC 15408 будет использоваться в контексте такой структуры для целей оценки.

e) Процедуры использования результатов оценки при аккредитации не входят в сферу применения стандарта ISO/IEC 15408. Аккредитация - это административный процесс, при котором предоставляются полномочия на эксплуатацию ИТ-продукта (или его набора) в его полной операционной среде, включая все ее части, не связанные с ИТ. Результаты процесса оценки являются частью при процессе аккредитации. Однако, поскольку для оценки свойств, не связанных с ИТ и их отношению к части безопасности ИТ, более подходят другие методы, по данным аспектам аккредитующими лицами должны делаться отдельные положения.

f) Предмет критериев оценки качеств, присущих криптографическим алгоритмам, не рассматривается в ISO/IEC 15408. В случаях необходимости независимой оценки математических свойств криптографии должна предусматриваться схема оценки, в соответствии с которой при оценивании применяется ISO/IEC 15408.

Стандарты ISO, такие как «может», «справочного характера», «возможно», «нормативный», «обязуется» и «должен», используемые во всем документе, определены в Директивах ISO/IEC, часть 2. Термин «должен» имеет дополнительный смысл, применяющийся при использовании этого стандарта. См. примечание ниже. Для использования «должен» в ISO/IEC 15408 дано следующее определение:

Должен - в нормативном тексте «должен» указывает «на то, что среди нескольких возможностей какая-либо из них рекомендуется в качестве наиболее подходящей, без упоминания или исключения других, или что определенный курс действий предпочтителен, но не требуется в обязательном порядке» (Директивы ISO/IEC, часть 2) .

Примечание - ISO/IEC 15408 интерпретирует «не требуется в обязательном порядке» как означающее, что выбор другой возможности требует обоснования причин, по которым не был выбран предпочтительный вариант

**Содержание**

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

# Информационные технологии
# Методы и средства обеспечения безопасности
# Критерии оценки безопасности информационных технологии

## Часть 1

## ВВЕДЕНИЕ И ОБЩАЯ МОДЕЛЬ

**Дата введения 2019-01-01**

### 1 Область применения

Настоящий стандарт устанавливает основные понятия и принципы оценки безопасности информационных технологий (ИТ), а также определяет общую модель оценки, предназначенную для использования при оценке характеристик безопасности продуктов ИТ.

В настоящем стандарте представлен обзор и описание всех частей ISO/IEC 15408; определены термины и сокращения, используемые во всех частях ISO/IEC 15408; установлено основное понятие объекта оценки (ОО), контекста оценки, описана целевая аудитория, которой адресованы критерии оценки. Представлены основные положения, необходимые для оценки продуктов ИТ.

В настоящем стандарте определяются операции, посредством которых функциональные компоненты и компоненты доверия, приведенные в СТ РК ISO/IEC 15408-2 и СТ РК ISO/IEC 15408-3 могут быть доработаны для конкретного применения путем использования разрешенных операций.

В настоящем стандарте определяются понятия профилей защиты (ПЗ), пакетов требований безопасности, а также рассматриваются вопросы, связанные с утверждениями о соответствии; описываются выводы и результаты оценки. В настоящем стандарте даны инструкции по спецификации заданий по безопасности (ЗБ) и описание структуры компонентов в рамках всей модели.

Дана общая информация о методологии оценки, приведенной в ISO/IEC 18045, и области действия системы оценки.

### 2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные документы. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения):

ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security -Part 2: Security functional components (Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в IT. Часть 2. Функциональные компоненты обеспечения безопасности)

ISO/IEC 15408-3:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components (Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в IT. Часть 3. Компоненты обеспечения гарантии безопасности)

ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security evaluation (Информационные технологии. Методы обеспечения безопасности. Методология оценки безопасности IT)

## 3 Термины и определения

В настоящем стандарте применяются следующие термины с соответствующими определениями:

Примечание - Данный раздел содержит только те термины, которые используются в ISO/IEC 15408. Специальные термины, используемые в ISO/IEC 15408, толкуются для ясности в контексте, в котором они используются и не требуют включения в настоящий раздел.

### 3.1 Термины и определения, употребляемые в ISO/IEC 15408

3.1.1 **Вредные воздействия** (adverse actions): Действия, осуществляемые агентом угрозы по отношению к ресурсу

3.1.2 **Активы** (assets): Объекты, которым придается важное значение при целевой оценке (TOE)

3.1.3 **Присваивание** (assignment): Спецификация какого-либо идентифицированного параметра в компоненте (ISO/IEC 15408) или требование

3.1.4 **Гарантия** (assurance): Основания уверенности, которым соответствует объект при оценке (TOE)

3.1.5 **Потенциал атаки** (attack potential): Мера усилий, затрачиваемых на атаку объекта оценки, выражаемая с учетом опыта, ресурсов и мотивации атакующего

3.1.6 **Аугментация** (augmentation): Добавление одного требования или более к программному пакету

3.1.7 **Данные аутентификации** (authentication data): Информация, используемая для верификации заявленной идентичности пользователя

3.1.8 **Авторизованный пользователь** (authorised user): Пользователь объекта оценки, который может выполнять операции в соответствии с функциональными требованиями безопасности (SFR)

3.1.9 **Класс** (class): Совокупность семейств ISO/IEC 15408, которые разделяют общую направленность

3.1.10 **Когерентный** (coherent): Логически упорядоченный и имеющий явный смысл

Примечание - В документации это касается как самого текста, так и структуры документа, с точки зрения его понятия для целевой аудитории.

3.1.11 **Полный** (complete): Свойство, обозначающее, что предоставлены все необходимые части объекта

Примечание - Что касается документации, это означает, что вся соответствующая информация в документации рассмотрена на таком подробном уровне, что дополнительных пояснений на данном уровне абстракции не требуется.

3.1.12 **Компонент** (component): Наименьший отделяемый набор элементов, на котором могут быть основаны требования

3.1.13 **Составной гарантийный пакет** (composed assurance package): Пакет гарантий, состоящий из требований, взятых из ISO/IEC 15408-3 из класса ACO), представляющих точку зрения по составу шкалы гарантий, предопределенной ISO/IEC 15408

3.1.14 **Подтверждать** (confirm): Заявить о подробном рассмотрении чего-либо с независимым определением достаточности

Примечание - Необходимый уровень строгости зависит от характера предмета. Данный термин применяется только к действиям оценщика.

3.1.15 **Подключаемость** (connectivity): Свойство объекта оценки, означающее возможность соединения с другими объектами IT, находящимися за пределами целевой оценки (TOE)

Примечание - Это включает в себя обмен данными с помощью проводных или беспроводных средств на каком-либо расстоянии, в какой-либо среде или конфигурации.

3.1.16 **Согласованный** (consistent): Характер отношений между двумя и более субъектами, в которых не имеется явных противоречий

3.1.17 **Противостоять**, **глагол** (counter, verb): Встречать нападение: при этом воздействие конкретной угрозы смягчается, но не обязательно ликвидируется

3.1.18 **Демонстрируемое соответствие** (demonstrable conformance): Связь между ST и PP, в которой ST предоставляет решение, решающее типовую проблему безопасности в PP

Примечание - PP и ST могут содержать совершенно разные заявления, которые обсуждают разные объекты, используют разные концепции и т. д. Демонстрируемое соответствие также подходит для типа TOE, в котором уже существуют несколько аналогичных PP, что позволяет автору ST одновременно заявлять о соответствии этим PP, экономя усилия.

3.1.19 **Демонстрировать** (demonstrate): Предоставлять заключение, полученное в результате анализа, в малой степени строгого, чем "доказательство"

3.1.20 **Зависимость** (dependency): Связь между компонентами: если требование, основанное на зависимом компоненте включено в PP, ST или пакет, то требование, основанное на компоненте, от которого идет зависимость, также должно быть включено в PP, ST или пакет.

3.1.21 **Описывать** (describe): Предоставлять конкретные детали по объекту

3.1.22 **Определять** (determine)**:** Утверждать конкретный вывод на основе независимого анализа с целью достижения конкретного заключения

Примечание - Использование этого термина подразумевает действительно независимый анализ, в отсутствие какого-либо предыдущего анализа. Сравните с терминами «подтвердить» или «проверить», которые подразумевают, что анализ уже выполнен, и его необходимо пересмотреть.

3.1.23 **Среда разработки** (development environmet): Среда, в которой разрабатывается объект оценки TOE

3.1.24 **Элемент** (element): Неделимый оператор нужд обеспечения безопасности

3.1.25 **Обеспечивать** (ensure): Гарантировать прочную причинную связь между действием и его последствиями

Примечание - Когда этому термину предшествует слово «помощь», это указывает на то, что следствие не является полностью определенным на основании одного только этого действия.

3.1.26 **Оценка** (evaluation): Произведение оценки PP, ST или TOE по определенным критериям

3.1.27 **Уровень гарантии оценки** (evaluation assurance level): Набор требований к гарантии, составленный в соответствии со стандартом ISO/IEC 15408-3, представляющим точку зрения по шкале гарантий, предопределенной ISO/IEC 15408, который формирует пакет гарантий

3.1.28 **Уполномоченный оценивающий орган** (evaluation authority): Орган, устанавливающий стандарты и контролирующий качество оценок, проводимых органами в конкретном сообществе, и внедряет ISO/IEC 15408 в данное сообщество посредством схемы оценки

3.1.29 **Схема оценки** (evaluation scheme): Административная и нормативная база, согласно которой ISO/IEC 15408 применяется уполномоченным оценивающим органом в рамках конкретного сообщества

3.1.30 **Исчерпывающий** (exhaustive): Характеристика методического подхода, предпринятого для проведения анализа или деятельности в соответствии с четким планом

Примечание - Данный термин используется в ISO/IEC 15408 в отношении проведения анализа или другой деятельности. Он связан с «систематическим», но является значительно более сильным, поскольку он указывает не только на то, что методический подход был применен для проведения анализа или деятельности в соответствии с четким планом, но и что план, который был соблюден, обеспечивал осуществление всех возможных путей.

3.1.31 **Объяснять** (explain): Давать аргумент, поясняющий причину выбора определенного хода действия

Примечание - Данный термин отличается от «описывать» и «демонстрировать». Он предназначен для ответа на вопрос «Почему?», и фактически необязательно утверждает, что выбранный курс действий был оптимальным.

3.1.32 **Расширение** (extension): Дополнение ST или PP функциональными требованиями, не содержащимися в ISO/IEC 15408-2, и/или гарантийными требованиями, не содержащимися в ISO/IEC 15408-3

3.1.33 **Внешний субъект** (external entity): Человек или субъект IT, с которыми допускается взаимодействие объекта оценки TOE за пределами границ TOE

Примечание - Внешний субъект, который тоже может считаться пользователем.

3.1.34 **Семейство** (family): Набор компонентов, которые имеют сходную цель, но отличаются по акценту или строгости

3.1.35 **Формальный** (formal): Выраженный ограниченным языком синтаксиса с определенной семантикой, основанной на четко определенных математических понятиях

3.1.36 **Методическая документация** (guidance documentation): Документация, описывающая осуществление, подготовку, операции, управление и/или использование TOE

3.1.37 **Идентичность** (identity): Представление, однозначно идентифицирующее объект (например, пользователя, процесс или диск) в контексте TOE

Примечание - Примером такого представления является строка. Для пользователя-человека представление может быть полным или сокращенным именем или псевдонимом (также уникальным).

3.1.38 **Неформальный** (informal): Изложенный простым языком

3.1.39 **Переходы между TSF** (inter TSF transfers): Передача данных между TOE и функционалом безопасности других доверенных IT-продуктов

3.1.40 **Внутренний канал коммуникации** (internal communication channel): Канал связи между отдельными частями TOE

3.1.41 **Внутренний переход TOE** (internal TOE transfer): Передача данных между отдельными частями TOE

3.1.42 **Внутренне согласованный** (internally consistent): Отсутствие очевидных противоречий между какими-либо аспектами субъекта

Примечание - В части документации это означает, что в документации не может быть никаких заявлений, противоречащих друг другу.

3.1.43 **Итерация** (iteration): Использование одного и того же компонента для выражения двух или более различных требований

3.1.44 **Обоснование** (justification): Анализ, приводящий к заключению

Примечание - «Обоснование» более строгий термин, чем демонстрация. Этот термин требует значительной строгости с точки зрения подробного объяснения каждого шага логического аргумента.

3.1.45 **Объект** (object): Пассивная структура в TOE, содержащая или получающая информацию, и над которым субъекты выполняют операции

3.1.46 **Операция** (operation): Модификация или повторение компонента

Примечание - Разрешенные операции над компонентами - присваивание, итерация, уточнение и выбор.

3.1.47 **Операция** (operation): Конкретный тип действия, выполняемый субъектом над объектом

3.1.48 **Операционная среда** (operational environment): Среда, в которой обрабатывается TOE

3.1.49 **Организационная политика обеспечения безопасности** (organizational security policy): Набор правил, процедур безопасности или инструкции для какой-либо организации

Примечание - Политика может относиться к конкретной операционной среде.

3.1.50 **Пакет** (package): Именованный набор функций безопасности или требований к гарантии обеспечения безопасности

Примечание - Примером пакета является “EAL 3”.

3.1.51 **Оценка профиля защиты** (Protection Profile evaluation): Оценка профиля защиты PP по определенным критериям

3.1.52 **Профиль защиты** (Protection Profile): Независимое от реализации заявление о потребностях обеспечения безопасности для TOE

3.1.53 **Доказать** (prove): Показать соответствие путем формального анализа в его математическом смысле

Примечание - Абсолютно строгий термин во всех отношениях. «Доказать» используется, когда необходимо показать соответствие между двумя представлениями TSF на высоком уровне строгости.

3.1.54 **Уточнение** (refinement): Добавление к компоненту деталей

3.1.55 **Роль** (role): Предопределенный набор правил, устанавливающих разрешенные взаимодействия между пользователем и TOE.

3.1.56 **Секрет** (secret): Информация, которая должна быть известна только авторизованным пользователям и/или TSF с целью исполнения конкретной SFP

3.1.57 **Безопасное состояние** (secure state): Состояние, в котором данные TSF являются согласованными, и TSF продолжают правильное выполнение SFR

3.1.58 **Атрибут безопасности** (security attribute): Свойство субъектов, пользователей (включая внешние IT-продукты), объектов, информации, сеансов и/или ресурсов, которые используются при определении SFR и значения которых используются для обеспечения соблюдения SFR

3.1.59 **Политика функций обеспечения безопасности** (security function policy): Набор правил, описывающих конкретное поведение безопасности, выполняемый TSF и выражаемый в виде набора SFR

3.1.60 **Цель обеспечения безопасности** (security objective): Заявление о намерении противостоять выявленным угрозам и/или соответствовать определенным политикам безопасности организации и/или допущениям

3.1.61 **Проблема безопасности** (security problem): Заявление, которое формальным образом определяет характер и сферу безопасности, с которыми TOE предназначено работать

Примечание - Данное утверждение состоит из следующего:
- угроз, которым должны противостоять TOE и его операционная среда,
- OSP, применяемые TOE и его рабочей средой, и
- допущения, которые поддерживаются для операционной среды TOE.

3.1.62 **Требование безопасности** (security requirement): Требование, изложенное на стандартизированном языке, которое предназначено для содействия достижению целей безопасности для TOE

3.1.63 **Цель безопасности** (Security Target): Зависящее от реализации заявление о потребностях безопасности для конкретного идентифицированного TOE

3.1.64 **Выбор** (selection): Выделение одного или нескольких элементов из списка в компоненте

3.1.65 **Полуформальный** (semiformal): Выраженный на ограниченном языке синтаксиса с определенной семантикой

3.1.66 **Конкретизировать** (specify): Предоставлять конкретные детали о субъекте строгим и точным образом

3.1.67 **Строгое соответствие** (strict conformance): Иерархическая связь между PP и ST, где все требования PP также существуют в ST

Примечание - Это отношение можно приблизительно определить как «ST должен содержать все утверждения, которые находятся в PP, но может содержать больше». Предполагается, что строгое соответствие будет использоваться в отношении строгих требований, которые должны соблюдаться единым образом.

3.1.68 **Оценка ST** (ST evaluation): Оценка ST по определенным критериям

3.1.69 **Субъект** (subject): Активное лицо в TOE, выполняющий операции над объектами

3.1.70 **Цель оценки** (target of evaluation): Набор программного обеспечения, прошивки и/или аппаратного обеспечения, сопровождаемый руководством

3.1.71 **Агент угрозы** (threat agent): Субъект, который может совершать негативные действия над ресурсами

3.1.72 **Оценка TOE** (TOE evaluation): Оценка TOE по определенным критериям

3.1.73 **Ресурс TOE** (TOE resource): Что-либо используемое или потребляемое в TOE

3.1.74 **Функциональность безопасности TOE** (TOE security functionality): комбинированные функциональные возможности всего аппаратного обеспечения, программного обеспечения и прошивки TOE, на которые необходимо полагаться для правильного применения SFR

3.1.75 **Отслеживать, глагол** (trace, verb): Проводить неофициальный анализ соответствия между двумя субъектами с минимальным уровнем строгости

3.1.76 **Переходы за пределами TOE**(transfers outside of the TOE): Передача данных посредством TSF объектам, находящимся вне контроля TSF

3.1.77 **Передача** (translation): Описывает процесс описания требований безопасности на стандартизованном языке.

Примечание - Использование термина «перевод» в этом контексте не является буквальным и не означает, что каждый SFR, выраженный на стандартизованном языке, также может быть передан обратно на цели безопасности.

3.1.78 **Доверенный канал** (trusted channel): Средство, с помощью которого TSF и другой доверенный IT-продукт могут взаимодействовать с необходимой уверенностью

3.1.79 **Доверенный IT-продукт** (trusted IT product): IT-продукт, не являющийся TOE, который имеет функциональные требования безопасности, административно координируемые с TOE, и предполагается, что он правильно выполняет свои функциональные требования безопасности

Примечание - Примером доверенного IT-продукта может служить отдельно оцененный.

3.1.80 **Доверенный путь** (trusted path): Средство, с помощью которого пользователь и TSF могут сообщаться с необходимой уверенностью

3.1.81 **Данные TSF** (TSF data): Данные для работы TOE, на которые полагается применение SFR

3.1.82 **Интерфейс TSF** (TSF interface): Средства, с помощью которых внешние объекты (или субъекты в TOE, но вне TSF) предоставляют данные в TSF, принимают данные из TSF и вызывают службы из TSF

3.1.83 **Данные пользователя** (user data): Данные для пользователя, которые не влияют на работу TSF

3.1.84 **Верифицировать** (verify): Строго рассмотреть в деталях с независимым определением достаточности

3.1.85 **Негативные действия** (adverse actions): Действия, выполняемые источником угрозы по отношению к активам

3.1.86 **Активы** (assets): Сущности, предположительно представляющие ценность для владельца ОО

3.1.87 **Назначение** (assignment): Спецификация определенного параметра в компоненте или требовании

3.1.88 **Доверие** (assurance): Основание для уверенности в том, что ОО отвечает конкретным ФТБ

3.1.89 **Потенциал нападения** (attack potential): Мера усилий, затрачиваемых при атаке на ОО, выраженная в показателях компетентности, ресурсов и мотивации нарушителя

3.1.90 **Усиление** (augmentation): Добавление одного или нескольких требований к пакету.

3.1.91 **Аутентификационные данные** (authentication data): Информация, используемая для верификации предъявленного идентификатора пользователя

3.1.92 **Уполномоченный пользователь** (authorised user): Пользователь ОО, которому в соответствии с ФТБ разрешено выполнять некоторую операцию

3.1.93 **Класс** (class): Совокупность семейств, объединенных общим назначением

3.1.94 **Четкий** (coherent): Логически упорядоченный и имеющий понятное значение

Примечание - В случае с документацией это относится как к имеющемуся тексту, так и к структуре документа в том смысле, понятен ли он его целевой аудитории.

3.1.95 **Полный** (complete): Свойство, обеспеченное наличием всех необходимых частей некоторой сущности.

Примечание - По отношению к документации это означает, что вся необходимая информация отражена в документации на уровне детализации, не требующем на данном уровне абстракции дальнейших пояснений

3.1.96 **Компонент** (component): Наименьшая выбираемая совокупность элементов, на которой могут основываться требования

3.1.97 **Составной пакет доверия** (composed assurance package): Пакет доверия, представляющий некоторое положение на предопределенной составной шкале доверия

3.1.98 **Подтвердить** (confirm): Декларировать, что что-то детально проверено с независимым определением достаточности

Примечание - Требуемый уровень строгости зависит от типа рассматриваемого предмета. Данный термин применим только к действиям оценщика.

3.1.99 **Внешняя связность** (connectivity): Свойство ОО, позволяющее ему взаимодействовать с сущностями ИТ, внешними по отношению к ОО

Примечание - Это взаимодействие включает обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации.

3.1.100 **Непротиворечивый** (consistent): Характеризует связь между двумя или более сущностями, указывая, что между этими сущностями нет никаких явных противоречий

3.1.101 **Противостоять** (counter): Характеризует противостояние некоторому нападению, при котором негативные последствия реализации некоторой конкретной угрозы уменьшаются, но не обязательно полностью ликвидируются

3.1.102 **Демонстрируемое соответствие** (demonstrable conformance): Связь между ЗБ и ПЗ, при которой ЗБ обеспечивает решение общей проблемы безопасности, определенной в ПЗ

Примечание - ПЗ и ЗБ могут содержать совершенно разные утверждения, относящиеся к разным сущностям, использующие разные понятия и т.д. Демонстрируемое соответствие также является подходящим для типа ОО, для которого уже существует несколько сходных ПЗ, позволяя разработчику ЗБ утверждать о соответствии одновременно всем этим ПЗ и, экономить трудозатраты.

3.1.103 **Демонстрировать** (demonstrate): Предоставить заключение, полученное в процессе анализа, который является менее строгим, чем "доказательство" ("proof")

3.1.104 **Зависимость** (dependency): Соотношение между компонентами, при котором, если некоторое требование, основанное на зависимом компоненте, включается в ПЗ, ЗБ или пакет, то и требование, основанное на компоненте, от которого зависит указанный выше компонент, должно быть, как правило, включено в ПЗ, ЗБ или пакет.

3.1.105 **Описывать** (describe): Представить конкретные подробности о некоторой сущности

3.1.106 **Делать заключение** (determine): Подтвердить некоторое заключение, основанное на независимом анализе для достижения этого заключения

Примечание - Использование данного термина подразумевает выполнение действительно независимого анализа, в условиях отсутствия какого бы то ни было предшествующего анализа. Термин "делать заключение" отличается от терминов "подтверждать" ("confirm") или "верифицировать" ("verify"), которые предполагают необходимость проверки ранее выполненного анализа.

3.1.107 **Среда разработки** (development environment): Среда, в которой осуществляется разработка ОО.

3.1.108 **Элемент** (element): Неделимое изложение некоторой потребности в безопасности

3.1.109 **Обеспечивать** (ensure): Гарантировать сильную причинно-следственную связь между некоторым действием и его последствиями

Примечание - Когда этому термину предшествует термин "способствовать", то это указывает, что одно данное действие не полностью определяет последствия.

3.1.110 **Оценка** (evaluation): Оценивание ПЗ, ЗБ или ОО по определенным критериям

3.1.111 **Оценочный уровень доверия** (evaluation assurance level): Набор требований доверия, представляющий некоторое положение на предопределенной шкале доверия и составляющий пакет доверия

3.1.112 **Орган оценки** (evaluation authority): Организация, устанавливающая стандарты и контролирующая качество оценок, проводимых организациями в пределах определенного сообщества, и обеспечивающая реализацию ISO/IEC 15408 для данного сообщества посредством системы оценки

3.1.113 **Система оценки** (evaluation scheme): Административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют ISO/IEC 15408

3.1.114 **Исчерпывающий** (exhaustive): Характеристика методического подхода, используемого применительно к проведению анализа или деятельности в соответствии с точно изложенным планом

Примечание - Этот термин используют применительно к проведению анализа или другой деятельности. Аналогичен термину "систематический" ("systematic"), но более строгий, так как указывает не только на то, что в соответствии с некоторым точно изложенным планом проведения анализа или другой деятельности был применен методический подход, но также и на то, что этот план достаточен для обеспечения проведения исследования по всем возможным направлениям.

3.1.115 **Объяснять** (explain): Предоставить аргументы, содержащие основания для выбора хода предпринимаемых действий

Примечание - Данный термин отличается от терминов "описывать" ("describe") и "демонстрировать" ("demonstrate"). Предназначен для ответа на вопрос "Почему?" без попытки аргументировать, что ход предпринимаемых действий обязательно оптимален.

3.1.116 **Расширение** (extension): Добавление в ЗБ или ПЗ функциональных требований, не содержащихся в ISO/IEC 15408-2, и/или требований доверия, не содержащихся в ISO/IEC 15408-3

3.1.117 **Внешняя сущность** (external entity): Человек или ИТ-сущность, взаимодействующие с ОО из-за пределов границ ОО

Примечание - В качестве внешней сущности может также рассматриваться пользователь ОО.

3.1.118 **Семейство** (family): Совокупность компонентов, которые направлены на достижение сходной цели, но отличаются акцентами или строгостью

3.1.119 **Формальный** (formal): Выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях.

3.1.120 **Документация руководств** (guidance documentation): Документация, описывающая поставку, установку, конфигурирование, эксплуатацию, управление и/или использование ОО

3.1.121 **Идентификатор** (identity): Представление, однозначно идентифицирующее сущность (например, пользователя, процесс или диск) в контексте конкретного ОО

Примечание - Примером такого представления может быть строка символов. Для человека-пользователя таким представлением может быть полное или сокращенное имя или (также уникальный) псевдоним.

3.1.122 **Неформальный** (informal): Выраженный на естественном языке

3.1.123 **Передача между ФБО** (inter TSF transfers): Передача данных между ОО и функциональными возможностями безопасности других доверенных продуктов ИТ.

3.1.124 **Внутренний канал связи** (internal communication channel): Канал связи между разделенными частями ОО

3.1.125 **Передача в пределах ОО** (internal TOE transfer): Передача данных между разделенными частями ОО

3.1.126 **Внутренне непротиворечивый** (internally consistent): Характеризует отсутствие очевидных противоречий между любыми аспектами сущности.

Примечание - Применительно к документации это означает, что в ней не может быть изложено что-либо, воспринимаемое как противоречащее чему-то другому.

3.1.127 **Итерация** (iteration): Использование компонента для выражения двух или более отдельных требований.

3.1.128 **Логическое обоснование** (justification): Анализ, приводящий к получению заключения

Примечание - Термин "логическое обоснование" является более строгим, чем термин "демонстрация". Этот термин требует точных и подробных объяснений каждого шага логических суждений.

3.1.129 **Объект** (object): Пассивная сущность в пределах ОО, которая содержит или получает информацию и над которой субъекты выполняют операции

3.1.130 **Операция** (над компонентом) (operation): Модификация или повторное использование компонента.

Примечание - Разрешенными операциями над компонентами являются назначение, итерация, уточнение и выбор.

3.1.131 **Операция** (над объектом) (operation): Определенный тип действия, выполняемого субъектом по отношению к объекту.

3.1.132 **Среда функционирования** (operation environment): Среда, в которой функционирует ОО.

3.1.133 **Политика безопасности организации** (organisational security policies): Совокупность правил, процедур или руководящих принципов в области безопасности для некоторой организации.

Примечание - Политика может быть также отнесена к какой-либо определенной среде функционирования.

3.1.134 **Пакет** (package): Именованная совокупность функциональных требований безопасности или требований доверия к безопасности

Примечание - Примером пакета может служить "ОУДЗ".

3.1.135 **Оценка профиля защиты** (protection profile evaluation): Оценивание ПЗ по определенным критериям.

3.1.136 **Профиль защиты** (protection profile): Независимое от реализации изложение потребностей в безопасности для некоторого типа ОО.

3.1.137 **Доказывать** (prove): Демонстрировать соответствие посредством формального анализа в математическом смысле

Примечание - Доказательство должно быть полностью строгим во всех отношениях. Термин "доказывать" используют, когда необходимо показать соответствие между двумя представлениями ФБО на высоком уровне строгости.

3.1.138 **Уточнение** (refinement): Добавление деталей в компонент

3.1.139 **Роль** (role): Предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО

3.1.140 **Секрет** (secret): Информация, которая должна быть известна только уполномоченным пользователям и/или ФБО для осуществления определенной ПФБ.

3.1.141 **Безопасное состояние** (secure state): Состояние, при котором данные ФБО являются непротиворечивыми и ФБО продолжают корректно реализовывать ФТБ

3.1.142 **Атрибут безопасности** (security attribute): Характеристика субъектов, пользователей (включая внешние продукты ИТ), объектов, информации, сеансов и/или ресурсов, которые используются при определении ФТБ, и значения которых используются при осуществлении ФТБ

3.1.143 **Политика функции безопасности** (security function policy): Совокупность правил, описывающих конкретный режим безопасности, реализуемый ФБО, и выраженных в виде совокупности ФТБ

3.1.144 **Цель безопасности** (security objective): Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям

3.1.145 **Проблема безопасности** (security problem): Изложение, которое в формализованном виде определяет характер и масштабы безопасности, которую должен обеспечивать ОО

Примечание - Данное изложение содержит сочетание:
- угроз, которым должно быть обеспечено противостояние со стороны ОО;
- ПБОр, осуществляемых ОО, и
- предположений, которые определены для ОО и его среды функционирования.

3.1.146 **Требование безопасности** (security requirement): Требование, изложенное на стандартизованном языке и направленное на достижение целей безопасности для ОО

3.1.147 **Задание по безопасности** (security target): Зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного ОО

3.1.148 **Выбор** (selection): Выделение одного или нескольких пунктов из перечня в компоненте

3.1.149 **Полуформальный** (semiformal): Выраженный на языке с ограниченным синтаксисом и определенной семантикой.

3.1.150 **Специфицировать** (specify): Предоставить конкретные подробности о некоторой сущности в строгой и точной форме

3.1.151 **Строгое соответствие** (strict conformance): Иерархическая связь между ПЗ и ЗБ, когда все требования из ПЗ также присутствуют в ЗБ

Примечание - Эта связь может быть определена как "ЗБ должен содержать все утверждения, которые присутствуют в ПЗ, но может содержать больше". Предполагается, что строгое соответствие будет применяться для обязательных требований, которые могут быть выполнены единственным способом.

3.1.152 **Оценка задания по безопасности** (security target evaluation): Оценивание ЗБ по определенным критериям

3.1.153 **Субъект** (subject): Активная сущность в ОО, выполняющая операции над объектами

3.1.154 **Объект оценки** (target of evaluation): Совокупность программного, программно-аппаратного и/или аппаратного обеспечения, возможно сопровождаемая руководствами

3.1.155 **Источник угрозы** (threat agent): Сущность, которая негативно воздействует на активы

3.1.156 **Оценка ОО** (TOE evaluation): Оценивание ОО по определенным критериям

3.1.157 **Ресурс ОО** (TOE resource): Все, что может быть использовано или потреблено ОО

3.1.158 **Функциональные возможности безопасности ОО** (TOE security functionality): Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения ОО, которые необходимо использовать для корректной реализации ФТБ

3.1.159 **Прослеживать или сопоставлять** (trace): Выполнять неформальный анализ соответствия между двумя сущностями с минимальным уровнем строгости

3.1.160 **Передача за пределы ОО** (transfers outside TOE): Опосредованная ФБО передача данных сущностям, не контролируемым ФБО

3.1.161 **Трансляция** (translation): Описание процесса изложения требований безопасности на стандартизованном языке.

Примечание - Использование термина "трансляция" не является буквальным и не подразумевает, что каждое ФТБ, выраженное на стандартизованном языке, может быть также обратно транслировано к целям безопасности.

3.1.162 **Доверенный канал** (trusted channel): Средство взаимодействия между ФБО и удаленным доверенным продуктом ИТ, обеспечивающее необходимую для этого степень уверенности в безопасности.

3.1.163 **Доверенный продукт ИТ** (trusted IT product): Продукт ИТ, отличный от ОО, для которого имеются свои функциональные требования, организационно скоординированные с ОО, и который, как предполагается, реализует свои функциональные требования корректно

Примечание - Примером доверенного продукта ИТ является продукт, который был отдельно оценен.

3.1.164 **Доверенный маршрут** (trusted path): Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую для этого степень уверенности в безопасности

3.1.165 **Данные ФБО** (TSF data): Данные, необходимые для функционирования ОО, на основе которых осуществляется реализация ФТБ.

3.1.166 **Интерфейс ФБО** (TSF interface): Средства, через которые внешние сущности (или субъект в ОО, но за пределами ФБО) передают данные к ФБО, получают данные от ФБО и обращаются к сервисам ФБО.

3.1.167 **Данные пользователя** (user data): Данные для пользователя, не влияющие на выполнение ФБО.

3.1.168 **Верифицировать** (verify): Провести строгую детальную проверку с независимым определением ее достаточности.

Примечание - См. также термин "подтверждать" (3.1.14). Термин "верифицировать" имеет более глубокий смысл. Он используется в контексте действий оценщика, когда требуются независимые усилия оценщика.

Примечание - Также см. «Подтвердить». Этот термин имеет более строгие коннотации. Термин «верифицировать» используется в контексте действий оценщика, когда от оценщика требуется независимое усилие.

### 3.2 Термины и определения, относящиеся к классу ADV

Примечание - Следующие термины используются в требованиях к внутреннему структурированию программного обеспечения. Некоторые из них взяты из IEEE Std 610.12-1990, Стандартного глоссария терминологии программной инженерии, Института инженеров по электротехнике и электронике.

3.2.1 **Администратор** (administrator): Лицо, имеющее уровень доверия в отношении всех политик, реализуемых TSF

Примечание - Не все PP или ST предлагают одинаковый уровень доверия для администраторов. Администраторы всегда придерживаются политик в ST TOE. Некоторые из этих политик могут быть связаны с функциональностью TOE, другие могут быть связаны с операционной средой.

3.2.2 **Дерево вызовов** (call tree): Идентифицирует модули в системе в виде диаграммы, показывающей, какие модули вызывают друг друга

Примечание - Адаптировано из IEEE Std 610.12-1990.

3.2.3 **Связность** (cohesion): Способ и степень, с которой задачи, выполняемые одним программным модулем, связаны друг с другом [IEEE Std 610.12-1990]

Примечание - Типы связности включают в себя совпадение, коммуникацию, функциональность, логичность, последовательность и временное. Эти типы связности описываются соответствующей терминологической записью.

3.2.4 **Случайная связность** (coincidental cohesion): Модуль с характеристикой выполнения несвязанных или слабо связанных между собой действий [IEEE Std 610.12-1990]

Примечание - См. также связность (3.2.3)

3.2.5 **Коммуникационная связность** (communicational cohesion): Модуль, содержащий функции, которые производят вывод или используют другие функции в модуле [IEEE Std 610.12-1990]

Примечания

1 см. также связность (3.2.3).

2 Примером коммуникационно-связного модуля является модуль проверки доступа, который включает в себя обязательные, дискреционные проверки и проверки возможностей.

3.2.6 **Анализ сложности** (complexity): Мера сложности для понимания программного обеспечения, и, анализа, тестирования и поддержки [IEEE Std 610.12-1990]

Примечание - Снижение уровня сложности - это конечная цель использования модульной декомпозиции, расслоения и минимизации. Контроль сцепления и связности в значительной степени способствует достижению этой цели.

Значительные усилия в области разработки программного обеспечения были потрачены на разработку метрик для оценки сложности исходного кода. Большинство этих показателей используют легко вычисляемые свойства исходного кода, такие как количество операторов и операнд, сложность граф потока управления (цикломатическая сложность), количество строк исходного кода, отношение комментариев к исполняемому коду, и аналогичные меры. Было установлено, что стандарты кодирования являются полезным инструментом для генерирования кода, который легче понять.

Семейство внутренних объектов TSF (ADV_INT) требует анализа сложности во всех компонентах. Ожидается, что разработчик предоставит поддержку претензий в отношении того, что имело место достаточное сокращение сложности. Эта поддержка может включать в себя стандарты программирования разработчика и указание того, что все модули соответствуют стандарту (или что есть некоторые исключения, которые оправданы аргументами разработки программного обеспечения). Он может включать результаты инструментов, используемых для измерения некоторых свойств исходного кода, или может включать другую поддержку, которую разработчик сочтет подходящей.

3.2.7 **Сцепление** (coupling): Способ и степень взаимозависимости между программными модулями [IEEE Std 610.12-1990]

Примечание - Типы сцепления включают вызов, общий и контентный интерфейс. Они характеризуются ниже.

3.2.8 **Сцепление вызовов** (call coupling): Связь между двумя модулями, связывающимися строго через свои документированные вызовы функций

Примечание - Примерами сцепления вызова являются данные, метка и управление

3.2.9 **Сцепление вызовов** (call coupling): Связь между двумя модулями, осуществляющая связь исключительно с использованием параметров вызова, которые представляют отдельные элементы данных

Примечание - См. также сцепление вызовов (3.2.8).

3.2.10 **Сцепление вызовов** (call coupling): Связь между двумя модулями, осуществляющая связь посредством использования параметров вызова, которые содержат несколько полей или которые имеют значимые внутренние структуры

Примечание - См. также сцепление вызовов (3.2.8).

3.2.11 **Сцепление вызовов** (call coupling): Связь между двумя модулями, если передается информация, предназначенная для воздействия на внутреннюю логику другого

Примечание - См. также сцепление вызовов (3.2.8).

3.2.12 **Сцепление по общей части** (common coupling): Взаимосвязь между двумя модулями, использующими общую область данных или другой общий системный ресурс

Примечание - Глобальные переменные указывают, что модули, использующие эти глобальные переменные, являются общими. Общая связь через глобальные переменные допускается, но только в ограниченной степени.

Например, переменные, помещенные в глобальную область, но используемые только одним модулем, помещены неправильно, и их следует удалить. Другими факторами, которые необходимо учитывать при оценке пригодности глобальных переменных, являются:

Число модулей, которые изменяют глобальную переменную: Только один модуль должен осуществлять контроль над содержимым глобальной переменной, но могут быть ситуации, когда второй модуль может разделять эту ответственность; В таком случае должно быть обеспечено достаточное обоснование. Недопустимо, чтобы эта ответственность разделялась более чем двумя модулями. (При проведении этой оценки следует уделять внимание определению модуля, фактически отвечающего за содержимое переменной: например, если одна единственная процедура используется для изменения переменной, но эта подпрограмма выполняет модификацию, запрошенную ее вызывающей стороной, то

она является вызывающим модулем, который несет ответственность, и может быть более одного такого модуля). Далее, в части определения сложности, если два модуля несут ответственность за содержимое глобальной переменной, должны быть четкие указания о координации изменений между ними.

Число модулей, которые ссылаются на глобальную переменную: нет ограничения на количество модулей, которые ссылаются на глобальную переменную, случаи, в которых многие модули делают такую ссылку, должны проверяться на предмет их достоверности и необходимости.

3.2.13 **Сцепление содержания** (content coupling): Взаимосвязь между двумя модулями, при которой делается прямая ссылка на внутренние элементы другой

Примечание - Примеры включают модификацию кода или ссылки на метки внутри этого модуля. В результате некоторая часть или все содержимое одного модуля эффективно включаются в другой. Сцепление контента можно рассматривать как использование нелицензированных интерфейсов модулей; это противоречит сцеплению вызовов, в котором используются только разрешенные интерфейсы модулей.

3.2.14 **Разделение предметных областей** (domain separation): Свойство архитектуры безопасности, по которому TSF определяет отдельные домены безопасности для каждого пользователя и для TSF и гарантирует, что ни один пользовательский процесс не сможет повлиять на содержимое домена безопасности другого пользователя или TSF

3.2.15 **Функциональная связность** (functional cohesion): Функциональное свойство модуля, которое выполняет действия, связанные с одной целью [IEEE Std 610.12-1990]

Примечание - Функционально связный модуль преобразует один тип ввода в один тип вывода, такой как менеджер стека или менеджер очередей. См. также связность (3.2.3).

3.2.16 **Взаимодействие** (interaction): Коммуникационная деятельность между субъектами

3.2.17 **Интерфейс** (interface): Средства взаимодействия с компонентом или модулем

3.2.18 **Наслоение** (layering): Метод разработки, при котором отдельные группы модулей (уровни) иерархически организованы так, чтобы иметь отдельные обязанности: один уровень зависит только от уровней ниже своего по иерархии для служб и предоставляет свои службы только для слоев над ним

Примечание - Строгое наслоение добавляет ограничение, согласно которому каждый слой получает услуги только из слоя, находящегося непосредственно под ним, а предоставляет услуги только тому уровню, который находится непосредственно над ним.

3.2.19 **Логическая связность** (loqical cohesion): Процедурная связность характеристики модуля, выполняющего аналогичные действия в разных структурах данных

Примечание - Модуль демонстрирует логическую связность, если его функции выполняют связанные, но разные операции на разных входах. См. также «связность».

3.2.20 **Модульная декомпозиция** (modular decomposition): Процесс разбиения системы на компоненты с целью облегчения проектирования, разработки и оценки [IEEE Std 610.12-1990]

3.2.21 **Невозможность обхода** (non–bypassability): Свойство архитектуры безопасности, посредством которого все действия, связанные с SFR, опосредуются TSF

3.2.22 **Разделение предметных областей** (security domains): Среды, предоставляемых TSF для использования недоверенными лицами, чтобы эти среды были изолированы и защищены друг от друга

3.2.23 **Последовательная связность** (sequential cohesion): Модуль, содержащий функции, каждая из которых выводит данные для следующей функции в модуле [IEEE Std 610.12-1990]

Примечание - Примером последовательно связного модуля является модуль, который содержит функции для фиксации записей аудита и ведения текущего счета накопленного количества нарушений аудита определенного типа.

3.2.24 **Программная инженерия** (software engineering): Применение систематического, дисциплинированного, поддающегося количественной оценке подхода к разработке и поддержке программного обеспечения; то есть применение инжиниринга к программному обеспечению [IEEE Std 610.12-1990]

Примечание - Как и в случае с инженерной практикой, при применении инженерных принципов следует придерживаться определенных принципов. На выбор влияет множество факторов, а не только применение мер модульной декомпозиции, расслоения и минимизации. Например, разработчик может спроектировать систему с предусмотренными приложениями, которые первоначально не будут реализованы. Разработчик может выбрать включение некоторой логики для обработки этих будущих приложений без их полной реализации; кроме того, разработчик может включить некоторые вызовы в еще не реализованные модули, оставляя заглушки вызовов. Обоснование разработчика для таких отклонений от хорошо структурированных программ должно оцениваться с использованием принципов, а также применения надлежащей дисциплины разработки программного обеспечения.

3.2.25 **Временная связность** (temporal cohesion): Характеристики модуля, содержащего функции, которые должны выполняться примерно в одно и то же время

Примечания

1 Адаптировано из [IEEE Std 610.12-1990].

2 Примеры временно связных модулей включают в себя модули инициализации, восстановления и завершения работы.

3.2.26 **Самозащита TSF** (TSF self-protection): Свойство архитектуры безопасности, при котором TSF не могут быть повреждены кодом или объектами, не являющимися TSF

### 3.3 Термины и определения, относящиеся к классу руководства

3.3.1 **Установка** (installation): Процедура, выполняемая пользователем, встраивающим TOE в его операционную среду и переводящим его в рабочее состояние

Примечание - Данная операция выполняется только один раз, после получения и принятия TOE. Ожидается, что TOE достигнет конфигурации, разрешенной ST. Если подобные процессы должны выполняться разработчиком, они обозначаются как «генерация» в течение ALC: поддержка жизненного цикла. Если TOE требует первоначального запуска, который не нужно повторять регулярно, этот процесс будет классифицироваться как установка.

3.3.2 **Операция** (operation): Этап использования TOE, включая «нормальное использование», администрирование и обслуживание TOE после поставки и подготовки

3.3.3 **Подготовка** (preparation): Деятельность на этапе жизненного цикла продукта, включающая принятие заказчиком поставленного TOE и его установку, которая может включать такие вещи, как загрузка, инициализация, запуск и продвижение TOE в состояние готовности к работе

### 3.4 Термины и определения, относящиеся к классу поддержка жизненного цикла

3.4.1 **Критерии принятия** (acceptance criteria): Критерии, которые должны применяться при выполнении процедур принятия (например, успешное рассмотрение документов или успешное тестирование в случае программного обеспечения, встроенного программного или аппаратного обеспечения)

3.4.2 **Процедуры принятия** (acceptance procedures): Процедуры, используемые для того, чтобы принять вновь созданные или измененные элементы конфигурации как часть TOE, или перенести их на следующий этап жизненного цикла

Примечание - Данные процедуры определяют роли лиц, ответственных за принятие, и критерии, которые должны применяться для решения о принятии.

Существует несколько типов ситуаций принятия, некоторые из которых могут пересекаться:

a) первичное принятие объекта в систему управления конфигурацией, в частности включение программного обеспечения, прошивки и аппаратных компонентов других производителей в TOE («интеграция»);

b) переход элементов конфигурации на следующую фазу жизненного цикла на каждом этапе построения TOE (например, модуль, подсистема, контроль качества готового TOE);

c) следующая за распределением элементов конфигурации (например, частей TOE или предварительных продуктов) между различными сторонами разработки;

d) после поставки TOE потребителю

3.4.3 **Управление конфигурацией CM** (configuration management CM): Дисциплина, применяющая техническое и административное руководство и надзор для идентификации и документирования функциональных и физических характеристик элемента конфигурации, контроля изменений этих характеристик, записи и обработки изменений и состояния реализации и проверки соответствия указанным требованиям

Примечание - Адаптировано из IEEE Std 610.12.

3.4.4 **Документация CM** (CM documentation): Вся документация CM, включая выход CM, список CM (список конфигураций), системные записи CM, документация по плану CM и использованию CM

3.4.5 **Очевидность управления конфигурацией** (configuration management evidence): Все то, что может быть использовано для подтверждения достоверности работы системы CM

Примечание - Например, вывод CM, обоснования, предоставленные разработчиком, наблюдения, эксперименты или опросы, сделанные оценщиком во время посещения объекта.

3.4.6 **Единица конфигурации** (configuration item): Объект, управляемый системой CM во время разработки TOE

Примечание - Это могут быть либо части TOE, либо объекты, связанные с разработкой TOE, такие как оценочные документы или инструменты разработки. Элементы CM могут храниться в системе CM (например, файлы) или по ссылке (например, в части оборудования) вместе с их версией.

3.4.7 **Список конфигураций** (configuration list): Выводной документ управления конфигурацией, в котором перечислены все элементы конфигурации для конкретного продукта вместе с точной версией каждого элемента управления конфигурацией, относящейся к конкретной версии всего продукта

Примечание - Этот список позволяет отличать элементы, принадлежащие оцениваемой версии продукта, от других версий этих элементов, принадлежащих другим версиям продукта. Окончательный список управления конфигурацией - это конкретный документ для конкретной версии конкретного продукта. (Конечно, список может быть электронным документом внутри инструмента управления конфигурацией, в этом случае его можно рассматривать как особый взгляд на систему или часть системы, а не на выход системы. Использование в оценке списка конфигураций, вероятно, будет поставляться как часть оценочной документации.) В списке конфигураций указаны элементы, которые находятся под управлением ALC_CMC для управления конфигурацией.

3.4.8 **Результаты управления конфигурацией** (configuration management output): Результаты, связанные с управлением конфигурацией, созданные или внедренные системой управления конфигурацией

Примечание - Эти результаты, связанные с управлением конфигурацией, могут иметь вид документов (например, заполненные бумажные бланки, записи системы управления конфигурацией, данные журналов, печатные копии и электронные выходные данные), а также действия (например, руководства для выполнения инструкций по управлению конфигурацией). Примерами таких результатов управления конфигурацией являются списки конфигурации, планы управления конфигурацией и/или поведением в течение жизненного цикла продукта.

3.4.9 **План управления конфигурацией** (configuration management plan): Описание использования системы управления конфигурацией для TOE

Примечание – Цель выпуска плана управления конфигурацией состоит в том, чтобы сотрудники могли ясно видеть, что им нужно делать. С точки зрения общей системы управления конфигурацией это можно рассматривать как выходной документ (т.к. он может быть создан как часть приложения системы управления конфигурацией). С точки зрения конкретного проекта это документ использования, так как члены проектной группы используют его, чтобы понять шаги, которые они должны выполнить в ходе проекта. План управления конфигурацией определяет использование системы для конкретного продукта; одна и та же система может использоваться в разной степени для других продуктов. Это означает, что в плане управления конфигурацией определяется и описывается выход системы управления конфигурацией компании, которая используется во время разработки TOE.

3.4.10 **Система управления конфигурацией** (configuration management system):
Набор процедур и инструментов (включая их документацию), используемых разработчиком для разработки и поддержки конфигураций его продуктов в течение их жизненного цикла

Примечание – Системы управления конфигурацией могут иметь различную степень строгости и функциональности. На более высоких уровнях системы управления конфигурацией могут быть автоматизированы, с устранением дефектов, контролем изменений и другими механизмами отслеживания.

3.4.11 **Записи системы управления конфигурацией** (configuration management system records): Результат, полученный в ходе работы системы управления конфигурацией, документирующей важные действия по управлению конфигурацией

Примечание – Примерами записей системы управления конфигурацией являются формы управления изменениями элементов управления конфигурацией или формы утверждения доступа к элементам управления конфигурацией.

3.4.12 **Инструменты управления конфигурацией** (configuration management tools): Управляемые вручную или автоматизированные инструменты, реализующие или поддерживающие систему управления конфигурацией

Примечание – Например, инструменты для управления версиями частей TOE

3.4.13 **Документация пользования управлением конфигурацией** (confiquration management usage documentation): Часть системы управления конфигурацией, в которой описывается определение системы управления конфигурацией и применение с использованием, например, справочников, правил и/или документации инструментов и процедур

3.4.14 **Поставка** (delivery): Передача готового TOE из производственной среды в руки заказчика

Примечание – Данная фаза жизненного цикла продукта может включать в себя упаковку и хранение на месте разработки, но не включает перевозку незавершенного TOE или его частей между разными разработчиками или различными объектами разработки.

3.4.15 **Разработчик** (developer): Организация, ответственная за разработку TOE.

3.4.16 **Разработка** (development): Этап жизненного цикла продукта, связанный с созданием представления реализации TOE

Примечание - На протяжении всего ALC: требования к поддержке жизненного цикла, разработка и связанные с ним термины (разработчик, разрабатывать) в более общем смысле подразумевают разработку и производство.

3.4.17 **Инструменты** разработки (development tools): Инструменты (включая тестовое программное обеспечение, если применимо), поддерживающие разработку и производство TOE

Примечание - Например, для программного обеспечения TOE, инструментами разработки являются языки программирования, компиляторы, компоновщики и генерирующие инструменты.

3.4.18 **Представление реализации** (implementation representation): Наименее абстрактное представление TSF, в частности то, которое используется для создания самого TSF без дальнейшего уточнения дизайна

Примечание – Исходный код, который затем компилируется, или чертеж оборудования, используемый для создания реального оборудования, являются примерами частей представления реализации.

3.4.19 **Жизненный цикл** (life-cycle): Последовательность этапов существования объекта (например, продукта или системы) во времени

3.4.20 **Определение жизненного цикла** (life-cycle definition): Определение модели жизненного цикла

3.4.21 **Модель жизненного цикла** (life-cycle model): Описание этапов и их взаимосвязей, которые используются в управлении жизненным циклом определенного объекта, описание последовательности этапов и характеристик высокого уровня, которые имеют этапы

Примечание – См. также рисунок 1.

3.4.22 **Производство** (production): Фаза жизненного цикла производства следует за этапом разработки и заключается в преобразовании представления реализации в реализацию TOE, то есть в состояние, приемлемое для поставки заказчику

Примечание - Данный этап может включать изготовление, интеграцию, генерацию, внутренние перевозки, хранение и маркировку TOE.

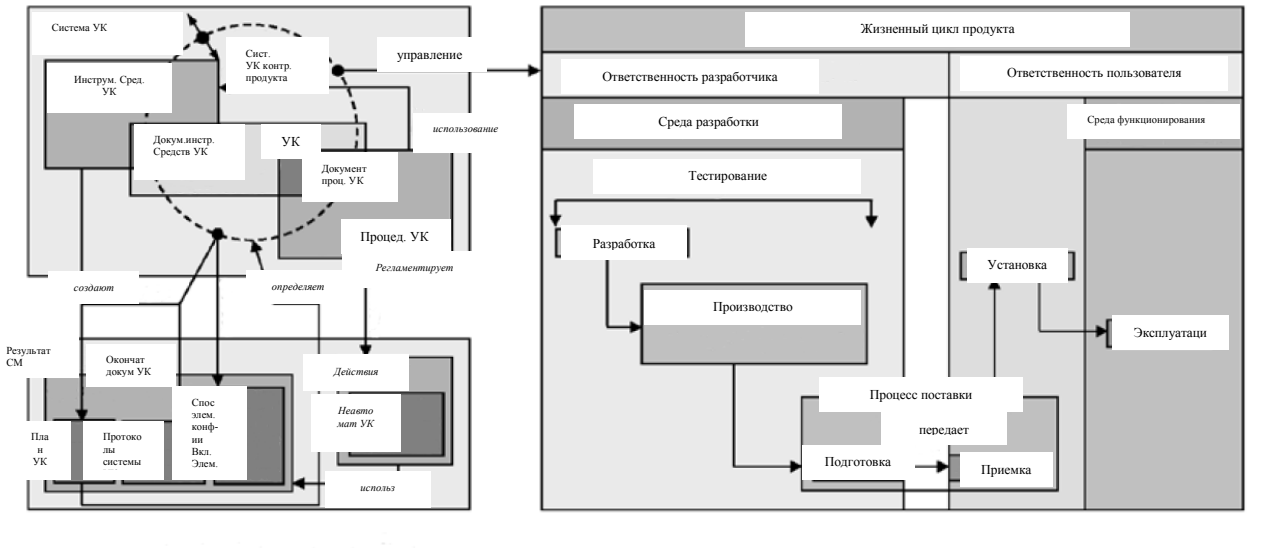



**Рисунок 1 - Терминология СМ и жизненного цикла продукта**

### 3.5 Термины и определения, относящиеся к классу оценки уязвимостей

3.5.1 **Скрытый канал** (covert channel): Защищенный, не указанный сигнальный канал, который позволяет пользователю тайно противостоять многоуровневой политике разделения и требованиям ненаблюдаемости TOE

3.5.2 **Обнаруженная потенциальная уязвимость** (encountered potential vulnerabilities): Потенциальная слабая сторона TOE, выявленная оценщиком при выполнении оценочных действий, которая может быть использованы для нарушения SFR

3.5.3 **Эксплуатационная уязвимость** (exploitable vulnerability): Слабая сторона в TOE, которая может быть использована для нарушения SFR в рабочей среде для TOE

3.5.4 **Мониторинговые атаки** (monitoring attacks): Типовая категория методов атаки, которая включает в себя методы пассивного анализа, направленные на раскрытие чувствительных внутренних данных TOE, путем использования TOE в соответствии с руководящими документами

3.5.5 **Потенциальная уязвимость** (potential vulnerability): Подозреваемая, но не подтвержденная слабая сторона

Примечание - Подозрение на основании постулированного пути атаки с целью нарушения SFR.

3.5.6 **Остаточная уязвимость** (residual vulnerability): Слабая сторона, которая не может быть использована в рабочей среде для TOE, но может использоваться для нарушения SFR атакующим с большим потенциалом, чем ожидается в рабочей среде для TOE

3.5.7 **Уязвимость** (vulnerability): Слабое место в TOE, которое может быть использовано для нарушения SFR в какой-либо среде

### 3.6 Термины и определения, относящиеся к классу композиции

3.6.1 **Компонент базы** (base component): Субъект в составном TOE, который сам был предметом оценки, предоставления услуг и ресурсов зависимому компоненту

3.6.2 **Совместимые (компоненты)** (compatible (components): Свойство компонента, способного предоставлять услуги, требуемые другим компонентом, через соответствующие интерфейсы каждого компонента в согласованных рабочих условиях

3.6.3 **Компонент TOE** (component TOE): Успешно оцененный TOE, являющийся частью другого составного TOE

3.6.4 **Составной TOE** (composed TOE): TOE, состоящий только из двух или более компонентов, которые успешно прошли оценку

3.6.5 **Зависимый компонент** (dependent component): Субъект в составном TOE, который сам является предметом оценки, опираясь на положение о службах с помощью базового компонента

3.6.6 **Функциональный интерфейс** (functional interface): Внешний интерфейс, обеспечивающий пользователю доступ к функциональным возможностям TOE, который о не участвует в обеспечении функциональных требований безопасности

Примечание - В составном TOE - это интерфейсы, предоставляемые базовым компонентом, которые требуются зависимым компонентом для поддержки работы составного TOE.

## 4 Обозначения и сокращения

ИПП (API) - интерфейс прикладного программирования
СПГ (CAP) - составной пакет гарантий
УК (CM) - управление конфигурацией
РКД (DAC) - разграничительный контроль доступа
УГО (EAL) - уровень гарантии оценки
ГЦ (GHz) - гигагерц
ГПИ (GUI) - графический пользовательский интерфейс
ИС (IC) - интегральная схема
УВВ (IOCTL) - управление вводом-выводом
ИП (IP) - интернет-протокол
ИТ (IT) - информационные технологии
МБ (MB) - мегабайт
ОС (OS) - операционная система
ОПБ (OSP) - организационная политика безопасности
ПК (PC) - персональный компьютер
СПК (PCI) - соединение периферийных компонентов
ИОК (PKI) - инфраструктура открытого ключа
ПЗ (PP) - профиль защиты
ОЗУ (RAM) - оперативное запоминающее устройство
ПДВП (RPC) - протокол дистанционного вызова процедур
ТГБ (SAR) - требование гарантии безопасности
ФТБ (SFR) - функциональное требование безопасности
ПОФБ (SFP) - политика обеспечений функций безопасности
ОПБ (SPD) - определение проблемы безопасности
ЗБ (ST) - задание по безопасности
УПТ (TCP) - управляющий протокол передачи
ОО (TOE)- объект оценки
ФБО (TSF) - функциональные возможности безопасности ОО
ИФБО (TSFI) - интерфейс ФБО
ВЧС (VPN)- виртуальная частная сеть

## 5 Краткий обзор

### 5.1 Общие положения

В этом разделе представлены основные концептуальные положения ISO/IEC 15408. В нем определены понятие "ОО", категории пользователей ISO/IEC 15408, контекст оценки и принятый подход к дальнейшему представлению материала в ISO/IEC 15408.

### 5.2 Объект оценки (ОО)

ISO/IEC 15408 является гибким в отношении того, что оценивается и, не привязывается, к границам только продуктов ИТ.

В контексте оценки в ISO/IEC 15408 используется термин "ОО" (объект оценки).

ОО определяется как набор программных, программно-аппаратных и/или аппаратных средств, возможно сопровождаемых руководствами.

Допускается, что ОО представляет собой продукт ИТ. ОО может быть продуктом ИТ, частью продукта ИТ, набором продуктов ИТ, уникальной технологией, которая может быть никогда не будет реализована в виде продукта, или сочетанием указанных вариантов.

Относительно ISO/IEC 15408 четкое соотношение между ОО и любыми продуктами ИТ является важным только в одном аспекте: оценку ОО, содержащего часть продукта ИТ, не следует ошибочно представлять как оценку продукта ИТ в целом.

Примерами ОО являются:

- прикладная программа;
- операционная система;
- прикладная программа в сочетании с операционной системой;
- прикладная программа в сочетании с операционной системой и рабочей станцией;
- операционная система в сочетании с рабочей станцией;
- интегральная схема смарт-карты;
- локальная вычислительная сеть, включая все терминалы, серверы, сетевое оборудование и программные средства;
- приложение базы данных за исключением программных средств удаленного клиента, ассоциируемых с приложением базы данных.

#### 5.2.1 Различные представления ОО

В ISO/IEC 15408 ОО может встречаться в нескольких представлениях (для программного ОО):

- список файлов в системе управления конфигурацией;
- отдельная мастер-копия, которая была только что скомпилирована;
- коробка, содержащая компакт-диск и руководства, готовая для поставки потребителю;
- установленная и функционирующая версия.

Все из перечисленного считается ОО: где в дальнейшем в ISO/IEC 15408 используется термин "ОО", его конкретное представление определяется из контекста.

#### 5.2.2 Различные конфигурации ТОЕ

Продукты ИТ могут быть сконфигурированы различными способами путем включения или отключения различных опций при инсталляции. Так как в процессе

оценки по ISO/IEC 15408 будет определяться, удовлетворяет ли ОО определенным требованиям, данная гибкость конфигурации может привести к проблемам, так как все возможные конфигурации ОО должны удовлетворять этим требованиям. По этим причинам частыми являются случаи, когда руководства как часть ОО строго ограничивают возможные конфигурации ОО. Руководства ОО могут отличаться от общих руководств для продукта ИТ.

Примером является продукт ИТ "Операционная система". Этот продукт может быть сконфигурирован различными способами (например, типы пользователей, количество пользователей, типы разрешенных/неразрешенных внешних подключений, включение/отключение опций и др.)

Если такой продукт ИТ должен быть ОО и оценен на соответствие обоснованному набору требований, его конфигурацию следует намного более тщательно контролировать, так как многие опции (например, разрешение всех типов внешних подключений или отсутствие необходимости аутентификации администратора системы) приведут к тому, что ОО не будет удовлетворять требованиям.

По этой причине нормальным бы являлось дифференциация руководств для продукта ИТ (допускающих много конфигураций) и руководств для ОО (допускающих только одну конфигурацию или только те конфигурации, которые не отличаются относительно способов обеспечения безопасности).

Если руководства ОО допускают более одной конфигурации, то все эти конфигурации вместе именуются "ОО", и каждая такая конфигурация должна удовлетворять требованиям, предъявляемым к ОО.

### 5.3 Пользователи ISO/IEC 15408

В оценке характеристик безопасности ОО заинтересованы в основном три группы пользователей: потребители, разработчики и оценщики. Критерии, представленные в настоящем документе, структурированы в интересах этих групп, потому что именно они рассматриваются как основные пользователи ISO/IEC 15408. Далее объясняется, какую пользу могут принести критерии каждой из этих групп.

#### 5.3.1 Потребители

ISO/IEC 15408 разработан, чтобы обеспечить посредством оценки удовлетворение запросов потребителей, поскольку это является основной целью и логическим обоснованием процесса оценки.

Результаты оценки помогают потребителям решить, удовлетворяет ли ОО их потребности в безопасности. Эти потребности определяются как следствие анализа рисков, а также направленности политики безопасности. Потребители могут также использовать результаты оценки для сравнения различных ОО. Иерархическое представление требований доверия способствует этому.

ISO/IEC 15408 предоставляет потребителям, особенно входящим в группы и сообщества с едиными интересами, независимую от реализации структуру, называемую профилем защиты (ПЗ), для однозначного выражения их требований безопасности.

#### 5.3.2 Разработчики

ISO/IEC 15408 предназначен для поддержки разработчиков при подготовке к оценке своих ОО и содействии в ее проведении, а также при установлении требований безопасности, которым должны удовлетворять эти ОО. Данные требования содержатся в

зависимой от реализации конструкции, называемой заданием по безопасности (ЗБ). Эти ЗБ могут базироваться на одном или нескольких ПЗ, чтобы показать, что ЗБ соответствуют требованиям безопасности, предъявленных потребителями, которые установлены в данных ПЗ.

ISO/IEC 15408 можно использовать для определения обязанностей и действий по предоставлению свидетельств, необходимых при проведении оценки ОО по этим требованиям. Он также определяет содержание и представление таких свидетельств.

### 5.3.3 Оценщики

В ISO/IEC 15408 содержатся критерии, предназначенные для использования оценщиками ОО при формировании заключения о соответствии объектов оценки предъявленным к ним требованиям безопасности. В ISO/IEC 15408 дается описание совокупности основных действий, выполняемых оценщиком. При этом в ISO/IEC 15408 не определены процедуры, которых следует придерживаться при выполнении этих действий. Дальнейшая информация по этим процедурам приведена в 5.5.

### 5.3.4 Прочие

Хотя ISO/IEC 15408 ориентирован на определение и оценку характеристик безопасности ИТ для объектов оценки, он также может служить справочным материалом для всех, кто интересуется вопросами безопасности ИТ или несет ответственность за них. Среди них можно выделить, например, следующие группы, представители которых смогут извлечь пользу из информации, приведенной в ISO/IEC 15408:

a) лица, ответственные за техническое состояние оборудования, и сотрудники служб безопасности, ответственные за определение и выполнение политики и требований безопасности организации в области ИТ;

b) аудиторы как внутренние, так и внешние, ответственные за оценку адекватности безопасности ИТ-решения (которое может состоять из ОО или включать ОО);

c) проектировщики систем безопасности, ответственные за характеристики безопасности продуктов ИТ;

d) аттестующие, ответственные за приемку ИТ-решения в эксплуатацию в конкретной среде;

e) заявители, заказывающие оценку и обеспечивающие ее проведение;

f) органы оценки, ответственные за руководство и надзор за программами проведения оценок безопасности ИТ.

## 5.4 Различные части ISO/IEC 15408

ISO/IEC 15408 состоит из нескольких отдельных, но взаимосвязанных частей, перечисленных ниже. Термины, используемые при описании отдельных частей ISO/IEC 15408, приведены в разделе 6.

a) Часть 1 "Введение и общая модель" является введением в ISO/IEC 15408. В ней определяются общие понятия и принципы оценки безопасности ИТ и приводится общая модель оценки.

b) Часть 2 "Функциональные компоненты безопасности" устанавливает совокупность функциональных компонентов, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать функциональные требования к ОО. ISO/IEC 15408-2 содержит каталог функциональных компонентов, систематизированных по семействам и классам.

с) Часть 3 "Компоненты доверия к безопасности" устанавливает совокупность компонентов доверия, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать требования доверия к ОО. ISO/IEC 15408-3 содержит каталог компонентов доверия, систематизированных по семействам и классам. Кроме того, в ISO/IEC 15408-3 определены критерии оценки профилей защиты и заданий по безопасности и представлены семь предопределенных пакетов доверия, которые названы оценочными уровнями доверия (ОУД).

В поддержку трех частей ISO/IEC 15408, перечисленных выше, опубликованы и другие документы. Например, ISO/IEC 18045 предоставляет методологию оценки безопасности ИТ, используя ISO/IEC 15408 как основу. Также будут опубликованы и другие документы, включая нормативно-методические материалы и руководства.

В таблице 1 показано, в каком качестве различные части ISO/IEC 15408 будут представлять интерес для каждой из трех основных групп пользователей ISO/IEC 15408.

**Таблица 1 - Рабочий план к «Критериям оценки обеспечения безопасности IT»**

| асти | Потребители | Разработчики | Оценщики |
|---|---|---|---|
| | Используют для получения общих сведений и должны использовать в качестве справочного руководства и руководства по структуре профилей защиты | Используют для получения общих сведений и в качестве справочного руководства. Должны использовать при разработке спецификаций безопасности для объектов оценки | Должны использовать в качестве справочного руководства и руководства по структуре профилей защиты и заданий по безопасности |
| | Используют в качестве руководства и справочника при формулировании требований для ОО | Должны использовать в качестве справочника при интерпретации изложения функциональных требований и формулировании функциональных спецификаций для объектов оценки | Должны использовать в качестве справочного руководства при интерпретации изложения функциональных требований |
| | Используют в качестве руководства при определении требуемых уровней доверия | Используют в качестве справочника при интерпретации изложения требований доверия и определении подходов к установлению доверия к объектам оценки | Используют в качестве справочного руководства при интерпретации изложения требований доверия |

### 5.5 Контекст оценки

Для достижения большей сравнимости результатов оценок их следует проводить в рамках официальной системы оценки, которая устанавливает стандарты, контролирует качество оценок и определяет нормы, которыми необходимо руководствоваться организациям, проводящим оценку, и самим оценщикам.

В ISO/IEC 15408 (во всех частях) не излагаются требования к правовой базе. Однако согласованность правовой базы различных органов оценки является необходимым условием достижения взаимного признания результатов оценок.

Второе направление достижения большей сравнимости результатов оценок заключается в использовании общей методологии получения этих результатов. Для всех частей ISO/IEC 15408 такая методология приведена в ISO/IEC 18045.

Использование общей методологии оценки позволяет достичь повторяемости и объективности результатов, но только этого недостаточно. Многие из критериев оценки требуют привлечения экспертных решений и базовых знаний, добиться согласованности которых бывает нелегко. Для повышения согласованности выводов, полученных при оценке, ее конечные результаты могут быть представлены на сертификацию.

Процесс сертификации представляет собой независимую экспертизу результатов оценки, которая завершается их утверждением или выдачей сертификата. Сведения о сертификатах публикуются и являются общедоступными. Сертификация является средством обеспечения большей согласованности в применении критериев безопасности ИТ.

Системы оценки и процессы сертификации находятся в ведении органов оценки, управляющих системами и процессами оценки, и не входят в область действия ISO/IEC 15408 (всех частей).

## 6 Общая модель

### 6.1 Введение к общей модели

В этом разделе представлены общие понятия, используемые во всех частях ISO/IEC 15408, включая контекст использования этих понятий, и подход ISO/IEC 15408 к их применению. ISO/IEC 15408-2 и ISO/IEC 15408-3, к которым должны обращаться пользователи ISO/IEC 15408-1, развивают эти понятия в рамках описанного подхода. Кроме того, тем пользователям ISO/IEC 15408-1, которые собираются выполнять виды деятельности по оценке, необходим ISO/IEC 18045. Данный раздел предполагает наличие определенных знаний по безопасности ИТ и не предназначен для использования в качестве учебного пособия в этой области.

Безопасность в ISO/IEC 15408 (во всех частях) рассмотрена с использованием совокупности понятий безопасности и терминологии. Их понимание является предпосылкой эффективного использования ISO/IEC 15408 (всех частей). Однако сами по себе эти понятия имеют самый общий характер и не предназначены для ограничения класса проблем безопасности ИТ, к которым применим ISO/IEC 15408.

### 6.2 Активы и контрмеры

Безопасность связана с защитой активов. Активы - это сущности, представляющие ценность для кого-либо. Примеры активов включают:

- содержание файла или сервера;
- подлинность голосов, поданных на выборах;
- доступность процесса электронной коммерции;
- возможность использовать дорогостоящий принтер;
- доступ к средствам ограниченного доступа.

Но так как ценность - это весьма субъективное понятие, то почти все, что угодно, может рассматриваться в качестве активов.

Среда, в которой размещаются эти активы, называется средой функционирования. Примерами (аспектами) среды функционирования являются:

- компьютерное помещение в банке;
- компьютерная сеть, подключенная к Интернету;

- локальная вычислительная сеть (ЛВС);
- офисная среда.

Многие активы представлены в виде информации, которая хранится, обрабатывается и передается продуктами ИТ таким образом, чтобы удовлетворить требования владельцев этой информации. Владельцы информации вправе требовать, чтобы доступность, распространение и модификация любой такой информации строго контролировались и активы были защищены от угроз контрмерами. Рисунок 2 иллюстрирует высокоуровневые понятия безопасности и их взаимосвязь

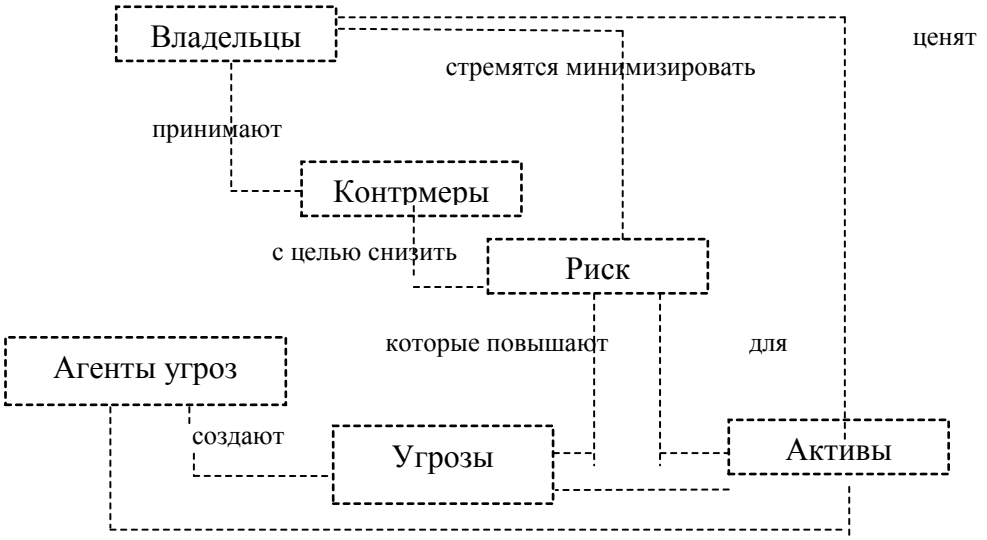



**Рисунок 2 - Концепции обеспечения безопасности и связи**

За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Примерами источников угрозы являются хакеры, злонамеренные пользователи, незлонамеренные пользователи (которые иногда делают ошибки), компьютерные процессы и сбои.

Владельцы активов будут воспринимать такие угрозы как потенциальную возможность нанесения такого ущерба активам, при котором ценность активов для владельцев уменьшилась бы. Специфичный для безопасности ущерб состоит в следующем (но не ограничивается этим): потеря конфиденциальности активов, потеря целостности активов или потеря доступности активов.

Эти угрозы увеличивают риски для активов, зависящие от вероятности реализации угрозы и ущерба активам при реализации рассматриваемой угрозы. Для того чтобы уменьшить риски для активов, реализуются контрмеры. Эти контрмеры могут включать ИТ-контрмеры (такие как межсетевые экран и смарт-карты) и не-ИТ-контрмеры (такие как охрана и процедуры). Более широкое рассмотрение контрмер (мер безопасности), а также способов их реализации и управления ими представлено в ISO/IEC 27001 и ISO/IEC 27002.

Поскольку за активы могут нести (несут) ответственность их владельцы, то им следует иметь возможность отстаивать принятое решение о приемлемости риска для активов, создаваемого угрозами.

При отстаивании этого решения должна иметься возможность продемонстрировать два важных момента, что:

- контрмеры являются достаточными, если контрмеры выполняют то, что заявлено, и угрозам, направленным на активы, обеспечивается противостояние;
- контрмеры являются корректными, если контрмеры выполняют то, что заявлено.

Многие владельцы активов не имеют знаний, опыта или ресурсов, необходимых для вынесения суждения о достаточности и корректности контрмер, и при этом они могут не захотеть полагаться исключительно на утверждения разработчиков этих контрмер. Вследствие этого данные потребители могут захотеть повысить свою уверенность в достаточности и корректности некоторых или всех контрмер путем заказа оценки этих контрмер.


**Рисунок 3 – Понятия, используемые при оценке, и их взаимосвязь**

### 6.2.1 Достаточность контрмер

При оценке достаточность контрмер анализируется через конструкцию, называемую заданием по безопасности. В данном пункте представлен упрощенный обзор этой конструкции: более детальное и полное описание можно найти в приложении А.

Задание по безопасности начинается с описания активов и угроз этим активам. Затем в задании по безопасности описываются контрмеры (в форме целей безопасности) и демонстрируется, что данные контрмеры являются достаточными, чтобы противостоять описанным угрозам: если контрмеры осуществляют то, что заявлено по отношению к ним, то обеспечено противостояние угрозам

Далее в задании по безопасности контрмеры делятся на две группы:

a) цели безопасности для ОО: они описывают контрмеры, корректность которых будет определяться при оценке;

b) цели безопасности для среды функционирования: они описывают контрмеры, корректность которых не будет определяться при оценке.

Причинами данного разделения являются:

- ISO/IEC 15408 применим только для оценивания корректности контрмер ИТ. Не-ИТ-контрмеры (например, сотрудники службы безопасности, процедуры) всегда относят к среде функционирования;

- оценивание корректности контрмер требует затрат времени и денег, возможно делая неосуществимой оценку корректности всех контрмер ИТ;

- корректность некоторых контрмер ИТ может быть уже оценена в ходе другой оценки. Экономически неэффективно проводить их повторную оценку.

В задании по безопасности для ОО (корректность контрмер ИТ которого будут оценивать в процессе оценки) требуется дальнейшая детализация целей безопасности для ОО в функциональных требованиях безопасности (ФТБ). Эти ФТБ формулируют на стандартном языке (описанном в ISO/IEC 15408-2), чтобы обеспечить точность и облегчить сопоставимость.

В задании по безопасности демонстрируется, что:

- ФТБ удовлетворяют целям безопасности для ОО;

- цели безопасности для ОО и цели безопасности для среды функционирования противостоят угрозам;

- ФТБ и цели безопасности для среды функционирования противостоят угрозам.

Корректный ОО (удовлетворяющий ФТБ) в сочетании с корректной средой функционирования (удовлетворяющей целям безопасности для среды функционирования) будет противостоять угрозам. Ниже отдельно рассматриваются корректность ОО и корректность среды функционирования.

### 6.2.2 Корректность ОО

Объект оценки может быть неправильно спроектирован и реализован и может, содержать ошибки, которые ведут к уязвимостям. Посредством использования этих уязвимостей, нарушители могут причинить ущерб и/или несанкционированно использовать активы.

Эти уязвимости могут являться результатом случайных ошибок, сделанных в течение разработки, ненадлежащего проектирования, преднамеренного внедрения вредоносного кода, ненадлежащего тестирования и др.

Для определения корректности ОО могут выполняться различные виды деятельности, такие как:

- тестирование ОО;

- исследование различных проектных представлений ОО;

- исследование физической безопасности среды разработки ОО.

Задание по безопасности обеспечивает структурированное описание этих видов деятельности для определения корректности в форме требований доверия к безопасности (ТДБ). Эти ТДБ формулируются на стандартном языке (описанном в ISO/IEC 15408-3), чтобы обеспечить точность и облегчить сопоставимость.

Если ТДБ удовлетворяются, то существует доверие к корректности ОО, и, меньше вероятность, что ОО содержит уязвимости, которые могут быть использованы нарушителем. Величина доверия, которое существует по отношению к корректности ОО, определяется самими ТДБ: несколько "слабых" ТДБ приведут к малому доверию, большое число "сильных" ТДБ приведет к большему доверию.

### 6.2.3 Корректность среды функционирования

Среда функционирования также может быть неправильно спроектирована и реализована и может, содержать ошибки, которые ведут к уязвимостям. Посредством использования этих уязвимостей, нарушители могут причинить ущерб и/или несанкционированно использовать активы.

Однако в ISO/IEC 15408 доверие не приобретается при рассмотрении корректности среды функционирования. Или, другими словами, среда функционирования не оценивается (см. 6.3).

Что касается оценки, то предполагается, что среда функционирования является на 100% правильным отражением целей безопасности для среды функционирования.

Это не мешает потребителю ОО использовать другие методы определения корректности конкретной среды функционирования, такие как:

- если для ОО типа "ОС" установлены цели безопасности для среды функционирования: "Среда функционирования должна обеспечить, что сущности из недоверенной сети (например, Интернета) могут осуществлять доступ к ОО только по ftp", то потребитель мог бы выбрать оцененный межсетевой экран и настроить его так, чтобы к ОО был разрешен доступ только по ftp;

- если для ОО установлены цели безопасности для среды функционирования: "Среда функционирования должна обеспечить, что никто из всего административного персонала не будет вести себя злонамеренно", то потребитель мог бы адаптировать свои контракты с административным персоналом для включения штрафных санкций за злонамеренное поведение, но это решение не является частью оценки в соответствии с ISO/IEC 15408.

### 6.3 Оценка

По стандарту ISO/IEC 15408 признают два типа оценки: оценка ЗБ/ОО, которая описывается ниже, и оценка ПЗ, которая определяется в ISO/IEC 15408-3. Много раз в ISO/IEC 15408 использован термин "оценка" (без уточнений) для ссылки на оценку ЗБ/ОО.

По ISO/IEC 15408 оценка ЗБ/ОО проходит в два этапа:

a) оценка ЗБ: на этом этапе определяют достаточность ОО и среды функционирования;

b) оценка ОО: на этом этапе определяют корректность ОО; как отмечалось ранее, оценка ОО не включает оценку корректности среды функционирования.

Оценку ЗБ выполняют путем применения критериев оценки заданий по безопасности (которые определены в разделе ASE ISO/IEC 15408-3). Конкретный способ применения критериев ASE определяется используемой методологией оценки.

Оценка ОО является более комплексной. Основные исходные данные для оценки ОО: свидетельства оценки, которые включают ОО и ЗБ, а также, как правило, исходные данные, получаемые из среды разработки, такие как проектная документация или результаты тестирования разработчиком.

Оценка ОО заключается в применении ТДБ (из задания по безопасности) к свидетельствам оценки. Конкретный способ применения конкретного ТДБ определяется используемой методологией оценки.

Как документировать результаты применения ТДБ, какие отчеты необходимо генерировать и в какой степени детализации - определяется в соответствии с используемой методологией оценки и в соответствии с требованиями системы оценки, в рамках которой выполняется оценка.

Результатом процесса оценки ОО будет:

- либо утверждение, что не все ТДБ удовлетворены, и поэтому не достигнут заданный уровень доверия к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ;
- либо утверждение, что все ТДБ удовлетворены, и поэтому достигнут заданный уровень доверия к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ.

Оценка ОО может быть выполнена после завершения разработки ОО или параллельно с разработкой ОО.

Способ изложения результатов оценки ЗБ/ОО описан в разделе 9. В этих результатах также идентифицируют ПЗ и пакет(ы), по отношению к которым заявлено соответствие ОО; эти конструкции описаны в следующем разделе.

## 7 Доработка требований безопасности для конкретного применения

### 7.1 Операции

Функциональные компоненты и компоненты доверия из ISO/IEC 15408 можно использовать точно так, как они сформулированы в ISO/IEC 15408-2 и ISO/IEC 15408-3, или же можно их конкретизировать, применяя разрешенные операции. При использовании операций разработчик ПЗ/ЗБ должен также отследить, чтобы зависимости других требований, которые зависят от данного требования, были удовлетворены. Разрешенные операции выбирают из следующей совокупности:

a) итерация (iteration): позволяет неоднократно использовать компонент при различном выполнении в нем операций;

b) назначение (assignment): позволяет определять параметры;

c) выбор (selection): позволяет выбирать один или более пунктов из перечня;

d) уточнение (refinement): позволяет осуществлять детализацию.

Операции "назначение" и "выбор" разрешены только в тех местах компонента, где они специально обозначены. Операции "назначение" и "выбор" разрешены для всех компонентов. Ниже операции описаны более детально.

Приложения ISO/IEC 15408-2 предоставляют руководство по допустимому выполнению операций выбора и назначения. Это руководство предоставляет нормативные инструкции по тому, как выполнять операции, и этим инструкциям необходимо следовать, если разработчик ПЗ/ЗБ логически не обоснует отклонение от этих инструкций:

a) "Нет" допускается как вариант выполнения выбора только если он явным образом предусмотрен.

Списки, предусмотренные для выполнения операций выбора, не должны быть пустыми. Если выбран вариант "Нет", не могут быть выбраны никакие другие дополнительные варианты. Если "Нет" не предусмотрено в качестве варианта выбора, допускается сочетание вариантов в операции выбора с союзами "и" и "или", если в операции выбора в явном виде не определено "выбрать одно из".

Операции выбора при необходимости можно сочетать с итерацией. В этом случае применение выбранного варианта для каждой итерации не должно пересекаться с предметом другой итерации выбора, так как они должны быть уникальными.

b) Операции выбора могут быть объединены путем итерации, где это необходимо. В этом случае применимость выбранного варианта для каждой итерации не должна пересекаться с предметом другого повторного отбора, поскольку они предназначены для исключения.

### 7.1.1 Операция "итерация"

Операция "итерация" может быть выполнена по отношению к любому компоненту. Разработчик ПЗ/ЗБ выполняет операцию "итерация" путем включения в ПЗ/ЗБ нескольких требований, основанных на одном и том же компоненте. Каждая итерация компонента должна отличаться от всех других итераций этого компонента, что реализуется завершением по-другому операций "назначение" и "выбор" или применением по-другому операции "уточнение".

Различные итерации следует уникально идентифицировать, чтобы обеспечить четкое обоснование и прослеживаемость от или к этим требованиям.

В ряде случаев операция "итерация" может быть выполнена по отношению к компоненту, для которого вместо его итерации можно было бы выполнить операцию "назначение", указав диапазон или список значений. В этом случае разработчик ПЗ/ЗБ может выбрать наиболее подходящую альтернативу, решив с учетом всех обстоятельств, есть ли потребность предоставления единого обоснования для всего диапазона значений или необходимо иметь отдельное обоснование для каждого из значений. Разработчику требуется определить необходимо ли отдельное прослеживание для этих значений.

### 7.1.2 Операция "назначение"

Операцию "назначение" осуществляют тогда, когда рассматриваемый компонент включает элемент с некоторым параметром, значение которого может быть установлено разработчиком ПЗ/ЗБ. Параметром может быть ничем не ограниченная переменная или правило, которое ограничивает переменную конкретным диапазоном значений.

Каждый раз, когда элемент в ПЗ предусматривает операцию "назначение", разработчик ПЗ должен выполнить одно из четырех действий:

a) оставить операцию "назначение" полностью невыполненной. Разработчик ПЗ, например, мог бы включить в ПЗ FIA_AFL.1.2 "При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить [назначение: *список действий*]";

b) полностью выполнить операцию "назначение". Например, разработчик ПЗ мог бы включить в ПЗ FIA_AFL.1.2 "При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны предотвращать в дальнейшем привязку соответствующей внешней сущности к какому-либо субъекту";

c) ограничить операцию "назначение", чтобы в дальнейшем ограничить диапазон допустимых значений. Например, разработчик ПЗ мог бы включить в ПЗ FIA_AFL.1.1 "ФБО должны обнаружить, когда произойдет [назначение: положительное целое число от 4 до 9] неуспешных попыток аутентификации **...**";

d) преобразовать "назначение" в "выбор", ограничивая "назначение". Например, разработчик ПЗ мог бы включить в ПЗ FIA_AFL.1.2 "При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны [выбор: предотвращать в дальнейшем привязку соответствующего пользователя к какому-либо субъекту, уведомлять администратора"].

Каждый раз, когда элемент в ЗБ предусматривает операцию "назначение", разработчик ЗБ должен завершить выполнение этой операции "назначение", как указано выше в варианте b). Варианты a), c) и d) для ЗБ не допускаются.

Значения, определенные в вариантах b), c) и d), должны соответствовать указанному типу значений, требуемому для данного "назначения".

Когда "назначение" должно быть завершено определением некоторой совокупности, например субъектов, в "назначении" можно перечислить совокупность

этих субъектов, но также можно привести некоторое описание этой совокупности, на основе которого могут быть определены элементы совокупности, такое как:

- все субъекты;
- все субъекты типа X;
- все субъекты, кроме субъекта A,

при условии, что понятно, какие субъекты имеются в виду.

### 7.1.3 Операция "выбор"

Операцию "выбор" осуществляют тогда, когда рассматриваемый компонент включает элемент, в котором разработчиком ПЗ/ЗБ должен быть сделан выбор из нескольких пунктов.

Каждый раз, когда элемент в ПЗ предусматривает операцию "выбор", разработчик ПЗ может выполнить одно из трех действий:

a) оставить операцию "выбор" полностью невыполненной;

b) полностью выполнить операцию "выбор" путем выбора одного или более пунктов;

c) ограничить операцию "выбор", удалив некоторые из вариантов, но оставив два или более.

Каждый раз, когда элемент в ЗБ предусматривает операцию "выбор", разработчик ЗБ должен завершить выполнение этой операции "выбор", как указано выше в варианте b). Варианты a) и c) для ЗБ не допускаются.

Пункт или пункты, выбранные при выполнении действий по вариантам b) и c), должны быть взяты из пунктов, предоставленных для выбора.

### 7.1.4 Операция "уточнение"

Операция "уточнение" может быть выполнена по отношению к любому требованию. Разработчик ПЗ/ЗБ выполняет уточнение путем изменения требования. Первое правило по отношению к уточнению состоит в том, чтобы ОО, удовлетворяющий уточненному требованию, также удовлетворял неуточненному требованию в контексте ПЗ/ЗБ (т.е. уточненное требование должно быть "более строгим", чем исходное требование). Если уточнение не удовлетворяет этому правилу, то результирующее уточненное требование считается расширенным требованием и будет рассматриваться как таковое.

Единственное исключение из этого правила состоит в том, что допускается, чтобы разработчик ПЗ/ЗБ уточнил ФТБ для его применения по отношению к некоторым, но не ко всем субъектам, объектам, операциям, атрибутам безопасности и/или внешним сущностям.

Однако это исключение не относится к уточнению ФТБ, которые взяты из ПЗ, о соответствии которым заявлено; эти ФТБ не могут быть уточнены чтобы относиться к меньшему количеству субъектов, объектов, операций, атрибутов безопасности и/или внешних сущностей, чем ФТБ в ПЗ.

Второе правило по отношению к уточнению состоит в том, что уточнение должно быть связано с исходным компонентом.

Особым случаем уточнения является редакционное уточнение, когда в требование вносят небольшие изменения, такие как перефразирование предложения, чтобы сделать его более понятным читателю. Не допускается, чтобы эти изменения каким-либо образом изменяли смысл требования.

## 8 Профили защиты и пакеты

### 8.1 Введение

Чтобы дать возможность заинтересованным группам или сообществам потребителей выражать свои потребности безопасности и облегчить разработку ЗБ, данная часть ISO/IEC 15408 предоставляет две специальные конструкции: пакеты и профили защиты (ПЗ). В 8.2 и 8.3 эти конструкции описаны более подробно. В 8.4 объясняется, как эти конструкции могут быть использованы.

### 8.2 Пакеты

Пакет - это именованный набор требований безопасности. Пакеты делятся на:

- функциональные пакеты, включающие только ФТБ;
- пакеты доверия, включающие только ТДБ.

Смешанные пакеты, включающие как ФТБ, так и ТДБ, не допустимы.

Пакет может быть определен какой-либо стороной и предназначен для многократного использования. Для этой цели он должен включать требования, которые в сочетании являются полезными и эффективными.

Пакеты могут использоваться при создании более крупных пакетов, ПЗ и ЗБ. В настоящее время не существует критериев оценки пакетов, поэтому любой набор ФТБ или ТДБ может быть пакетом.

Примерами пакетов доверия являются оценочные уровни доверия (ОУД), определенные в ISO/IEC 15408-3.

### 8.3 Профили защиты

В то время как ЗБ всегда описывает конкретный ОО (например, межсетевой экран X-2, версия 3.1), ПЗ предназначен для описания типа ОО (например, межсетевые экраны прикладного уровня). Поэтому один и тот же ПЗ можно использовать в качестве шаблона для множества различных ЗБ, которые будут использовать в различных оценках. Подробное описание ПЗ приведено в приложении В.

ЗБ описывает требования для ОО и его формирует разработчик ОО, в то время как ПЗ описывает общие требования для некоторого типа ОО и поэтому разрабатывается:

- сообществом пользователей, стремящихся прийти к консенсусу относительно требований для данного типа ОО;
- разработчиком ОО или группой разработчиков подобных ОО, желающих установить минимальный базис для конкретного типа ОО;
- правительственной организацией или крупной корпорацией, определяющими свои требования как часть процесса закупки.

ПЗ определяет допустимый тип соответствия ЗБ профилю защиты. То есть в ПЗ устанавливают (в разделе ПЗ "Утверждение о соответствии", см. В.5), какие типы соответствия являются допустимыми для ЗБ, а именно:

- если в ПЗ установлено, что требуется "строгое соответствие", то ЗБ должно в строгой форме соответствовать ПЗ;
- если в ПЗ установлено, что требуется "демонстрируемое соответствие", то ЗБ должно либо строго соответствовать ПЗ, либо его соответствие ПЗ может быть продемонстрировано.

Иными словами, для ЗБ допускается "демонстрируемое соответствие" ПЗ, только если ПЗ в явном виде это разрешает.

Если в ЗБ заявляют о соответствии нескольким ПЗ, то оно должно соответствовать (как описано выше) каждому из этих ПЗ в такой форме, как это предписано в этом ПЗ. Это подразумевает, что ЗБ может строго соответствовать одним ПЗ и демонстрируемо соответствовать другим ПЗ.

Задание по безопасности либо соответствует рассматриваемому ПЗ, либо не соответствует. ISO/IEC 15408 не признает "частичное" соответствие. Поэтому обязанность разработчика ПЗ - обеспечить, чтобы ПЗ не был чрезмерно перегруженным и не создавал бы, препятствий разработчикам ПЗ/ЗБ при заявлении о соответствии ПЗ.

ЗБ эквивалентно ПЗ либо является более ограничительным, если:

- ОО, который удовлетворяет ЗБ, также удовлетворяет ПЗ;

- все среды функционирования, которые удовлетворяют ПЗ, также удовлетворяют ЗБ.

Проще говоря, ЗБ должен наложить те же самые или большие ограничения на ОО и те же самые или меньшие ограничения на среду функционирования ОО:

a) Определение проблемы безопасности: обоснование соответствия в ЗБ должно продемонстрировать, что определение проблемы безопасности в ЗБ является эквивалентным (или более ограничительным) по отношению к определению проблемы безопасности в ПЗ. Это означает, что:

- ОО, который бы отвечал определению проблемы безопасности в ЗБ, также отвечал бы определению проблемы безопасности в ПЗ;

- все среды функционирования, которые отвечали бы определению проблемы безопасности в ПЗ, также отвечали бы определению проблемы безопасности в ЗБ.

b) Цели безопасности: обоснование соответствия в ЗБ должно продемонстрировать, что цели безопасности в ЗБ являются эквивалентными (или более ограничительными) по отношению к целям безопасности в ПЗ. Это означает что:

- ОО, который бы отвечал целям безопасности для ОО в ЗБ, также отвечал бы целям безопасности для ОО в ПЗ;

- все среды функционирования, которые отвечали бы целям безопасности для среды функционирования в ПЗ, также отвечали бы целям безопасности для среды функционирования в ЗБ.

Если определено строгое соответствие профилям защиты, то применяют следующие требования:

Если указано строгое соответствие профилям защиты, то применяются следующие требования:

a) Определение проблемы безопасности:

- ЗБ должно включать определение проблемы безопасности из ПЗ, может определять дополнительные угрозы и ПБОр, но не может определять дополнительные предположения

Он должен содержать все предположения, определенные в РР, с двумя возможными исключениями, как в следующих двух марках;

- допущение (или часть предположения), указанные в ПЗ, могут быть исключены из ПБ, если все цели безопасности для рабочей среды, определенные в ПЗ, адресующие это предположение (или эту часть предположения), заменены целями безопасности для ОО в ЗБ;

- новое допущение может быть добавлено в ЗБ к набору допущений, определенных в ПЗ, если это новое предположение не уменьшает угрозу (или часть угрозы), предназначенную для решения целей безопасности для ОО в ПЗ, и если Это предположение не соответствует ПОБ (или части ПОБ), предназначенному для решения задач безопасности для ОО в ПЗ;

b) цели безопасности: ЗБ:

- должно включать все цели безопасности для ОО из ПЗ, но может определять дополнительные цели безопасности для ОО;

- должен содержать все цели безопасности для операционной среды, как определено в ПЗ, за двумя исключениями, как в следующих двух пунктах;

- должен содержать все цели безопасности для ОО из ПЗ, но может указывать дополнительные цели безопасности для ОО;

- может указывать, что определенные цели для операционной среды в РР являются целями безопасности для ОО в ЗБ. Это называется переназначением цели безопасности. Если цель безопасности переустанавливается в TOE, обоснование целей безопасности должно четко указывать, какое допущение или часть предположения могут не понадобиться больше;

- может определить, что определенные цели для среды функционирования из ПЗ являются целями безопасности для ОО в ЗБ. Это называется переназначением цели безопасности. Если цель безопасности переназначена для ОО, то обоснование целей безопасности должно четко показать, какое предположение или часть предположения больше не требуются

c) Требования безопасности: ЗБ должно включать все ФТБ и ТДБ из ПЗ, но может определять дополнительные или иерархичные, более строгие ФТБ и ТДБ. Выполнение операций в ЗБ должно быть согласовано с выполнением операций в ПЗ; либо выполнение операций в ЗБ будет таким же, как и в ПЗ, либо приведет к более ограничивающим требованиям (при применении правил уточнения).

Если определено "демонстрируемое соответствие" профилям защиты, то применяют следующие требования:

- ЗБ должно включать обоснование того, почему ЗБ рассматривается как "эквивалентное или более ограничительное" по отношению к ПЗ;

- демонстрируемое соответствие позволяет разработчику ПЗ описать общую проблему безопасности, которая должна быть решена, и обеспечить общее руководство по требованиям, необходимым для ее решения, с пониманием того, что, вероятно, существует более чем один способ ее решения.

Оценка ПЗ является необязательной. Оценка выполняется с применением к нему критериев класса APE, перечисленных в ISO/IEC 15408-3. Цель такой оценки состоит в том, чтобы продемонстрировать, что ПЗ полный, непротиворечивый, технически правильный и, подходящий для использования в качестве шаблона для формирования других ПЗ или ЗБ.

Базирование ПЗ/ЗБ на оцененном ПЗ имеет два преимущества:

- существует намного меньше риска, что в ПЗ есть ошибки, неясности или пропуски. Если какие-либо проблемы с ПЗ (которые были бы выявлены при оценке этого ПЗ) обнаружат во время разработки или оценки нового ЗБ, то может пройти значительное время прежде, чем ПЗ будет исправлен;

- при оценке новых ПЗ/ЗБ часто могут быть повторно использованы результаты оценки оцененного ПЗ, что обеспечивает уменьшение усилий по оценке новых ПЗ/ЗБ

### 8.4 Использование ПЗ и пакетов

Если в ЗБ утверждается о соответствии одному или более пакету и/или профилю защиты, оценка данного ЗБ будет (среди других характеристик данного ЗБ) демонстрировать, что ЗБ действительно соответствует этим пакетам и/или ПЗ, по отношению к которым утверждается о соответствии. Подробности этого определения соответствия можно найти в приложении А.

Это делает возможным следующий процесс:

a) организация, заинтересованная в приобретении конкретного типа продукта безопасности ИТ, излагает свои потребности в безопасности в ПЗ, затем обеспечивает его оценку и выпуск;

b) разработчик получает этот ПЗ, разрабатывает ЗБ, которое содержит утверждение о соответствии данному ПЗ, и обеспечивает оценку этого ЗБ;

c) затем разработчик создает ОО (или использует существующий) и обеспечивает его оценку на соответствие ЗБ.

В результате разработчик может доказать, что его ОО удовлетворяет потребностям в безопасности организации: поэтому организация может закупить этот ОО. Аналогичный порядок может применяться в отношении пакетов

### 8.5 Многократное использование профилей защиты

ISO/IEC 15408 также допускает соответствие профилей защиты другим ПЗ, предусматривая создание цепочек профилей защиты, в которых каждый последующий ПЗ базируется на предыдущем (предыдущих) ПЗ.

Например, можно было бы взять ПЗ для интегральной схемы и ПЗ для ОС смарт-карты и использовать их для разработки ПЗ для смарт-карты (ИС и ОС), в котором утверждается о соответствии двум исходным ПЗ. Затем можно было бы разработать ПЗ для смарт-карт для общественного транспорта, базируясь на ПЗ для смарт-карт и ПЗ для загружаемого в них приложения. В конечном счете, разработчик мог бы затем разработать ЗБ, базируясь на этом ПЗ для смарт-карт для общественного транспорта.

## 9 Результаты оценки

### 9.1 Введение

В этом разделе представлены ожидаемые результаты оценки ПЗ и ЗБ/ОО, выполненной в соответствии с ISO/IEC 18045:

- оценки профилей защиты позволяют создавать каталоги (реестры) оцененных ПЗ;
- оценка ЗБ дает промежуточные результаты, которые затем используются при оценке ОО;

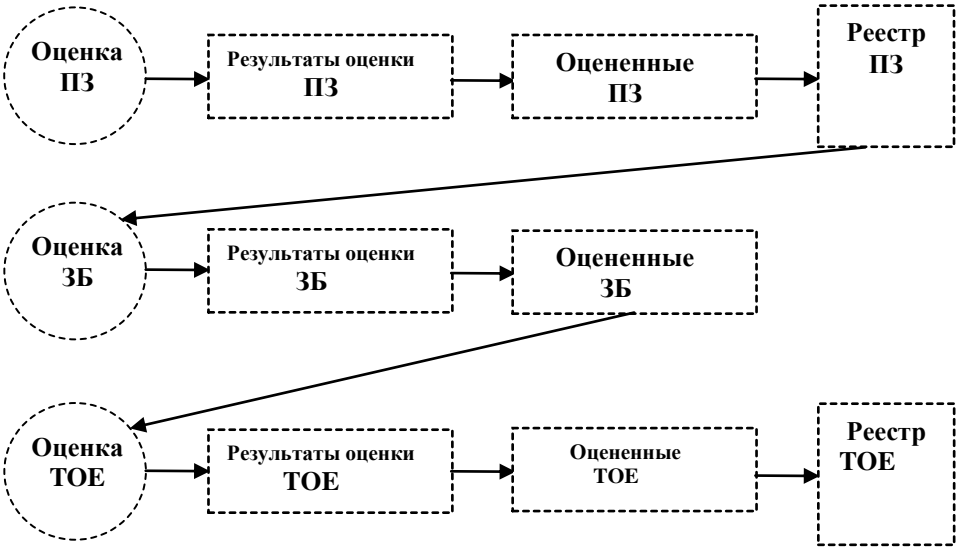



**Рисунок 4 – Результаты оценки**

- оценки ЗБ/ОО позволяют создавать каталоги (реестры) оцененных ОО. Во многих случаях эти каталоги будут ссылаться на продукты ИТ, на основе которых определены эти ОО, а не на конкретные ОО. Наличие продукта ИТ в каталоге не должно интерпретироваться как признак того, что весь продукт ИТ прошел оценку; реальный объем оценки ЗБ/ОО определяется ЗБ. На рисунке 5 продемонстрированы ожидаемые результаты оценки ПЗ и ЗБ/ОО.

ЗБ могут базироваться на пакетах, оцененных ПЗ, неоцененных ПЗ; тем не менее, совсем не обязательно, чтобы ЗБ на чем-то базировались.

Необходимо, чтобы оценка приводила к объективным и повторяемым результатам, на которые затем можно ссылаться как на свидетельство даже при отсутствии абсолютно объективной шкалы для представления результатов оценки безопасности ИТ. Наличие совокупности критериев оценки является необходимым предварительным условием для того, чтобы оценка приводила к значимому результату, предоставляя техническую основу для взаимного признания результатов оценки различными органами оценки.

Результат оценки представляет собой итоговые данные специфического типа исследования характеристик безопасности ОО. Такой результат не гарантирует пригодность к использованию в какой-либо конкретной среде применения. Решение о приемке ОО к использованию в конкретной среде применения основывается на учете многих аспектов безопасности, включая и выводы оценки

### 9.2 Результаты оценки ПЗ

ISO/IEC 15408-3 содержит критерии оценки, которые оценщику необходимы для того, чтобы установить, является ли ПЗ полным, непротиворечивым, технически правильным и, пригодным для использования при разработке ЗБ.

Результаты оценки должны также включать "Утверждение о соответствии" (см. 9.4).

### 9.3 Результаты оценки ЗБ/ТОЕ

ISO/IEC 15408-3 содержит критерии оценки, которые оценщику необходимы для того, чтобы установить, существует ли достаточное доверие к тому, что ОО удовлетворяет ФТБ из ЗБ.

Результат оценки ОО должен формулироваться как "соответствие/несоответствие" по отношению к ЗБ. Если и для ЗБ, и для ОО результат оценки - "соответствует", то соответствующий продукт получает право включения в реестр. Результаты оценки должны также включать "Утверждение о соответствии", как определено в 9.4.

Результаты оценки в дальнейшем будут использованы в процессе сертификации, но этот процесс находится вне области ISO/IEC 15408.

### 9.4 Утверждение о соответствии

Утверждение о соответствии указывает источник совокупности требований, которым удовлетворяет ПЗ или ЗБ, проходящие оценку. Это утверждение о соответствии содержит утверждение о соответствии ISO/IEC 15408, которое:

a) описывает ту версию ISO/IEC 15408, о соответствии которой заявлено в ПЗ или ЗБ;

b) описывает соответствие ISO/IEC 15408-2 (функциональные требования безопасности), включающее одно из следующего:

- "соответствие ISO/IEC 15408-2" - ПЗ или ЗБ соответствует ISO/IEC 15408-2, если все ФТБ в данном ПЗ или ЗБ основаны только на функциональных компонентах из ISO/IEC 15408-2;

- "расширение ISO/IEC 15408-2" - ПЗ или ЗБ является расширенным по отношению к ISO/IEC 15408-2, если одно ФТБ в данном ПЗ или ЗБ не основано на функциональных компонентах из ISO/IEC 15408-2;

c) описывает соответствие ISO/IEC 15408-3 (требования доверия к безопасности), включающее одно из следующего:

- "соответствие ISO/IEC 15408-3" - ПЗ или ЗБ соответствует ISO/IEC 15408-3, если все ТДБ в данном ПЗ или ЗБ основаны только на компонентах доверия из ISO/IEC 15408-3;

- "расширение ISO/IEC 15408-3" - ПЗ или ЗБ является расширенным по отношению к ISO/IEC 15408-3, если одно ТДБ в данном ПЗ или ЗБ не основано на компонентах доверия из ISO/IEC 15408-3.

Утверждение о соответствии может включать утверждение, сделанное относительно пакетов требований; в данном случае оно включает одно из следующего:

- "соответствие именованному пакету" - ПЗ или ЗБ соответствует предопределенному именованному пакету (например, ОУД), если:

ФТБ в ПЗ или ЗБ идентичны ФТБ в пакете или ТДБ в ПЗ или ЗБ идентичны ТДБ в пакете;

- "усиление именованного пакета" - ПЗ или ЗБ является усилением предопределенного именованного пакета, если:

- ФТБ в ПЗ или ЗБ включают все ФТБ из пакета, а также содержат одно дополнительное ФТБ или ФТБ, которое является иерархичным по отношению к некоторому ФТБ из пакета;

- ТДБ в ПЗ или ЗБ включают все ТДБ из пакета, а также содержат одно дополнительное ТДБ или ТДБ, которое является иерархичным по отношению к некоторому ТДБ из пакета.

При успешном прохождении ОО оценки на соответствие ЗБ, любые утверждения о соответствии задания по безопасности также относятся и к ОО. ОО также, например, может соответствовать ISO/IEC 15408-2.

Утверждение о соответствии может также включать два утверждения относительно профилей защиты:

a) "соответствие ПЗ" - ПЗ или ОО удовлетворяет конкретному(ым) профилю(ям) защиты, который(ые) перечислен(ы) как часть утверждения о соответствии;

b) "изложение соответствия" (только для профилей защиты) - В данном изложении описывается способ, которым должно быть обеспечено соответствие профилей защиты или заданий по безопасности рассматриваемому ПЗ: строгое или демонстрируемое. Более подробная информация по вопросу "изложения соответствия" приведена в приложении В

### 9.5 Использование результатов оценки ЗБ/ОО

После оценки ЗБ и ОО у владельцев активов имеется доверие (как определено в ЗБ) к тому, что ОО вместе со средой функционирования противостоят конкретным угрозам. Результаты оценки могут быть использованы владельцем активов при принятии решения о принятии риска, связанного с подверженностью активов воздействию конкретных угроз.

При этом владелец активов должен тщательно проверить следующее:

a) соответствует ли определение проблемы безопасности в ЗБ конкретной проблеме безопасности владельца активов;

b) соответствует ли среда функционирования у владельца активов (или может ли быть обеспечено ее соответствие) целям безопасности для среды функционирования, описанным в ЗБ.

Если что-либо из перечисленного не выполняется, то ОО может оказаться непригодным с точки зрения целей владельца активов.

После ввода оцененного ОО в эксплуатацию сохраняется возможность проявления в ОО ранее неизвестных ошибок или уязвимостей. В этом случае разработчик может внести изменения в ОО (чтобы устранить уязвимости) или изменить ЗБ, чтобы исключить уязвимости из области оценки. В любом случае прежние результаты оценки могут оказаться уже недействительными.

Если окажется необходимым восстановить уверенность, то потребуется переоценка. Для переоценки может быть использован ISO/IEC 15408, однако подробные процедуры переоценки находятся вне области данной части ISO/IEC 15408.

## Приложение А
*(информационное)*

## Спецификация заданий по безопасности

### А.1 Цель и структура данного приложения

Цель данного приложения состоит в изложении концепции задания по безопасности (ЗБ). В данном приложении не определены критерии класса ASE; соответствующее определение содержится в ISO/IEC 15408-3 и поддержано документами, приведенными в Библиографии.

Приложение А состоит из четырех основных частей:

a) Что должно содержать ЗБ. Краткая информация по этому вопросу изложена в А.2, более подробно в А.4-А.10. В указанных подразделах описано обязательное содержание ЗБ, взаимосвязи в рамках содержания ЗБ, а также представлены примеры.

b) Как следует использовать ЗБ. Краткая информация по этому вопросу изложена в А.3, более подробно - в А.11. В указанных разделах описано, каким образом следует использовать ЗБ, а также приведены вопросы, на которые могут быть даны ответы в ЗБ.

c) ЗБ для низкого уровня доверия (упрощенное ЗБ). ЗБ для низкого уровня доверия представляют собой ЗБ с сокращенным содержанием. Такие ЗБ описаны в А.12.

d) Утверждение о соответствии стандартам. В разделе А.13 описано, каким образом разработчик ЗБ может сделать утверждение, что ОО удовлетворяет некоторому конкретному стандарту.

### А.2 Обязательное содержание ЗБ

На рисунке А.1 представлено содержание ЗБ, установленное в ISO/IEC 15408-3. Рисунок А.1 также можно использовать как структурную схему ЗБ, однако допустимы и альтернативные структуры. Например, если обоснование требований безопасности является очень объемным, то оно может быть вынесено в приложение к ЗБ вместо включения в раздел "Требования безопасности". Разделы ЗБ и содержание этих разделов кратко рассмотрены ниже; в А.4-А.10 приведены более подробные пояснения. ЗБ содержит:

a) раздел "Введение ЗБ", содержащий описание ОО на трех различных уровнях абстракции;

b) раздел "Утверждения о соответствии", указывающий, утверждается ли в ЗБ о соответствии каким-либо ПЗ и/или пакетам, и если "да", то каким ПЗ и/или пакетам;

c) раздел "Определение проблемы безопасности", в котором указываются угрозы, ПБОр и предположения;

d) раздел "Цели безопасности", показывающий, каким образом решение проблемы безопасности распределено между целями безопасности для ОО и целями безопасности для среды функционирования ОО;

e) раздел "Определение расширенных компонентов" (опционально), в котором могут быть определены новые компоненты (т.е. компоненты, не содержащиеся в ISO/IEC 15408-2 или ISO/IEC 15408-3). Эти новые компоненты необходимы, чтобы определить расширенные функциональные требования и расширенные требования доверия;

f) раздел "Требования безопасности", в котором цели безопасности для ОО преобразованы в изложение на стандартизованном языке. Этот стандартизированный

язык представляет собой форму представления ФТБ. Кроме того, в рассматриваемом разделе определяют ТДБ;

g) раздел "Краткая спецификация ОО", показывающий, как ФТБ реализованы в ОО

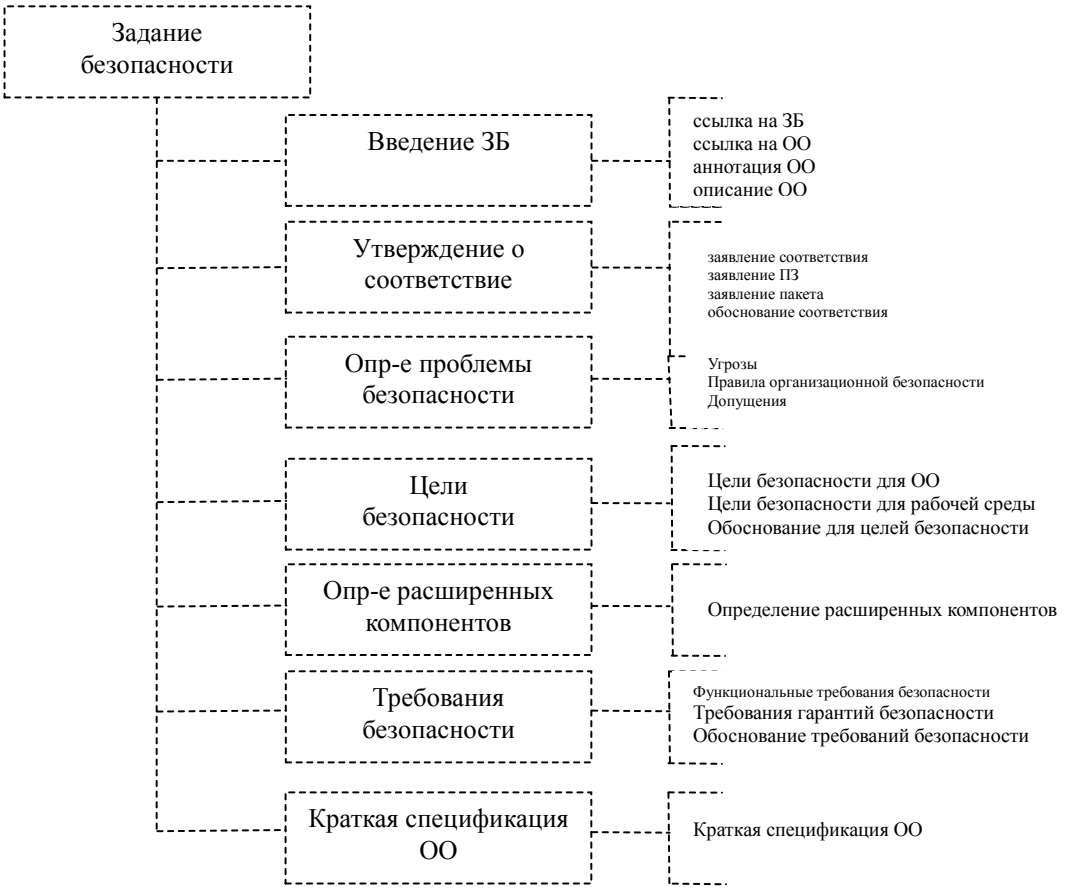



**Рисунок А.1 - Содержание задания по безопасности**

## А.3 Использование ЗБ

### А.3.1 Как должно использоваться ЗБ

Типовое ЗБ выполняет две роли:

Перед оценкой и в процессе оценки ЗБ определяет, "что должно быть оценено". В этой роли ЗБ служит основой для соглашения между разработчиком и оценщиком о точных характеристиках безопасности ОО и точной области оценки. Техническая правильность и полнота являются основными проблемными вопросами для этой роли. В разделе А.7 описано, каким образом следует использовать ЗБ в данной роли.

После оценки ЗБ определяет, "что было оценено". В этой роли ЗБ служит основанием для соглашения между разработчиком или поставщиком ОО и потенциальным потребителем ОО. ЗБ описывает точные характеристики безопасности ОО в краткой форме, и потенциальный потребитель может доверять этому описанию, так как ОО был оценен на предмет удовлетворения данному ЗБ. Удобство использования и понятность являются основными проблемными вопросами для этой роли. В разделе А.11 описано, каким образом следует использовать ЗБ в данной роли.

### А.3.2 Как не следует использовать ЗБ

Две роли (из многих), для которых не следует использовать ЗБ:

- детальная спецификация: ЗБ разрабатывается в качестве спецификации безопасности на относительно высоком уровне абстракции. В ЗБ не следует включать детальные спецификации протоколов, детальное описание алгоритмов и/или механизмов, длинное описание детализированных операций и т.д.;
- полная спецификация: ЗБ разрабатывается в качестве спецификации безопасности, а не общей спецификации. Кроме относящихся к безопасности, другие характеристики, такие как возможности взаимодействия, физические размеры и масса, требуемое напряжение и т.д., не следует включать в ЗБ. Это означает, что в целом ЗБ может быть частью полной спецификации, но не полной спецификацией само по себе.

## А.4 Введение ЗБ (ASE_INT)

В разделе "Введение ЗБ" описывают ОО в повествовательной форме на трех уровнях абстракции:

a) ссылка на ЗБ и ссылка на ОО, обеспечивающие идентификационные материалы для ЗБ и ОО, на который ссылается ЗБ;

b) аннотация ОО, в которой кратко описывается ОО;

c) описание ОО, в котором более подробно описывается ОО.

### А.4.1 Ссылка на ЗБ и ссылка на ОО

ЗБ содержит четкую ссылку на ЗБ, которая идентифицирует данное ЗБ. Типичная ссылка на ЗБ состоит из наименования ЗБ, версии, разработчика и даты выпуска. Пример ссылки на ЗБ - "MauveRAM Database ST, version 1.3, MauveCorp Specification Team, 11 October 2002".

ЗБ также содержит ссылку на ОО, идентифицирующую ОО, для которого требуется соответствие ЗБ. Типичная ссылка на ОО состоит из наименования разработчика, наименования ОО и номера версии ОО. Пример ссылки на ОО - "MauveCorp MauveRAM Database v2.11". Поскольку один и тот же ОО может быть оценен несколько раз, например, по инициативе различных потребителей этого ОО, для него может существовать несколько ЗБ, и поэтому ссылка на ОО не обязательно является уникальной.

Если ОО сформирован на основе одного или более известных продуктов, то допускается отразить это в ссылке на ОО путем указания наименований этих продуктов. Однако это не должно вводить потребителей в заблуждение: ситуации, когда основные части или функциональные возможности безопасности не были рассмотрены в процессе оценки, но в ссылке на ОО это не отражено, являются недопустимыми.

Ссылка на ЗБ и ссылка на ОО облегчают индексацию и ссылку на ЗБ и ОО и их включение в состав сводной информации списков оцененных ОО/продуктов.

### А.4.2 Аннотация ОО

Аннотация ОО нацелена на потенциальных потребителей ОО, просматривающих списки оцененных ОО/продуктов, чтобы найти ОО, которые могут удовлетворить их потребности в безопасности и поддерживаться их аппаратным, программным и программно-аппаратным обеспечением. Как правило, объем аннотации ОО - несколько параграфов.

В аннотации ОО кратко описывают использование ОО и его основные характеристики безопасности, идентифицируют тип ОО и все основные аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО, но требуемые для ОО.

### А.4.2.1 Использование и основные характеристики безопасности ОО

Описание использования и основных характеристик безопасности ОО предназначено, чтобы дать общее представление о возможностях ОО с точки зрения безопасности и о том, для чего можно использовать ОО в контексте безопасности. Это должно быть написано для (потенциальных) потребителей ОО с описанием использования и основных характеристик ОО в терминах бизнес-операций и на языке, понятном потребителям.

Пример такого описания: "The MauveCorp MauveRAM Database v2.11 является многопользовательской системой управления базами данных, предназначенной для использования в сетевой среде. Она предоставляет возможность одновременной работы до 1024 пользователей, возможность использовать аутентификацию, основанную на пароле/токене, а также - биометрическую аутентификацию; обеспечивает защиту от случайного повреждения данных и откат назад на десять тысяч транзакций. Существует возможность настройки механизмов аудита в широком диапазоне, позволяющая осуществлять детальный аудит по отношению к некоторым пользователям и транзакциям, обеспечивая при этом приватность для других пользователей и транзакций".

### А.4.2.2 Тип ОО

В аннотации ОО идентифицируют общий тип ОО, такой как: межсетевой экран, шлюз виртуальной частной сети, смарт-карта, интранет, веб-сервер, система управления базами данных, веб-сервер вместе с системой управления базами данных, ЛВС, ЛВС с веб-сервером и системой управления базой данных и др.

Возможна ситуация, когда ОО не может быть легко отнесен к имеющемуся типу, при которой приемлемым является указание на то, что ОО не отнесен ни к одному типу.

В некоторых случаях тип ОО может ввести в заблуждение потребителей. Например:

- от ОО с учетом его типа могут ожидать определенные функциональные возможности, в то время как у данного ОО эти функциональные возможности отсутствуют. Например:

ОО типа "АТМ-карта", который не поддерживает какие-либо функциональные возможности идентификации/аутентификации;

ОО типа "межсетевой экран", который не поддерживает протоколы, используемые почти повсеместно;

ОО типа "ИОК", у которого нет функциональных возможностей аннулирования сертификатов.

- от ОО с учетом его типа могут ожидать возможность функционирования в определенной среде, в то время как для данного ОО такая возможность отсутствует. Например:

ОО типа "операционная система ПК", который не может безопасно функционировать при наличии у ПК сетевого подключения, накопителя на гибких дисках, CD/DVD-дисковода;

межсетевой экран, который может безопасно функционировать только при условии, что все пользователи, которые могут подключаться через этот межсетевой экран, являются благонадежными.

#### А.4.2.3 Требуемые аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО

В то время как некоторые ОО не зависят от других ИТ, многие ОО (особенно программные ОО) зависят от дополнительных, не входящих в ОО, аппаратных средств/программного обеспечения и/или программно-аппаратных средств. В последнем случае в "Аннотации ОО" требуется идентифицировать соответствующие, не входящие в ОО, аппаратные средства/программное обеспечение и/или программно-аппаратные средства. Полная и абсолютно детальная идентификация дополнительных аппаратных средств/программного обеспечения и/или программно-аппаратных средств не требуется, но при этом необходима полнота и детализация идентификации, достаточная для определения потенциальными потребителями основных аппаратных средств, программного обеспечения и/или программно-аппаратных средств, необходимых для использования ОО.

Примеры идентификации аппаратных средств/программного обеспечения/программно-аппаратных средств:

- стандартный ПК с процессором 1 ГГц или более и ОП 512 Мб или более, функционирующий под управлением операционной системы Yaiza версии 3.0 с установленным обновлением 6d, с или 7 или версии 4.0;
- стандартный ПК с процессором 1 ГГц или более и ОП 512 Мб или более, функционирующий под управлением операционной системы Yaiza версии 3.0 с установленным обновлением 6d, с, установленной графической картой WonderMagic 1.0 с набором драйверов для WM версии 1.0;
- стандартный ПК с операционной системой Yaiza версии 3.0 (или выше);
- интегральная схема CleverCard SB2067;
- интегральная схема CleverCard SB2067 с установленной операционной системой для смарт-карт QuickOS;
- локальная вычислительная сеть департамента транспорта по состоянию на декабрь 2002 года.

### А.4.3 Описание ОО

"Описание ОО" представляет собой описание ОО в повествовательной форме, возможно в объеме нескольких страниц. Описание ОО должно обеспечить оценщикам и потенциальным потребителям общее понимание возможностей безопасности ОО с большей детализацией, чем в аннотации ОО. Описание ОО можно также использовать для описания более широкого прикладного контекста, для которого ОО будет подходящим.

В описании ОО рассматривают физические границы ОО: список всех аппаратных, программно-аппаратных, программных частей и руководства, которые составляют ОО. Этот список должен быть описан на уровне детализации, достаточном, чтобы обеспечить пользователю ЗБ общее понимание этих частей.

В описании ОО следует также рассмотреть логические границы ОО: логические характеристики безопасности, обеспечиваемые ОО, на уровне детализации, достаточном, чтобы обеспечить пользователю ЗБ общее понимание этих характеристик.

Предполагается, что данное описание будет более подробным, чем описание общих характеристик безопасности в аннотации ОО.

Важная роль физических и логических границ заключается в том, что они описывают ОО способом, не оставляющим неясностей в том, входит ли определенная часть или характеристика в ОО или не входит. Это особенно важно, когда ОО интегрирован с сущностями, не входящими в ОО, и не может быть легко выделен из них.

Примеры, когда ОО интегрирован с сущностями, не входящими в ОО:

- ОО является ИС смарт-карты, за исключением криптографического сопроцессора;
- ОО является частью межсетевого экрана MinuteGap версии 18.5, связанной с трансляцией сетевых адресов.

### А.5 Утверждения о соответствии (ASE_CCL)

В данном подразделе ЗБ описывается соответствие ЗБ:

- части 2 и части 3 настоящего стандарта;
- профилям защиты (если применимо);
- пакетам (если применимо).

Описание соответствия ЗБ ISO/IEC 15408 состоит из двух пунктов: ссылка на используемый ISO/IEC 15408 и указание на то, содержит ли ЗБ расширенные требования безопасности или не содержит (см. А.8).

Описание соответствия ЗБ профилям защиты предусматривает перечисление в ЗБ профилей защиты, по отношению к которым требуется соответствие. Пояснения см. в 9.4.

Описание соответствия ЗБ пакетам предусматривает перечисление в ЗБ пакетов, по отношению к которым требуется соответствие. Пояснения см. в 9.4.

### А.6 Определение проблемы безопасности (ASE_SPD)

#### А.6.1 Введение

В разделе ЗБ "Определение проблемы безопасности" определяется проблема безопасности, которая должна быть решена. Определение проблемы безопасности относительно ISO/IEC 15408 является аксиоматическим. Процесс установления определения проблемы безопасности находится вне области применения ISO/IEC 15408.

Однако полноценность результатов оценки в существенной степени зависит от ЗБ, а полноценность ЗБ в существенной степени зависит от качества определения проблемы безопасности. Поэтому зачастую необходимо потратить существенные ресурсы и использовать четкие процессы и процедуры анализа, чтобы получить надлежащее определение проблемы безопасности.

Согласно ISO/IEC 15408-3 не обязательно иметь изложение всех подразделов определения проблемы безопасности; ЗБ, в котором изложены угрозы, не обязательно должно содержать изложение ПБОр и наоборот. Кроме того, в ЗБ могут быть опущены предположения.

Когда ОО является физически распределенным, может оказаться предпочтительным рассмотреть соответствующие угрозы, ПБОр и предположения отдельно для различных областей (доменов) среды функционирования ОО.

### А.6.2 Угрозы

Данный подраздел раздела "Определение проблемы безопасности" представляет угрозы, которым должен противостоять ОО, его среда функционирования или их сочетание.

Угроза определяется негативным действием, выполняемым источником угрозы по отношению к некоторому активу.

Негативные действия - действия, выполняемые источником угрозы по отношению к некоторому активу. Эти действия влияют на одну или более характеристик актива, которые связаны со значимостью данного актива.

Источники угроз могут быть описаны как отдельные сущности, но в некоторых случаях может оказаться предпочтительным описать их как типы сущностей, группы сущностей и т.п.

Примеры источников угроз - хакеры, пользователи, компьютерные процессы и инциденты. Далее источники угроз могут быть описаны через такие аспекты, как компетентность, доступные ресурсы, возможности и мотивация.

Примеры угроз:

- хакер (со значительной компетентностью, стандартным оборудованием и профинансированный для реализации угрозы), осуществляющий удаленное копирование конфиденциальных файлов из сети компании;
- компьютерный "червь", существенно снижающий производительность глобальной сети;
- системный администратор, нарушающий приватность пользователя;

пользователь Интернета, прослушивающий трафик конфиденциального электронного обмена.

### А.6.3 Политика безопасности организации (ПБОр)

Данный подраздел раздела "Определение проблемы безопасности" представляет ПБОр, которые должны быть реализованы ОО, его средой функционирования или их сочетанием.

ПБОр - правила безопасности, процедуры или руководящие принципы, предписанные (или предполагаемые быть предписанными) в настоящее время и/или в будущем фактической или гипотетической организацией в среде функционирования. ПБОр может быть установлена организацией, управляющей средой функционирования ОО, или может быть установлена законодательными или регулирующими органами. ПБОр может относиться к ОО и/или к среде функционирования ОО.

Примеры ПБОр:

- все продукты, которые используются государственными организациями, должны соответствовать национальным стандартам по генерации пароля и криптографии;
- только пользователям с привилегиями системного администратора и допуском секретного отдела должно быть разрешено управление файл-сервером Департамента.

### А.6.4 Предположения

Данный подраздел раздела "Определение проблемы безопасности" представляет предположения, которые сделаны по отношению к среде функционирования ОО для обеспечения функциональных возможностей безопасности. Если ОО помещен в среду функционирования, которая не отвечает этим предположениям, то ОО, возможно,

окажется уже не в состоянии обеспечить все свои функциональные возможности безопасности. Предположения могут

быть по отношению к физическим аспектам, персоналу и внешней связности в среде функционирования.

Примеры предположений:

- предположения, связанные с физическими аспектами среды функционирования:

- предполагается, что ОО будет размещен в помещении, где выполнены работы по минимизации электромагнитных излучений;

- предполагается, что консоли администратора ОО будут помещены в зону ограниченного доступа.

- предположения, связанные с персоналом среды функционирования:

- предполагается, что пользователи ОО будут в достаточной степени обученными, чтобы эксплуатировать ОО;

- предполагается, что пользователи ОО допущены к информации ограниченного доступа;

- предполагается, что пользователи ОО не будут записывать свои пароли.

- предположения по отношению к аспектам связности среды функционирования:

- предполагается, что на автоматизированном рабочем месте на базе ПК для работы ОО доступно 10 Гб дискового пространства;

- предполагается, что ОО является единственным, кроме ОС, приложением, работающим на конкретной рабочей станции;

- предполагается, что ОО не будет связан с недоверенной сетью.

- процессе оценки эти предположения считаются верными: они в любом случае не проверяются.

По этим причинам предположения могут быть сделаны только по отношению к среде функционирования. Предположения никогда не могут делаться по отношению к режиму функционирования ОО, потому что оценка состоит из оценки утверждений, сделанных по отношению к ОО, а не из предположений, что утверждения по отношению к ОО являются верными.

### А.7 Цели безопасности (ASE_OBJ)

Цели безопасности - это краткое и абстрактное изложение предполагаемого решения проблемы, определенной в разделе ЗБ "Определение проблемы безопасности". У целей безопасности тройная роль:

- предоставить высокоуровневое на естественном языке описание решения проблемы;

- разделить данное решение на две части, отражающие, что различные сущности решают свою часть проблемы;

- продемонстрировать, что эти части решения формируют полное решение проблемы.

#### А.7.1 Высокоуровневое решение

Цели безопасности состоят из совокупности коротких и четких утверждений без чрезмерно больших подробностей, которые формируют высокоуровневое решение проблемы безопасности. Уровень абстракции целей безопасности должен быть таким, чтобы они были ясными и понятными для хорошо осведомленных потенциальных потребителей ОО. Цели безопасности излагаются на естественном языке.

### А.7.2 Части решения проблемы

В ЗБ высокоуровневое решение проблемы, которое описывается целями безопасности, делится на две части. Эти части описания решения названы целями безопасности для ОО и целями безопасности для среды функционирования. Это отражает, что данные части решения обеспечиваются двумя различными сущностями: ОО и средой функционирования.

#### А.7.2.1 Цели безопасности для ОО

ОО обеспечивает функциональные возможности безопасности для решения некоторой части проблемы, определенной в разделе ЗБ "Определение проблемы безопасности". Данная часть решения названа целями безопасности для ОО и включает совокупность целей, которые должны быть достигнуты ОО, чтобы решить свою часть проблемы.

Примеры целей безопасности для ОО:

- ОО должен обеспечивать конфиденциальность содержания всех файлов, передаваемых между ним и сервером;
- ОО должен выполнять идентификацию и аутентификацию всех пользователей до предоставления им доступа к сервису передачи информации, предоставляемого ОО;
- ОО должен ограничить доступ пользователей к данным согласно политике доступа к данным, описанной в приложении к ЗБ.

Если ОО является физически распределенным, может оказаться предпочтительным разделить подраздел ЗБ, содержащий цели безопасности для ОО, на несколько пунктов, чтобы учесть это.

#### А.7.2.2 Цели безопасности для среды функционирования

В среде функционирования ОО применяются технические и процедурные меры для поддержки ОО в отношении корректной реализации его функциональных возможностей безопасности (которые определены целями безопасности для ОО). Данная часть решения проблемы названа целями безопасности для среды функционирования и включает совокупность утверждений, описывающих цели, которые должны быть достигнуты средой функционирования.

Примеры целей безопасности для среды функционирования:

- в среде функционирования должно быть предоставлено автоматизированное рабочее место с установленной ОС Inux версии 3.01b для функционирования ОО на его базе;
- в среде функционирования должно быть обеспечено, чтобы все люди - пользователи ОО были соответствующим образом обучены до того, как им будет разрешено работать с ОО;
- среда функционирования ОО должна ограничить физический доступ к ОО, разрешая такой доступ только персоналу, выполняющему функции администраторов, и персоналу технической поддержки в сопровождении администраторов;
- среда функционирования должна обеспечить конфиденциальность журналов аудита, сгенерированных ОО, до их отправки на центральный сервер аудита.

Если среда функционирования ОО состоит из нескольких областей, каждая из которых обладает разными характеристиками, может оказаться предпочтительным разделить подраздел ЗБ, содержащий цели безопасности для среды функционирования, на несколько пунктов, чтобы учесть это.

### А.7.3 Взаимосвязь между целями безопасности и определением проблемы безопасности

ЗБ также содержит подраздел "Обоснование целей безопасности", включающий два пункта:

- прослеживание, показывающее, какие цели безопасности направлены на какие угрозы, ПБОр и предположения;
- совокупность логических обоснований, показывающих, что все угрозы, ПБОр и предположения надлежащим образом учтены в целях безопасности.

#### А.7.3.1 Прослеживание целей безопасности к определению проблемы безопасности

Прослеживание показывает, каким образом цели безопасности сопоставлены с угрозами, ПБОр и предположениям, приведенным в разделе "Определение проблемы безопасности", обеспечивая при этом следующее:

a) Отсутствие избыточных целей: каждая цель безопасности сопоставлена, с одной угрозой, ПБОр или предположением.

b) Полноту по отношению к определению проблемы безопасности: для каждой угрозы, ПБОр и предположения имеется, одна цель безопасности, сопоставленная с ними.

c) Корректность сопоставления: так как предположения всегда делаются по отношению к среде функционирования, то цели безопасности для ОО не сопоставляются с предположениями. Сопоставления, допустимые в соответствии с ISO/IEC 15408-3, представлены на рисунке А.2.

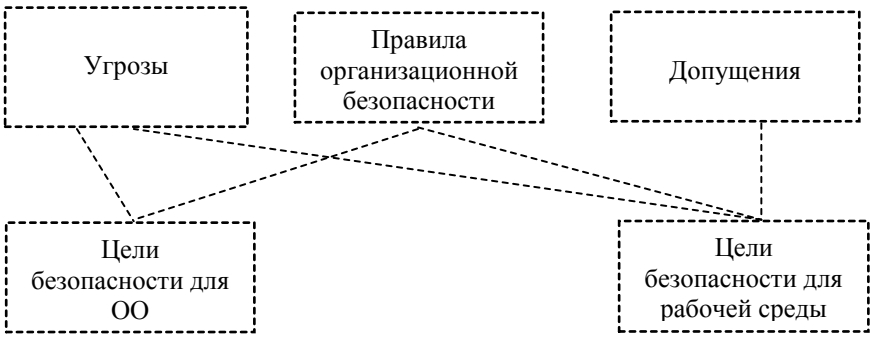



**Рисунок А.2 - Сопоставление целей безопасности и определения проблемы безопасности**

Несколько целей безопасности могут быть сопоставлены с одной и той же угрозой, указывая на то, что сочетание этих целей безопасности направлено на противостояние данной угрозе. Подобное утверждение справедливо для ПБОр и предположений.

#### А.7.3.2 Предоставление логического обоснования для сопоставления

Обоснование целей безопасности демонстрирует, что сопоставление является надлежащим: все определенные угрозы, ПБОр и предположения учтены (т.е., угрозам обеспечено противостояние, ПБОр осуществлена, предположения реализованы, если все

цели безопасности, сопоставленные с конкретной угрозой, ПБОр или предположением, достигнуты).

Данная демонстрация содержит результаты анализа эффекта от достижения соответствующих целей безопасности по противостоянию угрозам, осуществлению ПБОр и реализации предположений и приводит к заключению, что это действительно так.

В некоторых случаях, когда элементы "Определения проблемы безопасности" являются очень близкими к изложению некоторых целей безопасности, демонстрация может быть очень простой. Пример: угроза "Т17: Источник угрозы Х читает конфиденциальную информацию при ее передаче между А и В", цель безопасности для ОО: "О12: ОО должен обеспечить сохранение конфиденциальности всей информации, передаваемой между А и В" и демонстрация: "Угрозе Т17 напрямую противостоит цельО12".

### А.7.3.3 Предотвращаемые угрозы

Противостояние угрозе не обязательно означает устранение угрозы, а может означать достаточное уменьшение этой угрозы или достаточное смягчение последствий реализации этой угрозы.

Примеры устранения угрозы:

- устранение возможностей со стороны источника угрозы осуществлять нежелательное действие;
- перемещение, изменение или защита актива таким образом, что нежелательное действие становится более не применимым к нему;
- устранение источника угрозы (например, отключение от сети ПК, которые часто "рушат" эту сеть).

Примеры уменьшения угрозы:

- ограничение способности источника угрозы по выполнению нежелательных действий;
- ограничение возможности выполнить нежелательное действие источником угрозы;
- уменьшение вероятности успешного результата, выполненного нежелательного действия;
- снижение мотивации источника угрозы выполнить нежелательное действие путем сдерживания;
- требование от источника угрозы большей компетентности или больших ресурсов.

Примеры смягчения последствий реализации угрозы:

- частое создание резервных копий актива;
- приобретение дополнительных копий актива;
- страхование актива;
- обеспечение своевременного обнаружения успешных нежелательных действий, чтобы предпринять соответствующие ответные действия.

### А.7.4 Цели безопасности: заключение

Основываясь на целях безопасности и обосновании целей безопасности, может быть сделано следующее заключение: если все цели безопасности достигнуты, то проблема безопасности, определенная в соответствии с ASE_SPD, решена: всем угрозам обеспечено противостояние, все ПБОр осуществлены и все предположения реализованы.

### А.8 Определение расширенных компонентов (ASE_ECD)

Во многих случаях требования безопасности в ЗБ (см. А.9) основаны на компонентах из ISO/IEC 15408-2 или ISO/IEC 15408-3. Однако в некоторых случаях в ЗБ могут быть требования, которые не основаны на компонентах из ISO/IEC 15408-2 или ISO/IEC 15408-3. В этом случае новые компоненты (расширенные компоненты) должны быть определены, и такое определение следует сделать в разделе ЗБ "Определение расширенных компонентов". Дополнительная информация по данному вопросу приведена в С.4 (приложение С).

Данный раздел ЗБ предназначен для изложения только расширенных компонентов, а не расширенных требований (требований, основанных на расширенных компонентах). Расширенные требования следует включать в раздел ЗБ "Требования безопасности" (см. А.9), и их предназначение то же, что и у требований, основанных на компонентах из ISO/IEC 15408-2 или ISO/IEC 15408-3.

### А.9 Требования безопасности (ASE_REQ)

Требования безопасности включают две группы требований:

a) функциональные требования безопасности (ФТБ): перевод целей безопасности для ОО на некоторый стандартизированный язык;

b) требования доверия к безопасности (ТДБ): описание того, каким образом должно быть получено доверие к тому, что ОО удовлетворяет ФТБ.

Эти две группы требований безопасности рассматриваются в 9.1 и 9.2.

### А.9.1 Функциональные требования безопасности

ФТБ являются результатом преобразования целей безопасности для ОО. ФТБ представлены на более детальном уровне абстракции, но они должны быть полным представлением (цели безопасности должны быть полностью учтены) и быть независимыми от любого конкретного технического решения (реализации). ISO/IEC 15408 требует их представления на некотором стандартизированном языке по следующим причинам:

- чтобы обеспечить точное описание того, что подлежит оценке. Поскольку цели безопасности для ОО формулируются на естественном языке, перевод их на стандартизированный язык способствует более точному описанию функциональных возможностей ОО;

- чтобы обеспечить сопоставление двух ЗБ. В то время как различные разработчики ЗБ могут использовать различную терминологию при описании целей безопасности, стандартизированный язык обеспечивает использование единой терминологии и понятий при изложении требований безопасности. Это позволяет легко сравнивать ЗБ.

ISO/IEC 15408 не требует перевода на стандартизированный язык целей безопасности для среды функционирования, так как среда функционирования не оценивается и поэтому не требует описания, направленного на ее оценку См. пункты раздела "Библиография", относящиеся к оценке безопасности автоматизированных систем.

Могут быть ситуации, когда части среды функционирования оценены в процессе другой оценки, но это - вне области действия текущей оценки. Например, для ОО "ОС" может потребоваться, чтобы в его среде функционирования присутствовал межсетевой экран. Межсетевой экран может быть оценен в рамках другой оценки, но такая оценка не имеет никакого отношения к оценке ОО "ОС".

### А.9.1.1 Способы преобразования целей безопасности в требования безопасности, поддерживаемые ISO/IEC 15408

ISO/IEC 15408 поддерживает преобразование целей безопасности в требования безопасности тремя способами:

a) путем предоставления предопределенного "точного языка", разработанного в целях точного описания того, что подлежит оценке. Этот язык определяется как совокупность компонентов, определенных в ISO/IEC 15408-2. Использование этого языка для четкого преобразования целей безопасности для ОО в ФТБ является обязательным,однако существуют некоторые исключения (см. 7.3);

b) путем предоставления операций - механизм, который позволяет разработчику ЗБ модифицировать ФТБ, чтобы обеспечить более точный учет целей безопасности для ОО. В данной части ISO/IEC 15408 определены четыре допустимые операции: назначение, выбор, итерация и уточнение. Дальнейшее их рассмотрение представлено в С.2 (приложение С);

c) путем определения зависимостей - механизм, который поддерживает более полное преобразование целей безопасности для ОО в ФТБ. На языке ISO/IEC 15408-2 ФТБ может иметь зависимости от других ФТБ. Это указывает, что если в ЗБ используется данное ФТБ, то в общем случае в ЗБ должны также быть использованы и ФТБ, от которых оно зависит. Это уменьшает для разработчика ЗБ возможность упустить включение в ЗБ необходимых ФТБ и улучшает полноту ЗБ. Дальнейшее рассмотрение зависимостей представлено в 7.2.

### А.9.1.2 Взаимосвязь между ФТБ и целями безопасности

ЗБ также содержит "Обоснование требований безопасности", включающее два пункта, касающихся ФТБ:

- прослеживание, показывающее, какие ФТБ какие цели безопасности для ОО учитывают;
- совокупность логических обоснований, показывающих, что все цели безопасности для ОО надлежащим образом учтены в ФТБ.

А.9.1.2.1 Прослеживание ФТБ к целям безопасности для ОО

Прослеживание показывает, каким образом ФТБ сопоставлены с целями безопасности для ОО, обеспечивая при этом следующее:

a) Отсутствие избыточных ФТБ: каждое ФТБ сопоставлено, с одной целью безопасности.

b) Полнота по отношению к целям безопасности для ОО: для каждой цели безопасности для ОО имеется, одно ФТБ, сопоставленное с ней.

Несколько ФТБ могут быть сопоставлены с одной и той же целью безопасности для ОО, указывая на то, что сочетание этих требований безопасности удовлетворяет данную цель безопасности для ОО.

А.9.1.2.2 Предоставление логического обоснования для сопоставления

Обоснование требований безопасности демонстрирует, что сопоставление является надлежащим: если все ФТБ, сопоставленные с конкретной целью безопасности для ОО, удовлетворены, то эта цель безопасности для ОО достигнута.

Данная демонстрация должна содержать результаты анализа эффекта от удовлетворения соответствующего ФТБ при достижении конкретной цели безопасности для ОО и приводить к заключению, что это действительно так.

В случаях, когда ФТБ являются очень близкими к изложению целей безопасности для ОО, демонстрация может быть очень простой.

### А.9.2 Требования доверия к безопасности (ТДБ)

ТДБ - описание того, каким образом должен быть оценен ОО. В данном описании используется стандартизированный язык по следующим причинам:

- чтобы обеспечить точное описание того, каким образом ОО должен быть оценен. Использование стандартизированного языка способствует точному описанию и исключению неоднозначности;

- чтобы обеспечить сопоставление двух ЗБ. В то время как различные разработчики ЗБ могут использовать различную терминологию, стандартизированный язык обеспечивает использование единой терминологии и понятий. Это позволяет легко сравнивать ЗБ.

Рассматриваемый стандартизированный язык определяется как совокупность компонентов, определенных в ISO/IEC 15408-3. Использование этого языка является обязательным,однако существуют некоторые исключения. ISO/IEC 15408 (все части) усиливает этот язык по двум направлениям:

a) путем предоставления операций - механизм, который позволяет разработчику ЗБ модифицировать ТДБ. В данной части ISO/IEC 15408 определены четыре допустимые операции: назначение, выбор, итерация и уточнение. Дальнейшее их рассмотрение представлено в С.2 (приложение С);

b) путем определения зависимостей - механизм, который поддерживает более полное выражение ТДБ. На языке ISO/IEC 15408-3 ТДБ может иметь зависимости от других ТДБ. Это указывает, что если в ЗБ используется данное ТДБ, то в общем случае должны также использоваться и ТДБ, от которых оно зависит. Это уменьшает для разработчика ЗБ возможность упустить включение в ЗБ необходимых ТДБ и, улучшает полноту ЗБ. Более подробное рассмотрение зависимостей представлено в 7.2.

### А.9.3 ТДБ и обоснование требований безопасности

ЗБ также содержит обоснование требований безопасности, которое содержит аргументы, позволяющие считать конкретную совокупность ТДБ надлежащей. Каких-либо конкретных требований к такому обоснованию не предъявляется. Цель этого обоснования заключается в том, чтобы обеспечить пользователям ЗБ понимание причины выбора конкретной совокупности ТДБ.

Примером несогласованности является ситуация, когда в "Описании проблемы безопасности" присутствуют угрозы, источник которых (нарушитель) обладает достаточными возможностями, а в совокупность ТДБ включен младший компонент из семейства AVA_VAN или вообще не включен никакой компонент из данного семейства.

### А.9.4 Требования безопасности: заключение

В ЗБ в "Определении проблемы безопасности" определяется проблема безопасности, которая включает угрозы, ПБОр и предположения. В разделе ЗБ "Цели безопасности" решение проблемы безопасности подразделяется на две части:

- цели безопасности для ОО;

- цели безопасности для среды функционирования.

Кроме того, приводится обоснование целей безопасности, показывающее, что если все цели безопасности достигнуты, то проблема безопасности решена: всем угрозам обеспечено противостояние, все ПБОр осуществлены и все предположения реализованы.

В разделе ЗБ "Требования безопасности" цели безопасности для ОО преобразуются в ФТБ и предоставляется обоснование требований безопасности, показывающее, что если все ФТБ удовлетворены, то все цели безопасности для ОО достигнуты.

Кроме того, здесь приводится совокупность ТДБ, чтобы показать, каким образом оценивается ОО, а также - пояснение выбора этих ТДБ.

Все вышеупомянутое может быть объединено в рамках следующего утверждения. Если все ФТБ и ТДБ удовлетворены и все цели безопасности для среды функционирования достигнуты, то имеется доверие к тому что проблема безопасности, определенная в соответствии с ASE_SPD, решена: всем угрозам обеспечено противостояние, все ПБОр осуществлены и все предположения реализованы. Данное утверждение проиллюстрировано на рисунке А.3.

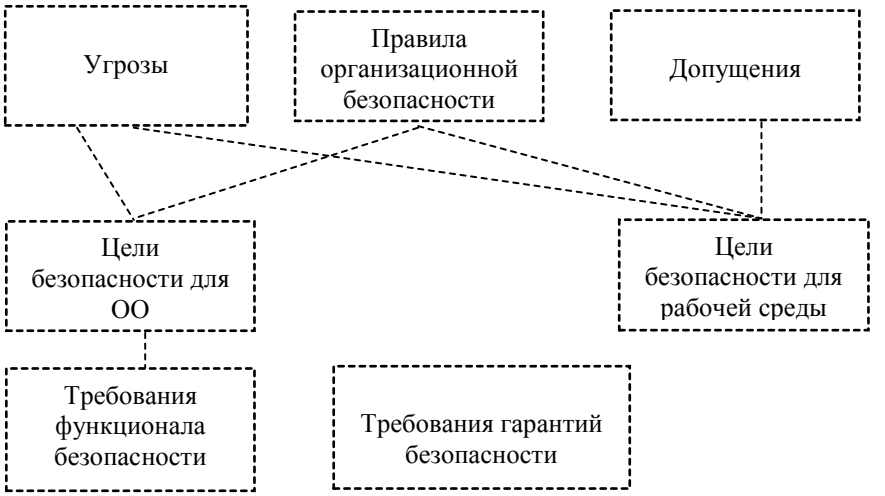



**Рисунок А.3 - Взаимосвязь между определением проблемы безопасности, целями безопасности и требованиями безопасности**

### А.10 Краткая спецификация ОО (ASE_TSS)

Цель "Краткой спецификации ОО" - предоставить потенциальным потребителям ОО описание того, каким образом ОО удовлетворяет все ФТБ. В разделе "Краткая спецификация ОО" следует привести описание основных технических механизмов, используемых ОО с этой целью. Уровень детализации данного описания должен быть достаточным, чтобы позволить потенциальным потребителям понять основной облик и реализацию ОО.

Например, если ОО является ПК, подключенным к Интернет, и ФТБ включают компонент FIA_UAU.1 для определения аутентификации, то в краткой спецификации ОО следует указать, каким образом выполняется аутентификация: посредством пароля, токена, сканирования радужной оболочки глаза и т.д.

Может быть также приведен больший объем информации, такой, например, как указание применимых стандартов, используемых в ОО для удовлетворения ФТБ, или более детальное описание.

### А.11 Вопросы, на которые можно ответить с помощью ЗБ

По окончании оценки ЗБ определяет "что было оценено". В этой роли ЗБ служит основой для соглашения между разработчиком или поставщиком ОО и потенциальным потребителем ОО. Поэтому с помощью ЗБ можно ответить на следующие (а также и на другие) вопросы:

a) Как найти необходимые ЗБ/ОО из множества существующих ЗБ/ОО? Этот вопрос обращен к "Аннотации ОО", в которой дается краткое (несколько параграфов) описание ОО;

b) Согласован ли ОО с существующей инфраструктурой ИТ? Этот вопрос обращен к "Аннотации ОО", в которой идентифицируются основные элементы аппаратных средств/программно-аппаратных средств/программного обеспечения, под управлением которых должен функционировать ОО;

c) Согласован ли ОО с существующей средой функционирования? Этот вопрос обращен к "Целям безопасности для среды функционирования", где определяются все ограничения на размещение ОО в среде функционирования;

d) Что делает (возможности) ОО (заинтересованный пользователь)? Этот вопрос обращен к "Аннотации ОО", в которой дается краткое (несколько параграфов) описание ОО;

e) Что делает ОО (потенциальный потребитель)? Этот вопрос обращен к "Описанию ОО", в котором дается более подробное, чем в "Аннотации ОО", описание ОО (на несколько страниц);

f) Что делает ОО (технический специалист)? Этот вопрос обращен к "Краткой спецификации ОО", в которой приводится высокоуровневое описание механизмов, использованных в ОО;

g) Что делает ОО (эксперт)? Этот вопрос обращен к ФТБ, которые обеспечивают достаточно абстрактное техническое описание, и к "Краткой спецификации ОО", в которой приводятся дополнительные подробности;

h) Решает ли ОО проблему с учетом требований государства/организации? Если государство/организация определили пакеты и/или ПЗ, чтобы определить решение, то ответ на указанный вопрос может быть найден в разделе ЗБ "Утверждения о соответствии", в котором перечисляются все пакеты и ПЗ, которым соответствует ЗБ;

i) Отвечает ли ОО конкретной проблеме безопасности (эксперт)? Каким угрозам противостоит ОО? Какую политику безопасности организации реализует ОО? Какие предположения сделаны относительно среды функционирования? На эти вопросы отвечает "Определение проблемы безопасности";

j) Каков объем доверия к ОО? Ответ на этот вопрос может быть найден в ТДБ в разделе ЗБ "Требования безопасности", в котором определен уровень доверия, использованный при оценке ОО, а - объем доверия к корректности ОО, обеспечиваемый в результате оценки.

### А.12 Задания по безопасности для низкого уровня доверия

Написание ЗБ является нетривиальной задачей и может, особенно при оценках для низких уровней доверия, составлять основную часть общих усилий, затрачиваемых разработчиком и оценщиком в течение всей оценки. Поэтому приемлемо также разрабатывать упрощенное ЗБ для низкого уровня доверия.

ISO/IEC 15408 допускает использование упрощенного ЗБ для оценки по ОУД1, но не по ОУД2 и выше. В ЗБ для низкого уровня доверия может быть заявлено

соответствие ПЗ для низкого уровня доверия (см. приложение В). В ЗБ (т.е. ЗБ с полным содержанием) может быть заявлено соответствие ПЗ для низкого уровня доверия.

ЗБ для низкого уровня доверия имеет значительно сокращенное содержание по сравнению с ЗБ:

- не требуется приводить определение проблемы безопасности;
- не требуется излагать цели безопасности для ОО. Но при этом цели безопасности для среды функционирования должны быть изложены;
- не требуется приводить обоснование целей безопасности, поскольку в ЗБ не приводится определение проблемы безопасности;
- в обосновании требований безопасности необходимо привести только обоснование неудовлетворения зависимостей, поскольку в ЗБ не приводятся цели безопасности для ОО.

Все, что остается в таком ЗБ, включает:

a) ссылки на ОО и ЗБ;

b) утверждение о соответствии;

c) различные описательные материалы:

1) аннотация ОО;

2) описание ОО;

3) краткая спецификация ОО;

d) цели безопасности для среды функционирования;

e) ФТБ и ТДБ (включая определение расширенных компонентов) и обоснование требований безопасности (только если конкретные зависимости не удовлетворены).

Сокращенное содержание ЗБ для низкого уровня доверия приведено на рисунке 4


**Рисунок А.4 – Содержание задания по безопасности для низкого уровня доверия**

### А.13 Ссылка в ЗБ на другие стандарты

В некоторых случаях разработчику ЗБ может потребоваться ссылка на какой-либо дополнительный стандарт, такой, например, как конкретный стандарт по криптографии или описание конкретного протокола. ISO/IEC 15408 позволяет сделать это тремя способами:

a) В качестве политики безопасности организации (или ее части).

Если, например, существует нормативный документ, определяющий, как выбираются пароли, это может быть изложено в ЗБ в качестве политики безопасности организации. На основе этого может быть изложена цель безопасности для среды функционирования (например, если пользователи ОО соответствующим образом должны выбирать пароли) или могут быть изложены цели безопасности для ОО, а затем - соответствующие ФТБ (вероятно, на основе класса FIA), если пароли генерирует ОО. В обоих случаях обоснование разработчика должно быть убедительным, что цели безопасности для ОО и ФТБ являются подходящими для реализации ПБОр. Оценщик должен определить, действительно ли это убедительно (и может изучить для этого упомянутый стандарт), действительно ли ПБОр реализована в ФТБ как приведено ниже.

b) В качестве стандарта (например, стандарта по криптографии), использованного при конкретизации ФТБ.

В этом случае соответствие конкретному стандарту является частью выполнения объектом оценки ФТБ и рассматривается, как будто полный текст стандарта является частью ФТБ. Далее соответствие конкретному стандарту определяется, как и любое другое соответствие ФТБ, при выполнении видов деятельности, предусмотренных классами ADV и ATE; соответствие определяется путем анализа проекта и тестирования на предмет того, что ФТБ полны и полностью реализованы ОО. Если необходима ссылка только на определенную часть стандарта, то эту часть следует однозначно указать при конкретизации ФТБ.

c) В качестве упоминания стандарта (например, стандарта по криптографии) в краткой спецификации ОО.

Краткая спецификация ОО рассматривается только в качестве пояснения того, как реализованы ФТБ, и не используется в качестве строгого требования к реализации, каковыми являются ФТБ или документы, поставляемые в соответствии с классом ADV. Оценщик может обнаружить несогласованность, если в краткой спецификации ОО есть ссылка на некоторый стандарт, но это не отражено в документации, предусмотренной классом ADV, и не предусмотрено соответствующей деятельностью, чтобы проверить выполнение стандарта.

## Приложение В
*(информационное)*

## Спецификация профилей защиты

### В.1 Цель и структура данного приложения

Цель данного приложения состоит в изложении концепции профиля защиты (ПЗ). В данном приложении не определены критерии класса APE; соответствующее определение содержится в ISO/IEC 15408-3 и поддержано документами, приведенными в Библиографии

Так как профили защиты и задания по безопасности имеют значительные совпадения, в данном приложении внимание сосредоточено на отличиях между ПЗ и ЗБ. Материал, который является идентичным для ЗБ и для ПЗ, изложен в приложении А.

Приложение В состоит из четырех основных частей:

a) Что должно содержать ПЗ. Краткая информация по этому вопросу изложена в В.2, более подробно в В.4-В.9. В указанных разделах описано обязательное содержание ПЗ, взаимосвязи в рамках содержания ПЗ, а также представлены примеры.

b) Как следует использовать ПЗ. Краткая информация по этому вопросу изложена в В.3.

c) ПЗ для низкого уровня доверия (упрощенный ПЗ). Упрощенные ПЗ представляют собой ПЗ с сокращенным содержанием. Такие ПЗ описаны в В.11.

d) Утверждение о соответствии стандартам. В разделе В.12 описано, каким образом разработчик ПЗ может сделать утверждение, что ОО должен удовлетворять некоторому конкретному стандарту

### В.2 Обязательное содержание ПЗ

На рисунке В.1 представлено содержание ПЗ, установленное в ISO/IEC 15408-3. Рисунок В.1 также можно использовать как структурную схему ПЗ,однако допустимы и альтернативные структуры. Например, если обоснование требований безопасности является очень объемным, то оно может быть вынесено в приложение к ПЗ вместо включения в раздел "Требования безопасности". Разделы ПЗ и содержание этих разделов кратко рассмотрены ниже; в В.4-В.9 приведены более подробные пояснения. ПЗ содержит:

a) раздел "Введение ПЗ", содержащий описание типа ОО;

b) раздел "Утверждения о соответствии", указывающий, утверждается ли в ПЗ о соответствии каким-либо ПЗ и/или пакетам, и если "да", то каким ПЗ и/или пакетам;

c) раздел "Определение проблемы безопасности", в котором указываются угрозы, ПБОр и предположения;

d) раздел "Цели безопасности", показывающий, каким образом решение проблемы безопасности распределено между целями безопасности для ОО и целями безопасности для среды функционирования ОО;

e) раздел "Определение расширенных компонентов" (опционально), в котором могут быть определены новые компоненты (т.е. компоненты, не содержащиеся в ISO/IEC 15408-2 или ISO/IEC 15408-3). Эти новые компоненты необходимы, чтобы определить расширенные функциональные требования и расширенные требования доверия;

f) раздел "Требования безопасности", в котором цели безопасности для ОО преобразованы в изложение на стандартизованном языке. Этот стандартизированный

язык представляет собой форму представления ФТБ. Кроме того, в рассматриваемом разделе определяют ТДБ.


**Рисунок В.1 – Содержание профиля защиты**

Существуют также ПЗ для низкого уровня доверия (упрощенные ПЗ), имеющие сокращенное содержание; подробно такие ПЗ описаны в В.11. За этим исключением все остальные части данного приложения предполагают ПЗ с полным содержанием.

### В.3 Использование ПЗ

#### В.3.1 Как следует использовать ПЗ

ПЗ представляет собой изложение потребностей в безопасности, в котором некоторое сообщество пользователей, регулирующий орган или группа разработчиков определяет общую совокупность потребностей в безопасности. ПЗ дает возможность потребителям ссылаться на эту совокупность и облегчает последующую оценку удовлетворения этих потребностей.

Поэтому ПЗ используют в качестве:

- части спецификации требований конкретного потребителя или группы потребителей, которые будут рассматривать приобретение продукта ИТ некоторого конкретного типа, только если он удовлетворяет ПЗ;
- части нормативного регулирования со стороны регулирующего органа, который разрешает использование продукта ИТ некоторого конкретного типа, только если он удовлетворяет ПЗ;

- базовой линии некоторой группы разработчиков, которые договариваются, что все продукты ИТ данного типа, которые они будут производить, будут удовлетворять данной базовой линии,

-однако это не исключает другого использования.

### В.3.2 Как не следует использовать ПЗ

Три роли (из многих), для которых не следует использовать ПЗ:

- детальная спецификация: ПЗ разрабатывается в качестве спецификации безопасности на относительно высоком уровне абстракции. В ПЗ не следует включать детальные спецификации протоколов, детальное описание алгоритмов и/или механизмов, длинное описание детализированных операций и т.д.;

- полная спецификация: ПЗ разрабатывается в качестве спецификации безопасности, а не общей спецификации. Кроме относящихся к безопасности, другие характеристики, такие как возможности взаимодействия, физические размеры и масса, требуемое напряжение и т.д., не следует включать в ПЗ. Это означает, что в целом ПЗ может быть частью полной спецификации, но не полной спецификацией сам по себе.

- спецификация некоторого отдельно взятого продукта. В отличие от ЗБ, ПЗ разрабатывается для описания определенного типа продуктов ИТ, а не отдельно взятого продукта ИТ. При описании некоторого отдельно взятого продукта ИТ лучше использовать для этой цели ЗБ.

## В.4 Введение ПЗ (APE_INT)

В разделе "Введение ПЗ" описывают ОО в повествовательной форме на двух уровнях абстракции:

a) ссылка на ПЗ, обеспечивающая идентификационные материалы для ПЗ;

b) аннотация ОО, в которой кратко описывается ОО.

### В.4.1 Ссылка на ПЗ

ПЗ содержит четкую ссылку на ПЗ, которая идентифицирует данный ПЗ. Типичная ссылка на ПЗ состоит из наименования ПЗ, версии, разработчика и даты выпуска. Ссылка должна быть уникальной, чтобы было возможно выделять различные ПЗ и различные версии одного и того же ПЗ.

Ссылка на ПЗ облегчает индексацию и ссылку на ПЗ и их включение в списки ПЗ.

### В.4.2 Аннотация ОО

Аннотация ОО нацелена на потенциальных потребителей ОО, просматривающих списки оцененных продуктов, чтобы найти ОО, которые могут удовлетворить их потребности в безопасности и поддерживаться их аппаратным, программным и программно-аппаратным обеспечением.

Аннотация ОО также предназначена для разработчиков, которые могут использовать ПЗ при разработке ОО или адаптации существующих продуктов.

Как правило, объем аннотации ОО - несколько параграфов.

В аннотации ОО кратко описывают использование ОО и его основные характеристики безопасности, идентифицируют тип ОО и все основные аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО, но доступные для ОО.

### B.4.2.1 Использование и основные характеристики безопасности ОО

Описание использования и основных характеристик безопасности ОО предназначено, чтобы дать общее представление о возможностях ОО и о том, для чего можно использовать ОО. Это должно быть написано для (потенциальных) потребителей ОО с описанием использования и основных характеристик ОО в терминах бизнес-операций и на языке, понятном потребителям ОО.

### B.4.2.2 Тип ОО

В аннотации ОО идентифицируют общий тип ОО, такой как: межсетевой экран, шлюз виртуальной частной сети, смарт-карта, интернет, веб-сервер, система управления базами данных, веб-сервер и система управления базами данных, ЛВС, ЛВС с веб-сервером и системой управления базой данных и др.

### B.4.2.3 Доступные аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО

В то время как некоторые ОО не зависят от других ИТ, многие ОО (особенно программные ОО) зависят от дополнительных, не входящих в ОО, аппаратных средств/программного обеспечения и/или программно-аппаратных средств. В последнем случае в "Аннотации ОО" требуется идентифицировать не входящие в ОО аппаратные средства/программное обеспечение и/или программно-аппаратные средства.

Поскольку профиль защиты не разрабатывают для конкретного продукта, во многих случаях в нем может быть дано только общее представление о доступных аппаратных средствах/программном обеспечении/программно-аппаратных средствах. В некоторых других случаях, например, при спецификации требований для конкретного потребителя, когда платформа уже известна, может быть предоставлена более конкретная информация.

Примеры идентификации аппаратных средств/программного обеспечения/программно-аппаратных средств:

- "отсутствует" (для полностью автономного ОО);
- операционная система Yaiza версии 3.0, функционирующая на ПК;
- интегральная схема CleverCard SB2067;
- интегральная схема CleverCard SB2067 с установленной операционной системой для смарт-карт QuickOS;
- локальная вычислительная сеть департамента транспорта по состоянию на декабрь 2002 года.

## B.5 Утверждения о соответствии (APE_CCL)

В данном разделе ПЗ описывают соответствие ПЗ другим ПЗ и пакетам. Это идентично разделу "Утверждения о соответствии" для ЗБ (см. A.5) за одним исключением: тип утверждения о соответствии.

В ПЗ в утверждении о соответствии излагается, каким образом ЗБ и/или другие ПЗ должны соответствовать данному ПЗ. Разработчик ПЗ выбирает, какой тип соответствия требуется: "строгое" соответствие или "демонстрируемое" соответствие. Более подробно этот вопрос рассмотрен в приложении D.

### B.6 Определение проблемы безопасности (APE_SPD)

Данный раздел идентичен разделу ЗБ "Определение проблемы безопасности", рассмотренному в А.6.

### B.7 Цели безопасности (APE_OBJ)

Данный раздел идентичен разделу ЗБ "Цели безопасности", рассмотренному в А.7.

### B.8 Определение расширенных компонентов (APE_ECD)

Данный раздел идентичен разделу ЗБ "Определение расширенных компонентов", рассмотренному в А.8.

### B.9 Требования безопасности (APE_REQ)

Данный раздел идентичен разделу ЗБ "Требования безопасности", рассмотренному в А.9.

Однако следует заметить, что правила выполнения операций в ПЗ немного отличаются от правил выполнения операций в ЗБ. Более подробно этот вопрос рассмотрен в 7.1.

### B.10 Краткая спецификация ОО

ПЗ не содержит краткой спецификации ОО.

### B.11 Профили защиты для низкого уровня доверия

ПЗ для низкого уровня доверия (упрощенное ПЗ) соотносится с о ПЗ (т.е. ПЗ с полным содержанием) так же, как и ЗБ для низкого уровня доверия (упрощенное ЗБ) соотносится с ЗБ. Это означает, что упрощенное ПЗ включает:

a) введение ПЗ, включающее ссылку на ПЗ и аннотацию ОО;
b) утверждения о соответствии;
c) цели безопасности для среды функционирования;
d) ФТБ и ТДБ (включая определение расширенных компонентов), а также обоснование требований безопасности (только в случае неудовлетворения зависимостей).

В упрощенном ПЗ может присутствовать утверждение о соответствии только некоторому упрощенному ПЗ (см. В.5). В ПЗ может также присутствовать утверждение о соответствии упрощенному ПЗ.

Сокращенное содержание упрощенного ПЗ приведено на рисунке В.2


**Рисунок В.2 – Содержание упрощенного ПЗ**

### В.12 Ссылка в ПЗ на другие стандарты

Этот раздел идентичен разделу А.13, посвященному ссылке на стандарты в ЗБ, за одним исключением: так как в ПЗ не содержится краткая спецификация ОО, то пункт с) раздела А.13 не применим по отношению к ПЗ.

Разработчику ПЗ необходимо учитывать, что ссылка в ФТБ на какой-либо стандарт может существенно добавить нагрузку на разработчика ОО, чтобы удовлетворить ПЗ (в зависимости от объема и сложности стандарта и требуемого уровня доверия); при этом может быть более приемлемым требовать использования альтернативных (не относящихся к частям стандарта ISO/IEC 15408) способов оценки соответствия стандарту, на который имеется ссылка в ПЗ.

## Приложение С
*(информационное)*

## Руководство по выполнению операций

### С.1 Введение

Профили защиты и задания по безопасности содержат предопределенные требования безопасности: разработчикам ПЗ и ЗБ при некоторых обстоятельствах также предоставляется возможность расширить список компонентов требований безопасности.

### С.2 Примеры операций

В 7.1 приведены четыре типа операций. Примеры выполнения различных операций рассмотрены ниже.

#### С.2.1 Операция "итерация"

Как описано в 7.1.1, операция "итерация" может быть выполнена по отношению к любому компоненту. Разработчик ПЗ/ЗБ выполняет операцию "итерация" путем включения нескольких требований, основанных на одном и том же компоненте. Каждая итерация компонента должна отличаться от всех других итераций этого компонента, что реализуется завершением по-другому операций "назначение" и "выбор" или применением по-другому операции "уточнение".

Различные итерации следует уникально идентифицировать, чтобы обеспечить четкое обоснование и прослеживаемость от или к этим требованиям.

Пример выполнения итерации - повторение дважды компонента FCS_COP.1 для того, чтобы потребовать реализации двух различных криптографических алгоритмов. Пример уникальной идентификации каждой итерации:

- Криптографическая операция (FCS_COP.1(1));
- Криптографическая операция (FCS_COP.1(2)).

#### С.2.2 Операция "назначение"

Как описано в 7.1.2, операцию "назначение" осуществляют тогда, когда рассматриваемый компонент включает элемент с некоторым параметром, значение которого может быть установлено разработчиком ПЗ/ЗБ. Параметром может быть ничем не ограниченная переменная или правило, которое ограничивает переменную конкретным диапазоном значений.

Пример элемента требований с операцией "назначение": FIA_AFL.1.2 "При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить [назначение: *список действий*]".

#### С.2.3 Операция "выбор"

Как описано в 7.1.3, операцию "выбор" осуществляют тогда, когда рассматриваемый компонент включает элемент, в котором разработчиком ПЗ/ЗБ должен быть сделан выбор из нескольких пунктов.

Пример элемента требований с операцией "выбор": FPT_TST.1.1 "ФБО должны выполнять пакет программ самотестирования [выбор: *при запуске, периодически в*

*процессе нормального функционирования, по запросу уполномоченного пользователя, при условиях* [назначение: *условия, при которых следует предусмотреть самотестирование*]] для демонстрации правильного выполнения ..."

### С.2.4 Операция "уточнение"

Как описано в 7.1.4, операция "уточнение" может быть выполнена по отношению к любому требованию. Разработчик ПЗ/ЗБ выполняет уточнение путем изменения требования.

Пример допустимого выполнения операции "уточнение": FIA_UAU.2.1 "ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя" уточнен следующим образом - "ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован на основе имени пользователя и пароля до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя".

Первое правило по отношению к уточнению состоит в том, чтобы ОО, удовлетворяющий уточненному требованию, также удовлетворял неуточненному требованию в контексте ПЗ/ЗБ (т.е. уточненное требование должно быть "более строгим", чем исходное требование).

Единственное исключение из этого правила состоит в том, что допускается, чтобы разработчик ПЗ/ЗБ уточнил ФТБ для его применения по отношению к некоторым, но не ко всем субъектам, объектам, операциям, атрибутам безопасности и/или внешним сущностям.

Пример подобного исключения: FIA_UAU.2.1 "ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя" уточнен следующим образом "ФБО должны требовать, чтобы каждый пользователь из Интернета был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя".

Второе правило по отношению к уточнению состоит в том, что уточнение должно быть связано с исходным компонентом. Например, уточнение компонента аудита путем добавления дополнительного элемента, связанного с предотвращением электромагнитного излучения, недопустимо.

Особым случаем уточнения является редакционное уточнение, когда в требование вносят небольшие изменения, такие как перефразирование предложения, чтобы сделать его более понятным читателю. Не допускается, чтобы эти изменения каким-либо образом изменяли смысл требования. Примеры редакционных уточнений:

ФТБ, основанное на компоненте FPT_FLS.1, "ФБО должны сохранить безопасное состояние при следующих типах сбоев: выход из строя одного процессора" могло бы быть уточнено следующим образом - FPT_FLS.1 "ФБО должны сохранить безопасное состояние при следующих типах сбоев: выход одного процессора из строя" или даже - FPT_FLS.1 "ФБО должны сохранить безопасное состояние при следующих типах сбоев: один процессор вышел из строя".

## С.3 Организация компонентов

Компоненты в ISO/IEC 15408-2 и ISO/IEC 15408-3 организованы в иерархические структуры: классы, состоящие из семейств, включающих компоненты, состоящие из элементов.

Данная организация иерархии "класс - семейство - компонент - элемент" помогает потребителям, разработчикам и оценщикам в поиске конкретных компонентов.

В ISO/IEC 15408 функциональные компоненты и компоненты доверия представлены в едином иерархическом стиле, по отношению к ним использована единая организация и терминология.

### С.3.1 Класс

Примером класса является класс FIA, который направлен на идентификацию пользователей, аутентификацию пользователей и связывание пользователей и субъектов.

### С.3.2 Семейство

Примером семейства является семейство "Аутентификация пользователя" (FIA_UAU), которое является частью класса FIA. Это семейство связано с аутентификацией пользователей.

### С.3.3 Компонент

Примером компонента является компонент FIA_UAU.3 "Аутентификация, защищенная от подделок", который связан с аутентификацией, защищенной от подделок.

### С.3.4 Элемент

Примером элемента является элемент FIA_UAU.3.2, который связан с предотвращением использования скопированных аутентификационных данных.

## С.4 Расширенные компоненты

### С.4.1 Определение расширенных компонентов

Всякий раз, когда разработчик ПЗ/ЗБ определяет расширенный компонент, это должно быть сделано способом, подобным существующим компонентам ISO/IEC 15408: четким, однозначным и оцениваемым (имеется возможность методично продемонстрировать выполнение требования, основанного на этом компоненте, для ОО). Расширенные компоненты должны использовать обозначение, способ выражения и уровень детализации, подобные существующим компонентам ISO/IEC 15408.

Разработчик ПЗ/ЗБ также должен убедиться, что все применимые зависимости расширенного компонента включены в определение этого расширенного компонента. Примерами возможных зависимостей являются следующие:

a) если расширенный компонент относится к аудиту то, вероятно, придется включить зависимости от компонентов класса FAU;

b) если расширенный компонент связан с модификацией или доступом к данным, то, вероятно, придется включить зависимости от компонентов семейства FDP_ACC;

c) если расширенный компонент использует конкретное описание проекта, то, вероятно, придется включить зависимость от компонентов соответствующего семейства (например, "Функциональная спецификация") класса ADV.

В случае расширенного функционального компонента разработчик ПЗ/ЗБ также должен включить в определение компонента применимую информацию, связанную с

аудитом и действиями по управлению, подобно тому, как это сделано для существующих компонентов ISO/IEC 15408-2. В случае расширенного компонента доверия разработчик ПЗ/ЗБ также должен предоставить соответствующую методологию оценки для данного компонента, подобную методологии, изложенной в ISO/IEC 18045.

Расширенные компоненты могут быть помещены в существующие семейства, в этом случае разработчик ПЗ/ЗБ должен показать, каким образом изменяются данные семейства. Если для новых компонентов не подходят существующие семейства, то они должны быть помещены в новое семейство. Новые семейства должны быть определены так же, как определены семейства в ISO/IEC 15408.

Новые семейства могут быть помещены в существующие классы, в этом случае разработчик ПЗ/ЗБ должен показать, каким образом изменяются данные классы. Если для новых семейств не подходят существующие классы, то они должны быть помещены в новый класс. Новые классы должны быть определены так же, как определены классы в ISO/IEC 15408.

## Приложение D
*(информационное)*

## Соответствие ПЗ

### D.1 Введение

ПЗ предназначен для использования в качестве "шаблона" для ЗБ. То есть ПЗ описывает совокупность потребностей пользователя, в то время как ЗБ, который соответствует этому ПЗ, описывает ОО, который удовлетворяет данные потребности.

Также возможно использовать один ПЗ в качестве "шаблона" для другого ПЗ. То есть ПЗ может требовать соответствие другому ПЗ. Этот случай полностью аналогичен утверждению о соответствии ПЗ в ЗБ. Для ясности в данном приложении описывается только случай ЗБ/ПЗ, но приложение применимо и для случая ПЗ/ПЗ.

ISO/IEC 15408 не допускает любой формы частичного соответствия, если в ПЗ или ЗБ заявлено о соответствии ПЗ, то данные ПЗ или ЗБ должны полностью соответствовать указанному (указанным) ПЗ, на которое (которые) имеется ссылка. Однако существуют два типа соответствия ("строгое" и "демонстрируемое"), при этом допустимый тип соответствия определяется в ПЗ. В ПЗ (в утверждении о соответствии ПЗ, см. В.5) устанавливаются допустимые типы соответствия для ЗБ. Данное отличие между строгим и демонстрируемым соответствием применимо на индивидуальной основе для каждого ПЗ, по отношению к которому в ЗБ утверждается о соответствии. Это может означать, что ЗБ "строго" соответствует одним ПЗ, а тип соответствия другим ПЗ - "демонстрируемое" соответствие. "Демонстрируемый" тип соответствия ПЗ допустим для ЗБ, только если в ПЗ это явно разрешено, в то же время ЗБ может "строго" соответствовать любому ПЗ.

Другими словами, для ЗБ является допустимым "демонстрируемое" соответствие ПЗ только, если ПЗ явно разрешает это.

Соответствие ПЗ означает, что ПЗ или ЗБ (а если для ЗБ имеется оцененный продукт, то и продукт также) отвечают всем требованиям данного ПЗ.

Выпущенные ПЗ будут требовать "демонстрируемого" соответствия. Это означает, что ЗБ, в котором утверждается о соответствии подобному ПЗ, должно предлагать решение общей проблемы безопасности, описанной в ПЗ, но может это сделать любым способом, который является эквивалентным или более ограничительным, по отношению к описанному в ПЗ. "Эквивалентный или более ограничительный" способ подробно определен в рамках ISO/IEC 15408, но в принципе это означает, что ПЗ и ЗБ могут содержать полностью различные утверждения, в которых рассматриваются различные сущности, используются различные понятия и т.д., при условии, что в целом ЗБ налагает идентичные ПЗ или большие ограничения по отношению к ОО, а также - идентичные ПЗ или меньшие ограничения по отношению к среде функционирования ОО.

### D.2 Строгое соответствие

Строгое соответствие ориентировано на разработчиков ПЗ, которым требуются свидетельства, что требования ПЗ удовлетворены, что ЗБ является примером реализации ПЗ,однако при этом ЗБ может быть более широким, чем ПЗ. По существу ЗБ определяет ОО, который выполняет, что определено в ПЗ, и среду функционирования, которая выполняет как максимум что определено в ПЗ.

Типичный пример использования строгого соответствия заключается в выборе для приобретения продукта, для которого ожидается точное соответствие требований безопасности требованиям, определенным в ПЗ.

ЗБ, подтверждающее строгое соответствие некоторому ПЗ, может вводить дополнительные ограничения по отношению к ПЗ.

### D.3 Демонстрируемое соответствие

Демонстрируемое соответствие ориентировано на разработчиков ПЗ, которым требуются свидетельства, что ЗБ является надлежащим для решения характерной проблемы безопасности, описанной в ПЗ.

Если в случае строго соответствия между ПЗ и ЗБ имеется четкое соотношение типа "подмножество - надмножество", то в случае демонстрируемого соответствия это соотношение менее четко определено. ЗБ, в которых утверждается о соответствии ПЗ, должны предлагать решение характерной проблемы безопасности, описанной в ПЗ.

Однако утверждение о соответствии допустимо только в случае, когда ЗБ налагает идентичные ПЗ или большие ограничения по отношению к ОО, а также - идентичные ПЗ или меньшие ограничения по отношению к среде функционирования ОО.

**Приложение В.А**
*(информационное)*

**Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств**

**Таблица В.А.1 - Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств**

| **Обозначение и наименование регионального стандарта** | **Степень соответствия** | **Обозначение и наименование национального стандарта, межгосударственного стандарта** |
|---|---|---|
| ISO/IEC 15408-2 Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в IT. Часть 2. Функциональные компоненты обеспечения безопасности) | IDT | СТ РК ГОСТ Р ISO/IEC 15408-2-2006 (ГОСТ Р ISO/IEC 15408-2-2002, IDT) Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности. Содержание |
| ISO/IEC 15408-3 Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в IT. Часть 3. Компоненты обеспечения гарантии безопасности | IDT | СТ РК ГОСТ Р ISO/IEC 15408-3-2006 (ГОСТ Р ISO/IEC 15408-3-2002,) Информационная технология. Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий Часть 3. Требования доверия к безопасности. |
| ISO/IEC 18045 Информационные технологии. Методы обеспечения безопасности. Методология оценки безопасности IT | IDT | СТ РК ISO/IEC 18045-2009 «Технологии информационные. Методы защиты. Методология оценки защиты информационных технологий» |

## Библиография

[1] ISO/IEC 15292, Information technology – Security techniques – Protection Profile regi3Бration procedures (Информационные технологии - Методы обеспечения безопасности - Процедуры регистрации профиля защиты)

[2] ISO/IEC 15443 (all parts), Information technology – Security techniques – A framework for IT security assurance (Информационные технологии – Методы обеспечения безопасности – Рабочая среда обеспечения IT-безопасности)

[3] ISO/IEC 15446, Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets (Информационные технологии – Методы обеспечения безопасности – Руководство по производству профилей защиты и заданий безопасности)

[4] ISO/IEC 19790, Information technology – Security techniques – Security requirements for cryptographic modules (Информационные технологии - Методы обеспечения безопасности – Требования безопасности для криптографических модулей)

[5] ISO/IEC 19791, Information technology – Security techniques – Security assessment of operational sy3Бems (Информационные технологии - Методы обеспечения безопасности – Оценка безопасности операционных систем)

[6] ISO/IEC 27001, Information technology – Security techniques – Information security management sy3Бems – Requirements (Информационные технологии - Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования)

[7] (ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management (Информационные технологии - Методы обеспечения безопасности – Свод практических правил управления информационной безопасностью)

[8] IEEE 3Бd 610.12-1990, In3Бitute of Electrical Engineers, 3Бandard Glossary of Software Engineering Terminology IEEE 3Бd 610.12-1990, (Институт инженеров электротехники и электроники, стандартный глоссарий терминологии в области технологий разработки программного обеспечения)

[9] Common Criteria portal, February 2009. CCRA, www.commoncriteriaportal.org (Портал общих критериев, февраль 2009. CCRA, www.commoncriteriaportal.org)

**УДК 681.324:006.354** **МКС 35.040**

**Ключевые слова:** информационная технология, критерии оценки безопасности, задание по безопасности, профиль защиты, объект оценки, функциональные возможности безопасности, доверие к безопасности

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, Мәңгілік Ел данғылы, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 27-08-01, 79-34-22