



ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технологиялар

ҚОРҒАУ ӘДІСТЕРІ

Ақпараттық технологияларды қорғауды бағалау әдіснамасы

ҚР СТ ИСО/МЭК 18045-2009

*ISO/IEC 18045:2008 (E) Information technology. Security techniques.
Methodology for IT security evaluation (IDT)*

II - том

Ресми басылым

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

Астана

Алғысөз

1 «Қазақстан стандарттау және сертификаттау институты» РМК және «Ұлттық ақпараттық технологиялар» АҚ Стандарттау жөніндегі «Ақпараттық технологиялар» 34 техникалық комитеті **ӘЗІРЛЕП ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті төрағасының 2009 жылғы 17 қарашадағы № 563-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт ISO/IEC 18045:2008 (e) Information technology. Security techniques. Methodology for IT security evaluation (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау әдіснамасы) атты халықаралық стандартпен бірдей

Халықаралық стандартты ИСО/МЭК ОТК 1 біріктірілген техникалық комитет, Ақпараттық технология, ПК 27 ішкі комитеті, АТ қауіпсіздігін қамтамасыз ету әдістері мен құралдары әзірледі

Ағылшын тілінен аудармасы (en)

Сәйкестік дәрежесі – бірдей (IDT)

4 Осы стандартта «Техникалық реттеу туралы» Қазақстан Республикасы Заңының, Саудадағы техникалық кедергілер (СТК) бойынша дүниежүзілік сауда ұйымының келісімінің нормалары мен ережелері жүзеге асырылды

**5 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ
ТЕКСЕРУ КЕЗЕҢДІЛІГІ**

**2014 жыл
5 жыл**

6 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Осы стандартқа енгізілетін өзгерістер туралы ақпарат «Стандарттау бойынша нормативтік құжаттар» сілтемесінде, ал өзгерістер мәтіні – ай сайынғы «Мемлекеттік стандарттар» ақпараттық сілтемесінде жарияланады. Осы стандартты қайта қараған немесе ауыстырған (жойған) жағдайда, тиісті ақпарат «Мемлекеттік стандарттар» ақпараттық сілтемесінде жарияланатын болады

Мазмұны

II - том

13	AVA қызметінің түрі. Осалдықты бағалау	273
14	АСО класы: Құрылым	308
	А қосымшасы (ақпараттық). Бағалау бойынша жалпы нұсқаулар	350
	Б қосымшасы (ақпараттық). Осалдықты бағалау (AVA)	362

Кіріспе

Осы мақсаттың мақсаттылы аудиториясы – бұл ИСО/МЭК 15408 көбінесе пайдаланатындар және бағалаушылардың әрекетін растайтын сертификаттау жөніндегі органдар сарапшылары; бағалау өткізуге өтініш берушілер, ҚП/БО авторлары, әзірлеушілері және екінші аудитория болып табылатын АТ қауіпсіздігіне мүдделі басқа тараптар.

Дербес жүйелермен өңделуі мүмкін әрекеттер әдіснамасымен байланысты тізімді А қосымшасынан табуға болады.

13 АВА қызметінің түрі. Осалдықты бағалау

13.1 Кіріспе

Осалдықты бағалау алдын ала белгіленген ортада БО кемшіліктерін немесе осал жерлерінің болатыны және пайдалануға жарамдылығы туралы қорытынды жасауға мүмкіндік береді. Бұл қорытынды бағалаушы орындаған бағалау куәліктерін және жалпы қолжетімді ақпарат көздерін талдауға негізделеді және бағалаушы орындайтын енуді тестілеумен сақталады.

13.2 Осалдықты талдау (AVA_VAN)

13.2.1 (AVA_VAN.1) қызметінің ішкі түрін бағалау

13.2.1.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты – БО өзінің алдын ала анықталған ортасында айқын осал, пайдалануға жарамды жерлердің болатыны туралы қорытынды жасау.

13.2.1.2 Бастапқы деректер

Қызметтің осы ішкі түрінің бағалау куәліктері болып табылады:

- а) ҚТ;
- б) нұсқау;
- в) тестілеу үшін жарамды БО;
- г) әлеуетті осалдықтарды табатын жалпы қолжетімді ақпарат.

Қызметтің осы ішкі түрінің қосымша бастапқы материалы айқын осалдықтарға қатысты ағымдағы ақпарат болып табылады (мысалы, сәйкестікті растау жөніндегі органнан болатын).

13.2.1.3 Қолдану бойынша ескертулер

Бағалаушы бағалау бойынша басқа әрекеттерді орындау уақытында табылған әлеуетті осалдықтың қосымша тестілерін орындауды ойластыруға тиіс.

Қызметтің осы ішкі түрінде нұсқау терминін пайдалану қолданыстағы нұсқауға және алдыңғы нұсқауға қатысты.

Осалдықтар жалпы қолжетімді ақпарат көздерінде идентификациялануы немесе идентификацияланбауы мүмкін және оларды пайдалану машығын талап етуі немесе етпеуі мүмкін. Осы екі аспекті байланысты, бірақ әр түрлі болып табылады. Осалдық жалпы қолжетімді көздерде идентификацияланғандықтан оңай пайдаланылуы мүмкін деп болжаған дұрыс емес.

13.2.1.4 AVA_VAN.1.1E операциясы

БО тестілеу үшін жарамды болуы қажет.

13.2.1.4.1 AVA_VAN.1-1 операциясы

Бағалаушы БО тестіленетін пішін үйлесімінің ҚТ анықталған бағалау пішін үйлесімімен келісілгені туралы қорытынды жасау үшін зерттеуге тиіс. Бағалаушының тестілеу үшін пайдаланатын БО УК (ALC_CMC) қызметінің

ішкі түрінің мүмкіндіктерімен белгіленетін дәл сондай бірегей таңбалауы болуы және ҚТ кіріспе бөлімінде идентификациялануы керек.

ҚТ бағалануға тиіс бірнеше пішін үйлесімі анықталуға тиіс. БО ҚТ сәйкестігіне тестіленуге тиіс әр түрлі бірқатар аппараттық және программалық жүзеге асырулардан тұруы мүмкін.

Бағалаушы барлық тестіленетін пішін үйлесімінің ҚТ келісілгенін верификациялайды.

Бағалаушы тестілеу ортасына қатысы болуы мүмкін БО қауіпсіздік ортасының аспектілеріне қатысты ҚТ сипатталған болжамдарды қарастыруы керек. ҚТ тестілеу ортасына қатысы болмайтын басқа да болжамдар болуы мүмкін. Мысалы, пайдаланушылардың рұқсатнамасына қатысты болжам тестілеу ортасына қатысты болмауы мүмкін, алайда, желіге қосылатын бірыңғай нүктеге қатысты болжам, әдетте, тестілеу ортасына қатысты болады.

Қандай да болмасын тестілеу құралдарын пайдаланған кезде (мысалы, өлшеуіштер, талдағыштар) осы құралдардың дұрыс калибрленуін қамтамасыз ету бағалаушының міндеті болады.

13.2.1.4.2 AVA_VAN.1-2 операциясы

Бағалаушы БО оның дұрыс орнатылғаны және белгілі күйінде болатыны туралы қорытынды жасау үшін зерттеуге тиіс.

Бағалаушының бірнеше тәсілдермен БО жай-күйі туралы қорытынды жасауға мүмкіндігі бар. Мысалы, осының алдындағы (AGD_PRE.1) қызметінің ішкі түрін сәтті аяқтау тестіленетін БО егер тиісті түрде орнатылғанына және белгілі жағдайда екендігіне бағалаушы әлі сенімді болмаса, осы операцияны орындалған деп санауға мүмкіндік береді. Егер бұл бұлай болмаса, онда бағалаушыға жеткізілген нұсқауды ғана пайдалана отырып, БО орнату, өндіру және іске қосу үшін әзірлеушінің процедураларын басшылыққа алу ұсынылады.

Егер бағалаушыға БО белгісіз жағдайда болғандықтан, орнату процедураларын орындауға тура келсе, онда осы операция сәтті аяқталған кезде AGD_PRE.1-3 операциясын қанағаттандырған болар еді.

13.2.1.5 AVA_VAN.1.2E әрекеті

13.2.1.5.1 AVA_VAN.1-3 операциясы

Бағалаушы БО әлеуетті осалдықтарды идентификациялау үшін жалпы қолжетімді ақпарат көздерін зерттеуге тиіс.

Бағалаушы БО әлеуетті осалдықтарды идентификациялау үшін жалпы қолжетімді ақпарат көздерін зерттеуге тиіс. Ерекше технологиялардағы белгілі осалдықтарды сипаттайтын поштамен жіберу тізімдері, бүкіләлемдік өрмектегі қауіпсіздік жөніндегі форумдар сияқты зерттелуге тиіс жалпы қолжетімді ақпарат көздері болады.

Бағалаушы өзінің жалпы қолжетімді ақпаратты зерттеулерін жоғарыда аталған көздермен шектемеуге тиіс, кез келген маңызды қолжетімді ақпаратты зерттеуі қажет.

Бағалаушы ұсынылатын куәліктерді талдаумен қатар, кезекті іздеу үшін жалпы қолжетімді ақпарат көздеріндегі ақпаратты пайдаланатын болады. Бағалаушы қызықты саланы анықтаған кезде, бағалаушы қызықты салаға қатысты жалпы қолжетімді ақпаратты зерттеуге тиіс.

Оңай қол жеткізетін ақпаратқа қол жеткізу бұзушыға идентификациялауға көмектеседі және шабуылға ықпал етеді, осы бұзушының шабуыл әлеуетін арттыра отырып елеулі әрекет етеді. Ғаламтордағы осалдықтар және жетік бұзу құралдары туралы ақпаратқа қол жеткізу осы ақпараттың БО әлеуетті осалдығын идентификациялау және оларды пайдалану әрекетінде пайдаланатындығы туралы ықтималдықты арттырады. Осындай ақпаратты уақытылы іздеу құралдары оны бағалаушы үшін оңай қол жететін етеді және жарияланған әлеуетті осалдықтарға және жақсы белгілі қарапайым шабуылдарға қарсы әрекетті анықтауға жоғары тиімді тәсілмен қол жеткізуге болады.

Жалпы қолжетімді ақпаратты іздеу типіне БО жататын өнімдермен айналысатын ресурстарда топталуға тиіс. Осындай іздеудің ұлғаюы мынадай факторлармен анықталуға тиіс: ОО типі, бағалаушының осындай типтегі БО жұмыс тәжірибесі, әлеуетті шабуылдар ықтималдығы және қолда бар куәліктер бойынша ADV деңгейі.

Бір әлеуетті осалдықты идентификациялау одан әрі зерттеуді қажет ететін басқа мүдделі саланы идентификациялауға әкелуі мүмкін қайталанатын идентификациялау процесі.

Бағалаушы жалпы қолжетімді ақпараттағы әлеуетті осалдықтарды идентификациялау үшін қандай әрекеттер жасалғанын көрсетуге тиіс. Алайда, бағалаушы мұндай іздеу әдісі кезінде әдіс іздеу уақытында алынған нәтижеде анықталуы мүмкін болғандықтан, зерттеуді бастар алдында әлеуетті осалдықтарды идентификациялау бойынша операцияны сипаттай алмайды.

Бағалаушы зерттелген куәліктерді әлеуетті осалдықтарды іздеуді аяқтаған кезде көрсетеді.

13.2.1.5.2 AVA_VAN.1-4 операциясы

Бағалаушы БТЕ тестілеуге кандидат болып табылатын және оның алдын ала анықталған ортасында БО қолданылатын идентификацияланған әлеуетті осалдықтарды көрсетуге тиіс.

Мүмкін, егер бағалаушы шаралардың не алдын ала анықталған ортада, не АТ, не АТ емес ортада алдын ала анықталған ортадағы осалдықтарды пайдалануды болдырмайтынын идентификацияласа, әлеуетті осалдықтарды одан әрі зерттеудің қажеті жоқтығы анықталатын болады.

Мысалы, тек уәкілетті пайдаланушыларға ғана БО жеке қол жеткізуін шектей отырып, пайдалану үшін жарамсыз қол сұғуға БО осалдығын нақты

жасауға болады. Егер бағалаушы әлеуетті осалдықтың алдын ала анықталған ортада жарамсыздығын анықтайтын болса, бағалаушы әлеуетті осалдықты зерттеуден бас тартуға арналған толық себепті көрсетеді.

Қалған жағдайларда, бағалаушы одан әрі зерттеулер үшін әлеуетті осалдықтарды көрсетеді.

БО оның алдын ала анықталған ортасында жарамды және енгізу тестілерін орындау үшін пайдаланылуы мүмкін әлеуетті осалдықтар тізімін бағалаушы БТЕ көрсетуге тиіс.

13.2.1.6 AVA_VAN.1.3E әрекеті

13.2.1.6.1 AVA_VAN.1-5 операциясы

Бағалаушы әлеуетті осалдықтарды тәуелсіз іздеуге негізделген енгізу тестілерін әзірлеуге тиіс.

Бағалаушы өту тестілеуіне жалпы қолжетімді ақпарат көздерінде іздеу барысында идентификацияланған әлеуетті осалдықтарға БО оның алдын ала анықталған ортасында қабылдағыштығын анықтау үшін жеткілікті түрде дайындалуға тиіс. Бағалаушыға белгілі әлеуетті осалдықтарға қатысты үшінші тараптан (мысалы, сертификаттау жөніндегі орган) ұсынылатын кез келген ағымдағы ақпаратты бағалаушы бағалау бойынша басқа әрекеттерді орындау барысында анықталатын кез келген әлеуетті осалдықпен қатар зерттеуі қажет.

Бағалаушының әрбір тестілер жиынтығы нақты осалдықты тестілеу үшін пайдаланылатын жерде бірқатар тестілер жиынтығын пайдалана отырып, өтуді тестілеуді орындау мақсатқа сәйкес деп санауы ықтимал.

Бағалаушының осалдық болатын затты шабуылды іске асыру үшін төмен әлеует талап етілетіндерден басқа, тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеулер нәтижесінде төменгіге қарағанда, жоғары шабуыл әлеуетімен ғана бұзушы пайдалануға жарамды болып табылатын кезде ол БТЕ қалдық осалдық сияқты беріледі.

13.2.1.6.2 AVA_VAN.1-6 операциясы

Бағалаушы нақтылауы тестілер өндірімділігін қамтамасыз ету үшін жеткілікті әлеуетті осалдықтар тізіміне негізделген өту тестілеріне арналған тестілеу құжаттамасын әзірлеуге тиіс.

Тестілеу құжаттамасында қамтылуы керек:

- а) тестіленетін БО осалдығын идентификациялау;
- б) енгізу тестісін өткізу үшін талап етілетін сияқты талап етілетін барлық тестілеу жабдықтарын қосу және орнату жөніндегі нұсқаулықтар;
- в) енгізу тестісін орындаудың барлық алғы шарттарын белгілеу жөніндегі нұсқаулықтар;
- г) ОФҚ инициирлеу жөніндегі нұсқаулықтар;
- д) ОФҚ орындау режимін қадағалау жөніндегі нұсқаулықтар;

е) күтілетін нәтижелермен салыстыру үшін ОФҚ қадағаланатын орындау режиміне қатысы бойынша орындалатын күтілетін барлық нәтижелерді және қажетті талдауды сипаттау;

ж) БО тестілеу жағдайынан кейінгі қажетті тестілеу және орнатуды аяқтау жөніндегі нұсқаулықтар.

Бағалаушы жалпы қолжетімді көздерде іздеу барысында идентификацияланған әлеуетті осалдықтар тізіміне негізделген енгізу тестілеуіне дайындалады.

Бағалаушының осалдық болатын затты шабуылды іске асыру үшін төмен әлеует талап етілетіндерден басқа, тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеулер нәтижесінде төменгіге қарағанда, жоғары шабуыл әлеуетімен ғана бұзушы пайдалануға жарамды болып табылатын кезде ол БТЕ қалдық осалдық сияқты беріледі.

Бағалаушы болжанатын осалдықты түсініп, БО қабылдағыштығын қолайлы тестілеу тәсілін анықтайды. Атап айтқанда, бағалаушы мынаны қарастырады:

а) ОФҚ орындау және олардың реакцияларын қадағалауды инициирлеу үшін пайдаланылатын ОФҚИ немесе басқа БО интерфейстері;

б) тестіні орындау үшін қажет болатын бастапқы шарттар (яғни, қажет болатын қандай да бір нақты объектілер немесе субъектілер және оларда болуы қажет қауіпсіздік атрибуттары);

в) ОФҚИ инициирлеу, не ОФҚИ қадағалау үшін қажет болатын тестілеуге арналған арнайы жабдық (дегенмен, арнайы жабдықтың айқын осалдықты пайдалану үшін қажет болуы екіталай).

г) жеке тестілеуді теориялық талдаумен ауыстыру, әсіресе, бастапқыда талдау нәтижелері қайталанатын шабуыл әрекеттерінің белгілі бір әрекеттер санынан кейін сәтті болу ықтималдығын көрсету үшін сыртқа таратылғаны маңызды.

Бағалаушының әрбір тесті жинағы нақты осалдықты тестілеу үшін пайдаланылатын жерде бірқатар тестілер жинағын пайдалана отырып, енуді тестілеуді орындау мақсатқа сәйкес деп санауы ықтимал.

Тестілеу құжаттамасында осы нақтылау деңгейін белгілеу мақсаты – басқа бағалаушыға тестіні қайталауға және балама нәтиже алуға мүмкіндік беру.

13.2.1.6.3 AVA_VAN.1-7 операциясы

Бағалаушы енуді тестілеуді жүргізуге тиіс.

Бағалаушы AVA_VAN.1-5 операциясында әзірленген ену тестілеріне арналған құжаттаманы ену тестілерін БО қатысы бойынша орындауға арналған негіз ретінде пайдаланады, бірақ бұл бағалаушыға қосымша арнайы ену тестілерін орындауға кедергі жасамайды. Егер қажет болса, бағалаушы

енуді тестілеу процесінде ақпаратты зерделеу нәтижесінде арнайы тестілер ойлап таба алады, егер бағалаушы орындаса, ену тестілеріне арналған құжаттамаға кіргізіледі. Мұндай тестілер күтпеген нәтижелер немесе қадағалауларды түсіну немесе бағалаушы алдын ала жоспарланған тестілеу уақытында болатынын аңғарған әлеуетті осалдықтарды зерттеу үшін қажет болуы мүмкін.

Шабуылды іске асыру үшін төменгі әлеует талап етілетіндерден басқа, бағалаушының осалдық болатын затты тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеу нәтижесінде төменгі шабуыл әлеуетіне қарағанда, бұзушының үлкен әлеуетті пайдалануы үшін ғана жарамды болып табылатын әлеуетті осалдықты байқаған кезде, ол БТЕ-де қалдық осалдық ретінде келтіріледі.

13.2.1.6.4 AVA_VAN.1-8 операциясы

Бағалаушы ену тестілерінің нақты нәтижелерін белгілеуге тиіс.

Дегенмен, тестілерді орындаудың нақты нәтижелерінің кейбір өзгеше бөлшектері күтілетіннен ерекшеленуі мүмкін (мысалы, аудит жазбасындағы уақыт өрісі және күні), жалпы нәтиже бірдей болуы қажет. Кез келген айырмашылықты қатаң түрде негіздеу керек.

13.2.1.6.5 AVA_VAN.1-9 операциясы

Бағалаушы БТЕ тестілеу тәсілін, тестіленетін пішін үйлесімін, тестілеу белгілемесі мен тестілеу нәтижелерін қысқаша баяндап, енуді тестілеу бойынша бағалаушының шарттары туралы ақпаратты келтіруге тиіс.

Бағалаушының БТЕ келтіретін тестілеу туралы ақпараты тестілеу бойынша қызмет түрін бағалау барысында жұмсалған күшті және тестілеуге арналған жалпы тәсілді беруге мүмкіндік жасайды. Осы ақпаратты ұсыну мәні тестілеу бойынша күшке қысқаша мазмұнды шолу жасау. БТЕ тестілеу туралы ақпараттың жеке тестілердің нақты тестілеу операциялары немесе нәтижелерінің дәл туындысы болуы міндетті емес. Әзірлеушінің БТЕ тестілеу туралы ақпаратының нақты тестілеу операциясының немесе жеке тестілер нәтижелерінің дәлме-дәл көшірмесі болуының мәні жоқ. Басқа бағалаушылар мен сертификаттау жөніндегі қызметкерлерге әзірлеушінің тестілеу тәсіліне қатысты орындалған тестілеу, БО тестіленетін пішін үйлесімдері көлемін және әзірлеушінің жалпы тестілеу нәтижелерін кейбір түсіну үшін мүмкіндік беретін жеткілікті нақтылаулар ұсыну мақсат болып табылады.

Әзірлеушінің енуді тестілеу жөніндегі ақпаратты, әдетте, БТЕ тиісті бөлімінен табуға болады, ол мынаны қамтиды:

а) БО тестіленетін пішін үйлесімдері. Енуді тестілеуге түсетін БО нақты пішін үйлесімдері;

б) Енуді тестілеуге түсетін ОФҚИ. Енуді тестілеу бағытталатын ОФҚИ және БО басқа интерфейстерінің қысқаша тізбесі;

в) Қызметтің осы ішкі түрі бойынша ұйғарым. Енуді тестілеу нәтижелері бойынша жалпы шешім.

Осы тізбе ешқандай жағдайда да БТЕ ұсынылуға тиіс бағалау барысында бағалаушы орындайтын енуді тестілеуге қатысты ақпарат типі туралы кейбір түсінік беру үшін ғана тағайындалған және жан-жақты болып табылмайды.

13.2.1.6.6 AVA_VAN.1-10 операциясы

Егер бағалаушыға БО белгісіз жағдайда болғандықтан, орнату процедураларын орындауға тура келсе, онда осы операция сәтті аяқталған кезде ADO_IGS.1-2 операциясын қанағаттандырған болар еді.

13.2.2.5 AVA_VAN.2.2Е әрекеті. AVA_VAN.2-3 операциясы

Бағалаушы БО әлеуетті осалдықтарды идентификациялау үшін жалпы қолжетімді ақпарат көздерін зерттеуге тиіс.

Бағалаушы барлық тестілеу нәтижелерін өзінің алдын ала анықталған ортасында болатын БО төменгі шабуыл әлеуетіне ие бұзушыға орнықты болып табылатынын анықтау үшін зерттеуге тиіс.

Егер нәтижелер өзінің алдын ала анықталған ортасында болатын БО орташа шабуыл әлеуетіне қарағанда аз әлеуетке ие бұзушының пайдалануы үшін жарамды осалдығы болатынын көрсетсе, онда осы әрекет бойынша бағалаушы теріс қорытынды жасайды.

Нақты осалдықты пайдалану үшін қажетті шабуыл әлеуетін және осының салдарынан берілген ортада оның пайдаланылуын анықтау үшін нұсқаудың В.4 тармағы пайдаланылуға тиіс. Орташаға қарағанда әлеуеті аз болатын бұзушының осалдықты пайдалана ма немесе жоқ па деген күдіктер болатын жағдайда қоспағанда, әр жолы шабуыл әлеуетін есептеп қажеті жоқ.

13.2.1.6.7 AVA_VAN.1-11 операциясы

Бағалаушы БТЕ әрбіреуі үшін нақтыланатын барлық пайдалануға жарамды осалдықтар мен қалдық осалдықтар туралы ақпаратты келтіруге тиіс:

а) оның көзі (мысалы, бағалау бойынша әрекеттерді орындаған кезде белгілі болған, бағалаушыға белгілі, жарияланымда оқылды);

б) ФҚТ жауап бермейтін;

в) сипаттау;

г) алдын ала анықталған ортада ол пайдаланыла ма, жоқ па (яғни, не пайдалану үшін жарамды немесе қалдық осалдық болып табылады);

д) В.4 қосымшасының В.2 және В.3 кестесін пайдалана отырып, осалдықты және тиісті мәндерді идентификациялауды орындау үшін қажетті уақыт көлемі, талдау деңгейі, БО білу деңгейі, мүмкіндіктер деңгейі және жабдық.

13.2.2 (AVA_VAN.2) қызметінің ішкі түрін бағалау

13.2.2.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты БО-ның өзінің алдын ала анықталған ортасында төменгі шабуыл әлеуеті болатын бұзушыға осалдықтың жарамды екенін анықтау.

13.2.2.2 Бастапқы деректер

Қызметтің осы ішкі түрінің бағалау куәліктері болып табылады:

- а) ҚТ;
- б) функционалдық сипаттізім;
- в) БО жобасы;
- г) қауіпсіздік құрылымын сипаттау;
- д) нұсқау;
- е) тестілеу үшін жарамды БО.

Қызметтің осы ішкі түрі үшін қалған болжанатын бағалау куәліктері сенім пакетінде қамтылатын құрауыштарға тәуелді болады. Әрбір құрауышты қамтамасыз ететін куәліктер қызметтің осы ішкі түрінде бастапқы ретінде пайдаланылады.

Қызметтің осы ішкі түрі үшін айқын осалдықтарға қатысты ағымдағы ақпарат қосымша бастапқы материал болып табылады (мысалы, сәйкестікті растау жөніндегі органнан болатын).

13.2.2.3 Қолдану бойынша ескертулер

Бағалаушы бағалау бойынша басқа әрекеттерді орындау уақытында байқалатын әлеуетті осалдықтардың қосымша тестілерін орындауды ойластыруға тиіс.

13.2.2.4 AVA_VAN.2.1E әрекеті

БО тестілеу үшін жарамды болуға тиіс.

13.2.2.4.1 AVA_VAN.2-1 операциясы

Бағалаушы БО тестіленетін пішін үйлесімінің ҚТ анықталған бағалау пішін үйлесімімен келісілгені туралы қорытынды жасау үшін зерттеуге тиіс.

Бағалаушының тестілеу үшін пайдаланатын БО УК (ALC_CMC) қызметінің ішкі түрінің мүмкіндіктерімен белгіленетін дәл сондай бірегей таңбалауы болуы және ҚТ кіріспе бөлімінде идентификациялануы керек.

ҚТ бағалануға тиіс бірнеше пішін үйлесімі анықталуға тиіс. БО ҚТ сәйкестігіне тестіленуге тиіс әр түрлі бірқатар аппараттық және программалық жүзеге асырулардан тұруы мүмкін.

Бағалаушы барлық тестіленетін пішін үйлесімінің ҚТ келісілгенін верификациялайды.

Бағалаушы тестілеу ортасына қатысы болуы мүмкін БО қауіпсіздік ортасының аспектілеріне қатысты ҚТ сипатталған болжамдарды қарастыруы керек. ҚТ тестілеу ортасына қатысы болмайтын басқа да болжамдар болуы мүмкін. Мысалы, пайдаланушылардың рұқсатнамасына қатысты болжам тестілеу ортасына қатысты болмауы мүмкін, алайда, желіге қосылатын

бірыңғай нүктеге қатысты болжам, әдетте, тестілеу ортасына қатысты болады.

Қандай да болмасын тестілеу құралдарын пайдаланған кезде (мысалы, өлшеуіштер, талдағыштар) осы құралдардың дұрыс калибрленуін қамтамасыз ету бағалаушының міндеті болады.

13.2.2.4.2 AVA_VAN.2-2 операциясы

Бағалаушы БО оның дұрыс орнатылғаны және белгілі күйінде болатыны туралы қорытынды жасау үшін зерттеуге тиіс.

Бағалаушының бірнеше тәсілдермен БО жай-күйі туралы қорытынды жасауға мүмкіндігі бар.

Мысалы, осының алдындағы (AGD_PRE.1) қызметінің ішкі түрін сәтті аяқтау тестіленетін БО егер тиісті түрде орнатылғанына және белгілі жағдайда екендігіне бағалаушы әлі сенімді болмаса, осы операцияны орындалған деп санауға мүмкіндік береді. Егер бұл бұлай болмаса, онда бағалаушыға жеткізілген нұсқауды ғана пайдалана отырып, БО орнату, өндіру және іске қосу үшін әзірлеушінің процедураларын басшылыққа алу ұсынылады.

Бағалаушы жалпы қолжетімді ақпарат көзін БО ықтимал әлеуетті осалдықтарды идентификациялауды қамтамасыз ету үшін зерттеуге тиіс. Мыналар сияқты зерттелуге тиіс жалпы қолжетімді ақпарат көздері көп болады:

- а) мамандандырылған басылымдар (журналдар, кітаптар);
- б) ғылыми мақалалар.

Бағалаушы жоғарыда жазылған жалпы қолжетімді ақпарат көздері көрсеткен өз зерттеулерін шектемеуге тиіс, қайта басқа кез келген маңызды қолжетімді ақпаратты зерттеуі керек.

Бағалаушы ұсынылатын куәліктерді талдаумен қатар, кезекті іздеу үшін жалпы қолжетімді ақпарат көздеріндегі ақпаратты пайдаланатын болады. Бағалаушы қызықты саланы анықтаған кезде, бағалаушы қызықты салаға қатысты жалпы қолжетімді ақпаратты зерттеуге тиіс. Оңай қол жеткізетін ақпаратқа қол жеткізу бұзушыға идентификациялауға көмектеседі және шабуылға ықпал етеді, осы бұзушының шабуыл әлеуетін арттыра отырып елеулі әрекет етеді. Ғаламтордағы осалдықтар және жетік бұзу құралдары туралы ақпаратқа қол жеткізу осы ақпараттың БО әлеуетті осалдығын идентификациялау және оларды пайдалану әрекетінде пайдаланатындығы туралы ықтималдықты арттырады. Осындай ақпаратты уақытылы іздеу құралдары оны бағалаушы үшін оңай қол жететін етеді және жарияланған әлеуетті осалдықтарға және жақсы белгілі қарапайым шабуылдарға қарсы әрекетті анықтауға жоғары тиімді тәсілмен қол жеткізуге болады.

Жалпы қолжетімді ақпаратты іздеу типіне БО жататын өнімдермен айналысатын ресурстарда топталуға тиіс. Осындай іздеудің ұлғаюы мынадай факторлармен анықталуға тиіс: ОО типі, бағалаушының осындай типтегі БО

жұмыс тәжірибесі, әлеуетті шабуылдар ықтималдығы және қолда бар куәліктер бойынша ADV деңгейі.

Бір әлеуетті осалдықты идентификациялау одан әрі зерттеуді қажет ететін басқа мүдделі саланы идентификациялауға әкелуі мүмкін қайталанатын идентификациялау процесі.

Бағалаушы жалпы қолжетімді ақпараттағы әлеуетті осалдықтарды идентификациялау үшін қандай әрекеттер жасалғанын көрсетуге тиіс.

Алайда, бағалаушы мұндай іздеу әдісі кезінде әдіс іздеу уақытында алынған нәтижеде анықталуы мүмкін болғандықтан, зерттеуді бастар алдында әлеуетті осалдықтарды идентификациялау бойынша операцияны сипаттай алмайды.

Бағалаушы зерттелген куәліктерді әлеуетті осалдықтарды іздеуді аяқтаған кезде көрсетеді.

Куәліктердің осы таңдамасы бұзушының қол жеткізуі мүмкін куәліктермен байланысты немесе бағалаушы ұсынатын басқа қисынды негіздемелерге сәйкес бағалаушының белгілі бір көздерден алуы мүмкін.

13.2.2.5 AVA_VAN.2.2E әрекеті. AVA_VAN.2-3 операциясы

Бағалаушы БО-дағы әлеуетті осалдықтарды идентификациялау үшін жалпы қолжетімді ақпарат көздерін зерттеуге тиіс.

Бағалаушы жалпы қолжетімді ақпарат көздерін БО-дағы ықтимал әлеуетті осалдықтарды идентификациялауды қамтамасыз ету үшін зерттеуге тиіс. Мыналар сияқты зерттелуге тиіс жалпы қолжетімді ақпарат көздері көп болады:

- а) мамандандырылған басылымдар (журналдар, кітаптар);
- б) ғылыми мақалалар.

Бағалаушы жоғарыда жазылған жалпы қолжетімді ақпарат көздері көрсеткен өз зерттеулерін шектемеуге тиіс, қайта басқа кез келген маңызды қолжетімді ақпаратты зерттеуі керек.

Бағалаушы ұсынылатын куәліктерді талдаумен қатар, кезекті іздеу үшін жалпы қолжетімді ақпарат көздеріндегі ақпаратты пайдаланатын болады. Бағалаушы қызықты саланы анықтаған кезде, бағалаушы қызықты салаға қатысты жалпы қолжетімді ақпаратты зерттеуге тиіс. Оңай қол жеткізетін ақпаратқа қол жеткізу бұзушыға идентификациялауға көмектеседі және шабуылға ықпал етеді, осы бұзушының шабуыл әлеуетін арттыра отырып әлеулі әрекет етеді. Ғаламтордағы осалдықтар және жетік бұзу құралдары туралы ақпаратқа қол жеткізу осы ақпараттың БО әлеуетті осалдығын идентификациялау және оларды пайдалану әрекетінде пайдаланатындығы туралы ықтималдықты арттырады. Осындай ақпаратты уақытылы іздеу құралдары оны бағалаушы үшін оңай қол жететін етеді және жарияланған әлеуетті осалдықтарға және жақсы белгілі қарапайым шабуылдарға қарсы әрекетті анықтауға жоғары тиімді тәсілмен қол жеткізуге болады.

Жалпы қолжетімді ақпаратты іздеу типіне БО жататын өнімдермен айналысатын ресурстарда топталуға тиіс. Осындай іздеудің ұлғаюы мынадай факторлармен анықталуға тиіс: ОО типі, бағалаушының осындай типтегі БО жұмыс тәжірибесі, әлеуетті шабуылдар ықтималдығы және қолда бар куәліктер бойынша ADV деңгейі.

Бір әлеуетті осалдықты идентификациялау одан әрі зерттеуді қажет ететін басқа мүдделі саланы идентификациялауға әкелуі мүмкін қайталанатын идентификациялау процесі.

Бағалаушы жалпы қолжетімді ақпараттағы әлеуетті осалдықтарды идентификациялау үшін қандай әрекеттер жасалғанын көрсетуге тиіс.

Алайда, бағалаушы мұндай іздеу әдісі кезінде әдіс іздеу уақытында алынған нәтижеде анықталуы мүмкін болғандықтан, зерттеуді бастар алдында әлеуетті осалдықтарды идентификациялау бойынша операцияны сипаттай алмайды.

Бағалаушы зерттелген куәліктерді әлеуетті осалдықтарды іздеуді аяқтаған кезде көрсетеді.

Куәліктердің осы таңдамасы бұзушының қол жеткізуі мүмкін куәліктермен байланысты немесе бағалаушы ұсынатын басқа қисынды негіздемелерге сәйкес бағалаушының белгілі бір көздерден алуы мүмкін.

13.2.2.6 AVA_VAN.2.3Е әрекеті

13.2.2.6.1 AVA_VAN.2-4 операциясы

Бағалаушы БО-дағы әлеуетті осалдықтарды идентификациялау үшін ҚТ, нұсқау, функционалдық сипаттізім, БО жобасы, қауіпсіздік құрылымының сипаттауын зерделеуге тиіс.

Куәліктерді іздеу осы сипаттізімге сәйкес аяқталуы керек және БО құжаттары талдануға тиіс және осыдан кейін БО-дағы осалдықтар туралы гипотезалар мен ұсыныстар құрылады.

Содан соң болжанатын осалдықтар бағаланған осалдықтың болу ықтималдығы негізінде және осалдықтың оны пайдалану үшін талап етілетін шабуыл әлеуеті негізінде болатын, сондай-ақ бұзушыға ұсынылатын мүмкіндіктер немесе нақты осалдықпен байланысты болжанатын зиян басымдықтары бойынша реттеледі. Әлеуетті осалдықтардың басымдықтар бойынша реттелген тізбесі БО енуді тестілеу нұсқауы үшін пайдаланылады.

Қауіпсіздік құрылымының сипаттауы әзірлеушінің талдауын қарастырады, соның салдарынан ондағы құжатталған ОФҚ сенімсіз субъектілердің қол сұғуынан қорғалады және жалпы қауіпсіздік талаптарын аралауды болдырмайды. Бағалаушының осының салдарынан ОФҚ қорғауды сипаттау деректерін ОФҚ бұзудың ықтимал жолдарын іздеуге арналған негіз ретінде пайдалануға тиіс.

Алдын ала анықталған ортада қатыстырылатын нақты қатерлерге байланысты, бағалаушы осалдықтарды тәуелсіз талдау кезінде мынадай тараулардың бірінің әрқайсысына тән осалдықты қарастыруы керек:

а) сертификаттау жөніндегі орган көрсетуі мүмкін бағаланатын БО нақты типіне тән осалдықтар;

б) аралау;

в) қол сұғу;

г) тура шабуылдар;

д) қадағалау;

е) дұрыс емес қолдану.

б) - е) тармақтары В қосымшасында барынша толық түсіндіріледі.

Қауіпсіздік құрылымын сипаттаулар жоғарыда аталған ерекше әлеуетті осалдықтарға қатысты зерттелуге тиіс.

Әрбір әлеуетті осалдық ОФҚ қорғауды аралау және ОФҚ қиратылатын кезде ықтимал жолдардың болу мәнін зерттеуге тиіс.

13.2.2.6.2 AVA_VAN.2-5 операциясы

Бағалаушы БТЕ тестілеуге кандидат болып табылатын және оның алдын ала анықталған ортасында БО қолданылатын идентификацияланған әлеуетті осалдықтарды көрсетуге тиіс.

Мүмкін, егер бағалаушы шаралардың не алдын ала анықталған ортада, не АТ алдын ала анықталған ортадағы осалдықтарды пайдалануды болдырмайтынын идентификацияласа, әлеуетті осалдықтарды одан әрі зерттеудің қажеті жоқтығы анықталатын болады. Мысалы, тек уәкілетті пайдаланушыларға ғана БО жеке қол жеткізуін шектей отырып, пайдалану үшін жарамсыз қол сұғуға БО осалдығын нақты жасауға болады.

Егер бағалаушы әлеуетті осалдықтың алдын ала анықталған ортада жарамсыздығын анықтайтын болса, бағалаушы әлеуетті осалдықты зерттеуден бас тартуға арналған толық себепті көрсетеді.

Қалған жағдайларда, бағалаушы одан әрі зерттеулер үшін әлеуетті осалдықтарды көрсетеді.

БО оның алдын ала анықталған ортасында жарамды және енгізу тестілерін орындау үшін пайдаланылуы мүмкін әлеуетті осалдықтар тізімін бағалаушы БТЕ көрсетуге тиіс.

13.2.2.7 AVA_VAN.2.4E әрекеті

13.2.2.7.1 AVA_VAN.2-6 операциясы

Бағалаушы әлеуетті осалдықтарды тәуелсіз іздеуге негізделген енгізу тестілерін әзірлеуге тиіс.

Бағалаушы өту тестілеуіне жалпы қолжетімді ақпарат көздерінде іздеу барысында идентификацияланған әлеуетті осалдықтарға БО оның алдын ала анықталған ортасында қабылдағыштығын анықтау үшін жеткілікті түрде дайындалуға тиіс. Бағалаушыға белгілі әлеуетті осалдықтарға қатысты үшінші тараптан (мысалы, сертификаттау жөніндегі орган) ұсынылатын кез келген ағымдағы ақпаратты бағалаушы бағалау бойынша басқа әрекеттерді орындау барысында анықталатын кез келген әлеуетті осалдықпен қатар зерттеуі қажет.

Бағалаушыға осалдықтарды іздеуде қауіпсіздік құрылымын сипаттауды талдау үшін (AVA_VAN.3-4 нақтыланған сияқты), тестілеудің құрылым қасиеттерін растаумен жүргізілу керектігі хабарланады. Қауіпсіздік құрылымының қасиеттерін теріске шығаратын теріс нәтижесі болатын тестінің қажет болуы ықтимал. Бағалаушы енуді тестілеу стратегиясын әзірлеуде қауіпсіздік құрылымын сипаттайтын барлық аспектілердің қолданылуын тестілеу және бағалаушының енуді тестілеуі сияқты тестіленгеніне көз жеткізуге тиіс.

Бағалаушының әрбір тестілер жиынтығы нақты осалдықты тестілеу үшін пайдаланылатын жерде бірқатар тестілер жиынтығын пайдалана отырып, өтуді тестілеуді орындау мақсатқа сәйкес деп санауы ықтимал.

Бағалаушының осалдық болатын затты шабуылды іске асыру үшін төмен әлеует талап етілетіндерден басқа, тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі).

Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеулер нәтижесінде төменгіге қарағанда, жоғары шабуыл әлеуетімен ғана бұзушы пайдалануға жарамды болып табылатын кезде ол БТЕ қалдық осалдық сияқты беріледі.

Әлеуетті осалдықты пайдалануға арналған қажетті шабуыл әлеуетін есептеу жөніндегі нұсқау В.4 қосымшасында берілген.

Төмен, орташа немесе жоғары шабуыл әлеуетіне ие бұзушылар ғана пайдалануы үшін жарамды болып болжанатын осалдықтар бағалаушының осы әрекеті бойынша теріс қорытындыға әкелмейді. Талдау материалдары осы гипотезаны растайтын кезде, онда тиісті осалдықтар енуді тестілеуге арналған бастапқы деректер ретінде қарастырылмайды. Алайда осындай осалдықтар БТЕ қалдық осалдықтар ретінде келтіріледі.

Төмен, орташа немесе жоғары шабуыл әлеуетіне ие бұзушылар ғана пайдалануы үшін жарамды болып болжанатын және қауіпсіздік мақсаттарының бұзылуына әкелетін осалдықтарды БО енуді тестілеуге арналған нұсқау үшін пайдаланылатын тізбеде болатын аса жоғары басымдықты әлеуетті осалдыққа жатқызуға болады.

13.2.2.7. AVA_VAN.2-7 операциясы

Бағалаушы нақтылауы тестілер өндірімділігін қамтамасыз ету үшін жеткілікті әлеуетті осалдықтар тізіміне негізделген өту тестілеріне арналған тестілеу құжаттамасын әзірлеуге тиіс.

Тестілеу құжаттамасында қамтылуы керек:

- а) тестіленетін БО айқын осалдығын идентификациялау;
- б) нақты енгізу тестісін өткізу үшін талап етілетін сияқты талап етілетін барлық тестілеу жабдықтарын қосу және орнату жөніндегі нұсқаулықтар;
- в) енгізу тестісін орындаудың барлық алғы шарттарын белгілеу жөніндегі нұсқаулықтар;

г) ОФҚ инициирлеу жөніндегі нұсқаулықтар;
д) ОФҚ орындау режимін қадағалау жөніндегі нұсқаулықтар;
е) күтілетін нәтижелермен салыстыру үшін ОФҚ қадағаланатын орындау режиміне қатысы бойынша орындалатын күтілетін барлық нәтижелерді және қажетті талдауды сипаттау;

ж) БО жай-күйін тестілеуден кейінгі қажетті тестілеу және орнатуды аяқтау жөніндегі нұсқаулықтар.

Бағалаушы жалпы қолжетімді орындардан іздеу және бағалау куәліктерін талдау барысында идентификацияланған әлеуетті осалдықтар тізбесіне негізделген енуді тестілеуге дайындалады.

Бағалаушының осалдық болатын затты шабуылды іске асыру үшін төмен әлеует талап етілетіндерден басқа, тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеулер нәтижесінде төменгіге қарағанда, жоғары шабуыл әлеуетімен ғана бұзушы пайдалануға жарамды болып табылатын кезде ол БТЕ қалдық осалдық сияқты беріледі.

Бағалаушы болжанатын осалдықты түсініп, БО қабылдағыштығын қолайлы тестілеу тәсілін анықтайды. Атап айтқанда, бағалаушы мынаны қарастырады:

а) ОФҚ орындау және олардың реакцияларын қадағалауды инициирлеу үшін пайдаланылатын ОФҚИ немесе басқа БО интерфейстері (Бағалаушыға қауіпсіздік құрылымын сипаттауда суреттелетін ОФҚ қасиеттерін көрсету үшін басқа ОФҚ емес, БО арналған интерфейс талап етіледі (ADV_ARC талап ететін сияқты)). Бұл БО осы интерфейстері ОФҚ қасиеттерін тестілеу тәсілдерін болжайтындығымен ескерілгенмен, олар тестілеу объектісі болып табылмайды;

б) тестіні орындау үшін қажет болатын бастапқы шарттар (яғни, қажет болатын қандай да бір нақты объектілер немесе субъектілер және оларда болуы қажет қауіпсіздік атрибуттары);

в) ОФҚИ инициирлеу, не ОФҚИ қадағалау үшін қажет болатын тестілеуге арналған арнайы жабдық (дегенмен, арнайы жабдықтың айқын осалдықты пайдалану үшін қажет болуы екіталай);

г) жеке тестілеуді теориялық талдаумен ауыстыру, әсіресе, бастапқыда талдау нәтижелері қайталанатын шабуыл әрекеттерінің белгілі бір әрекеттер санынан кейін сәтті болу ықтималдығын көрсету үшін сыртқа таратылғаны маңызды.

Бағалаушының әрбір тесті жинағы нақты осалдықты тестілеу үшін пайдаланылатын жерде бірқатар тестілер жинағын пайдалана отырып, енуді тестілеуді орындау мақсатқа сәйкес деп санауы ықтимал.

Тестілеу құжаттамасында осы нақтылау деңгейін белгілеу мақсаты – басқа бағалаушыға тестіні қайталауға және балама нәтиже алуға мүмкіндік беру.

13.2.2.7.3 AVA_VAN.2-8 операциясы

Бағалаушы енуді тестілеуді жүргізуге тиіс.

Бағалаушы AVA_VAN.2-6 операциясында әзірленген ену тестілеріне арналған құжаттаманы ену тестілерін БО қатысы бойынша орындауға арналған негіз ретінде пайдаланады, бірақ бұл бағалаушыға қосымша арнайы ену тестілерін орындауға кедергі жасамайды. Егер қажет болса, бағалаушы енуді тестілеу процесінде ақпаратты зерделеу нәтижесінде арнайы тестілер ойлап таба алады, егер бағалаушы орындаса, ену тестілеріне арналған құжаттамаға кіргізіледі. Мұндай тестілер күтпеген нәтижелер немесе қадағалауларды түсіну немесе бағалаушы алдын ала жоспарланған тестілеу уақытында болатынын аңғарған әлеуетті осалдықтарды зерттеу үшін қажет болуы мүмкін.

Егер енгізу тестісі болжанатын әлеуетті осалдықтың болмайтынын көрсетсе, бағалаушы бағалаушының өзінің талдауының дұрыс болмағанын немесе дайындалған бағалаудың дұрыс емес немесе жеткіліксіз екенін анықтауға тиіс.

Шабуылды іске асыру үшін төменгі әлеует талап етілетіндерден басқа, бағалаушының осалдық болатын затты тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеу нәтижесінде төменгі шабуыл әлеуетіне қарағанда, бұзушының үлкен әлеуетті пайдалануы үшін ғана жарамды болып табылатын әлеуетті осалдықты байқаған кезде, ол БТЕ-де қалдық осалдық ретінде келтіріледі.

13.2.2.7.4 AVA_VAN.2-9 операциясы

Бағалаушы ену тестілерінің нақты нәтижелерін белгілеуге тиіс.

Дегенмен, тестілерді орындаудың нақты нәтижелерінің кейбір өзгеше бөлшектері күтілетіннен ерекшеленуі мүмкін (мысалы, аудит жазбасындағы уақыт өрісі және күні), жалпы нәтиже бірдей болуы қажет. Кез келген айырмашылықты қатаң түрде негіздеу керек.

13.2.2.7.5 AVA_VAN.2-10 операциясы

Бағалаушы БТЕ тестілеу тәсілін, тестіленетін пішін үйлесімін, тестілеу белгілемесі мен тестілеу нәтижелерін қысқаша баяндап, енуді тестілеу бойынша бағалаушының шарттары туралы ақпаратты келтіруге тиіс.

Бағалаушының БТЕ келтіретін тестілеу туралы ақпараты тестілеу бойынша қызмет түрін бағалау барысында жұмсалған күшті және тестілеуге арналған жалпы тәсілді беруге мүмкіндік жасайды. Осы ақпаратты ұсыну мәні тестілеу бойынша күшке қысқаша мазмұнды шолу жасау. БТЕ тестілеу туралы ақпараттың жеке тестілердің нақты тестілеу операциялары немесе

нәтижелерінің дәл туындысы болуы міндетті емес. Әзірлеушінің БТЕ тестілеу туралы ақпаратының нақты тестілеу операциясының немесе жеке тестілер нәтижелерінің дәлме-дәл көшірмесі болуының мәні жоқ. Басқа бағалаушылар мен сертификаттау жөніндегі қызметкерлерге әзірлеушінің тестілеу тәсіліне қатысты орындалған тестілеу, БО тестіленетін пішін үйлесімдері көлемін және әзірлеушінің жалпы тестілеу нәтижелерін кейбір түсіну үшін мүмкіндік беретін жеткілікті нақтылаулар ұсыну мақсат болып табылады.

Әзірлеушінің енуді тестілеу жөніндегі ақпаратты, әдетте, БТЕ тиісті бөлімінен табуға болады, ол мынаны қамтиды:

а) БО тестіленетін пішін үйлесімдері. Енуді тестілеуге түсетін БО нақты пішін үйлесімдері;

б) Енуді тестілеуге түсетін ОФҚИ. Енуді тестілеу бағытталатын ОФҚИ және БО басқа интерфейстерінің қысқаша тізбесі;

в) Қызметтің осы ішкі түрі бойынша ұйғарым. Енуді тестілеу нәтижелері бойынша жалпы шешім.

Осы тізбе ешқандай жағдайда да БТЕ ұсынылуға тиіс бағалау барысында бағалаушы орындайтын енуді тестілеуге қатысты ақпарат типі туралы кейбір түсінік беру үшін ғана тағайындалған және жан-жақты болып табылмайды.

13.2.2.7.6 AVA_VAN.2-11 операциясы

Бағалаушы барлық тестілеу нәтижелерін өзінің алдын ала анықталған ортасында болатын БО төменгі шабуыл әлеуетіне ие бұзушыға орнықты болып табылатынын анықтау үшін зерттеуге тиіс.

Егер нәтижелер өзінің алдын ала анықталған ортасында болатын БО орташа шабуыл әлеуетіне қарағанда аз әлеуетке ие бұзушының пайдалануы үшін жарамды осалдығы болатынын көрсетсе, онда осы әрекет бойынша бағалаушы теріс қорытынды жасайды.

Нақты осалдықты пайдалану үшін қажетті шабуыл әлеуетін және осының салдарынан берілген ортада оның пайдаланылуын анықтау үшін нұсқаудың В.4 тармағы пайдаланылуға тиіс.

Орташаға қарағанда әлеуеті аз болатын бұзушының осалдықты пайдалана ма немесе жоқ па деген күдіктер болатын жағдайда қоспағанда, әр жолы шабуыл әлеуетін есептеп қажеті жоқ.

13.2.2.7.7 AVA_VAN.2-12 операциясы

Бағалаушы БТЕ әрбіреуі үшін нақтыланатын барлық пайдалануға жарамды осалдықтар мен қалдық осалдықтар туралы ақпаратты келтіруге тиіс:

а) оның көзі (мысалы, бағалау бойынша әрекеттерді орындаған кезде белгілі болған, бағалаушыға белгілі, жарияланымда оқылды);

б) ФҚТ жауап бермейтін;

в) сипаттау;

г) алдын ала анықталған ортада ол пайдаланыла ма, жоқ па (яғни, не пайдалану үшін жарамды немесе қалдық осалдық болып табылады);

д) В.4 қосымшасының В.2 және В.3 кестесін пайдалана отырып, осалдықты және тиісті мәндерді идентификациялауды орындау үшін қажетті уақыт көлемі, талдау деңгейі, БО білу деңгейі, мүмкіндіктер деңгейі және жабдық.

13.2.3 (AVA_VAN.3) қызметінің ішкі түрін бағалау

13.2.3.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты БО-ның өзінің алдын ала анықталған ортасында төменгі шабуыл әлеуеті болатын бұзушыға осалдықтың жарамды екенін анықтау.

13.2.3.2 Бастапқы деректер

Қызметтің осы ішкі түрінің бағалау куәліктері болып табылады:

- а) ҚТ;
- б) функционалдық сипаттізім;
- в) БО жобасы;
- г) қауіпсіздік құрылымын сипаттау;
- д) таңдалған ішжиынды жүзеге асыру;
- е) нұсқау;
- ж) тестілеу үшін жарамды БО;
- и) әлеуетті осалдықтарды идентификациялауды қамтамасыз ететін жалпы қолжетімді ақпарат.

Қызметтің осы ішкі түрі үшін қалған болжанатын бағалау куәліктері сенім пакетінде қамтылатын құрауыштарға тәуелді болады. Әрбір құрауышты қамтамасыз ететін куәліктер қызметтің осы ішкі түрінде бастапқы ретінде пайдаланылады.

Қызметтің осы ішкі түрі үшін айқын осалдықтарға қатысты ағымдағы ақпарат қосымша бастапқы материал болып табылады (мысалы, сәйкестікті растау жөніндегі органнан болатын).

13.2.3.3 Қолдану бойынша ескертулер

Бағалаушы бағалау бойынша әрекеттерді орындаған уақытта мүдделі саланы идентификациялай алады.

Бағалаушы қалдыратын БО куәліктерінің осы ерекше бөлімдері куәлікпен байланысты қызмет талаптарына жауап береді. Үлгі үшін, жеке интерфейс сипаттізімі арнайы жиынтықты іздейді және сондықтан БО әзірлеу уақытындағы сияқты БО пайдалану уақытында қате жіберуге бейім болады. Осы операцияда әлеуетті осалдықтың одан әрі зерттеуде талап етпеуі анық. Бұл кездейсоқ емес, сондықтан одан әрі зерттеуде талап етеді.

Әлеуетті осалдықты идентификациялаудың арнайы әдісі бұл ақпаратта болатын кез келген әлеуетті осалдықты идентификациялау мақсатында куәландыруды талдау. Бұл әдіс анықталмағандықтан, құрастырылмаған талдау. Талдауға арналған кезекті нұсқаулар В қосымшасында көрсетілген.

13.2.3.4 AVA_VAN.3.1E әрекеті

БО тестілеу үшін жарамды болуға тиіс.

13.2.3.4.1 AVA_VAN.3-1 операциясы

Бағалаушы БО тестіленетін пішін үйлесімінің ҚТ анықталған бағалау пішін үйлесімімен келісілгені туралы қорытынды жасау үшін зерттеуге тиіс.

Бағалаушының тестілеу үшін пайдаланатын БО УК қызметінің ішкі түрінің мүмкіндіктерімен белгіленетін дәл сондай бірегей таңбалауы болуы және ҚТ кіріспе бөлімінде идентификациялануы керек.

ҚТ бағалануға тиіс бірнеше пішін үйлесімі анықталуға тиіс. БО ҚТ сәйкестігіне тестіленуге тиіс әр түрлі бірқатар аппараттық және программалық жүзеге асырулардан тұруы мүмкін.

Бағалаушы тестілеу ортасына қатысы болуы мүмкін БО қауіпсіздік ортасының аспектілеріне қатысты ҚТ сипатталған болжамдарды қарастыруы керек. ҚТ тестілеу ортасына қатысы болмайтын басқа да болжамдар болуы мүмкін. Мысалы, пайдаланушылардың рұқсатнамасына қатысты болжам тестілеу ортасына қатысты болмауы мүмкін, алайда, желіге қосылатын бірыңғай нүктеге қатысты болжам, әдетте, тестілеу ортасына қатысты болады.

Қандай да болмасын тестілеу құралдарын пайдаланған кезде (мысалы, өлшеуіштер, талдағыштар) осы құралдардың дұрыс калибрленуін қамтамасыз ету бағалаушының міндеті болады.

13.2.3.4.2 AVA_VAN.3-2 операциясы

Бағалаушы БО оның дұрыс орнатылғаны және белгілі күйінде болатыны туралы қорытынды жасау үшін зерттеуге тиіс.

Бағалаушының бірнеше тәсілдермен БО жай-күйі туралы қорытынды жасауға мүмкіндігі бар.

Мысалы, осының алдындағы (AGD_PRE.1) қызметінің ішкі түрін сәтті аяқтау тестіленетін БО егер тиісті түрде орнатылғанына және белгілі жағдайда екендігіне бағалаушы әлі сенімді болмаса, осы операцияны орындалған деп санауға мүмкіндік береді. Егер бұл бұлай болмаса, онда бағалаушыға жеткізілген нұсқауды ғана пайдалана отырып, БО орнату, өндіру және іске қосу үшін әзірлеушінің процедураларын басшылыққа алу ұсынылады.

Егер бағалаушыға БО белгісіз жай-күйде болуы салдарынан орнату процедураларын орындауға тура келсе, онда сәтті аяқтаған кезде осы операция AGD_PRE.1-3 операциясын қанағаттандырған болар еді.

13.2.3.5 AVA_VAN.3.2E әрекеті. AVA_VAN.3-3 операциясы

Бағалаушы БО әлеуетті осалдықтарын идентификациялау үшін жалпы қолжетімді ақпарат көздерін зерттеуге тиіс.

Бағалаушы БО әлеуетті осалдықтарын идентификациялау үшін жалпы қолжетімді ақпаратты зерттеуге тиіс.

Бағалаушы, мысалы, бүкіләлемдік өрмекте қолжетімді ақпаратты пайдалана отырып зерттеуге тиіс жалпы қолжетімді ақпарат көздері болады, мыналарды қоса алғанда:

- а) конференция хаттамалары;
- б) мамандандырылған басылымдар (журналдар, кітаптар);
- в) ғылыми мақалалар.

Бағалаушы өзінің жалпы қолжетімді ақпаратты зерттеулерін жоғарыда аталған көздермен шектемеуге тиіс, кез келген маңызды қолжетімді ақпаратты зерттеуі қажет.

Бағалаушы ұсынылатын куәліктерді талдаумен қатар, кезекті іздеу үшін жалпы қолжетімді ақпарат көздеріндегі ақпаратты пайдаланатын болады. Бағалаушы қызықты саланы анықтаған кезде, бағалаушы қызықты салаға қатысты жалпы қолжетімді ақпаратты зерттеуге тиіс.

Оңай қол жеткізетін ақпаратқа қол жеткізу бұзушыға идентификациялауға көмектеседі және шабуылға ықпал етеді, осы бұзушының шабуыл әлеуетін арттыра отырып елеулі әрекет етеді. Ғаламтордағы осалдықтар және жетік бұзу құралдары туралы ақпаратқа қол жеткізу осы ақпараттың БО әлеуетті осалдығын идентификациялау және оларды пайдалану әрекетінде пайдаланатындығы туралы ықтималдықты арттырады. Осындай ақпаратты уақытылы іздеу құралдары оны бағалаушы үшін оңай қол жететін етеді және жарияланған әлеуетті осалдықтарға және жақсы белгілі қарапайым шабуылдарға қарсы әрекетті анықтауға жоғары тиімді тәсілмен қол жеткізуге болады.

Жалпы қолжетімді ақпаратты іздеу типіне БО жататын өнімдермен айналысатын ресурстарда топталуға тиіс. Осындай іздеудің ұлғаюы мынадай факторлармен анықталуға тиіс: ОО типі, бағалаушының осындай типтегі БО жұмыс тәжірибесі, әлеуетті шабуылдар ықтималдығы және қолда бар куәліктер бойынша ADV деңгейі.

Бір әлеуетті осалдықты идентификациялау одан әрі зерттеуді қажет ететін басқа мүдделі саланы идентификациялауға әкелуі мүмкін қайталанатын идентификациялау процесі.

Бағалаушы жалпы қолжетімді ақпараттағы әлеуетті осалдықтарды идентификациялау үшін қандай әрекеттер жасалғанын көрсетуге тиіс. Алайда, бағалаушы мұндай іздеу әдісі кезінде әдіс іздеу уақытында алынған нәтижеде анықталуы мүмкін болғандықтан, зерттеуді бастар алдында әлеуетті осалдықтарды идентификациялау бойынша операцияны сипаттай алмайды.

Бағалаушы әлеуетті осалдықтарды іздеуді аяқтаған кезде зерттелген куәліктерді көрсетеді. Аталған куәліктер таңдамасы бұзушының қолы жетуі мүмкін болып саналатын куәліктермен байланысты немесе бағалаушы ұсынатын қисынды негіздемелерге сәйкес бағалаушы анықтайтын көздерден алынуы мүмкін.

13.2.3.6 AVA_VAN.3.3E әрекеті

13.2.3.6.1 AVA_VAN.3-4 операциясы

Бағалаушы БО-дағы әлеуетті осалдықтарды идентификациялау үшін ҚТ, нұсқау, функционалдық сипаттізім, БО жобасы, қауіпсіздік құрылымының сипаттауын зерделеуге тиіс.

Куәліктерді іздеу осы сипаттізімге сәйкес аяқталуы керек және БО құжаттары талдануға тиіс және осыдан кейін БО-дағы осалдықтар туралы гипотезалар мен ұсыныстар құрылады.

Бағалаушы БО әзірлемесіндегі әлеуетті кемшіліктерді және БО қолданылатын осы әдістердегі әлеуетті қателіктерді идентификациялау үшін, кемшіліктер туралы болжамдар жасау үшін жеткізілген БО алынатын БО жобасы мен пайдалану мәнін пайдаланады.

Қауіпсіздік құрылымының сипаттауы әзірлеушінің талдауын қарастырады, соның салдарынан ондағы құжатталған ОФҚ сенімсіз субъектілердің қол сұғуынан қорғалады және жалпы қауіпсіздік талаптарын аралауды болдырмайды. Сондықтан бағалаушы осы куәліктерді талдаудан алынатын ОФҚ қорғау түсінігіне сүйенуге тиіс және содан кейін ғана оларды ADV басқа әзірлемелерінің куәліктерін талдаудан алынған біліммен дамытуы қажет.

Бағалау жөніндегі әрекеттерді іске асыру барысында куәліктерді талдау уақытында идентификацияланған мүдделер саласында көрсетілген және бағалау үшін ұсынылған әзірлемелер мен нұсқаулардың ерекше үлгілерімен кепілдік берілген осы әдіс анықталады.

Таңдама жөніндегі нұсқауды А қосымшасынан қараңыз. Аталған нұсқау мынаны негізге ала отырып, ішжиынды таңдау кезінде зерделенуге тиіс:

- а) таңдауда пайдаланылған тәсіл;
- б) куәліктің осындай әдіске жарамдылығы.

Мүдделер саласы қауіпсіздік құрылымын сипаттауда ерекше толық қорғау қасиеттерінің жеткіліктілігімен байланысты болуы мүмкін.

Бағалау барысында пайдаланылатын куәліктер бұзушының ие болуы мүмкін деп болжанатын куәліктермен байланысты болуы ықтимал. Үлгі үшін, әзірлеуші БО жобасын және жүзеге асыру көрсетілімін қорғауы мүмкін, демек, бұзушының қолы жететін ақпарат бұл тек функционалдық сипаттізім мен нұсқау (жалпы қолжетімді). Сондықтан, БО сенімділік объектілерінің БО жобасының жобаны көрсету талаптарына жауап беретініне кепілдік беретініне қарамастан, мүдделі салаларды одан әрі зерттеу үшін ғана пайдаланылуы мүмкін.

Екінші жағынан, егер көз жалпы қолжетімді болса, бұзушының ресурсқа қолы жететінін және оны БО шабуыл әрекеті үшін пайдалана алатынын дәлелді жобалауға болады. Сондықтан көз арнайы талдамдау әдісімен зерттелуі керек.

Төменде талданатын куәліктердің ішжиынынан таңдауға арналған үлгілер беріледі:

а) жоба абстракциясының барлық деңгейі функционалдық сипаттізімнен бастап жүзеге асыруды көрсетуге дейін ұсынылатын жердегі барлық бағалау үшін бұзушы үшін интерфейс бөлшектерін қолжетімді жасайтын функционалды сипаттізім және жобаның барлық басқа абстракцияларында орындалған жобаның шешімін біріктіретін жүзеге асыруды көрсету ретінде таңдалуы мүмкін.

Сондықтан БО жобасы туралы ақпарат көрсетуді жүзеге асыру бөлігі ретінде зерттелетін болады.

б) жобаның әрбір көрсетіміндегі ақпараттың жеке ішжиынын талдау бағалауды қарастырады.

в) жобаның әрбір көрсетімі арқылы жеке ФҚТ бүркеу бағалауды қарастырады.

г) жобаның әрбір көрсетілімі ішінде әр түрлі ФҚТ зерттейтін бағалауға ұсынылатын жобаның әрбір көрсетімін талдау.

д) бағалаушы алған әлеуетті осалдықтар туралы ақпаратпен байланысты бағалауға ұсынылатын куәліктер аспектілерін талдау (мысалы, бағалау жүйелерінен).

Әлеуетті осалдықтың осы идентификациялау әдісі – бұл талдауға арналған жүйені пайдалану үшін реттелген және жоспарлы тәсіл.

Бағалаушы болжамдар жасалған ақпарат талданған тәсіл, куәліктер ішінде талданатын ақпаратта қандай куәліктер зерттелгені мәнінде пайдаланылған әдістерді сипаттайды.

Төменде жасалуға тиіс болжамдар үлгісі беріледі:

а) интерфейсстерге арналған пішіні өзгерген кіруді талдау сыртқы интерфейсстер болатын бұзушыға ғана қолжетімді;

б) процесті бөлу сияқты қауіпсіздік құрылымын сипаттауға сүйенетін қауіпсіздік механизмінің кілтін талдау, бөлуді нашарлатуы мүмкін аралықшаны толтыру болжанады;

в) БО көрсетімін жүзеге асыруда кез келген объектіні идентификациялауға бағытталған іздеу толық бақыланады, ал содан соң ОФҚ болмайды және ФҚТ бұзу үшін бұзушының пайдалануы мүмкін.

Мысалы, бағалаушы интерфейсстердің БО әлсіз жағы болып табылатынын идентификациялай және «функционалдық сипаттізімде ұсынылатын барлық интерфейсстердің сипаттізімі және БТЕ жобасында әлеуетті осалдықтарды болжау қарастырылатыны» бойынша анықтай және болжамдар үшін пайдаланылатын әдістерді түсіндіруді жалғастыра алады.

Бір әлеуетті осалдықты идентификациялау одан әрі зерттеуді қажет ететін басқа мүдделі саланы идентификациялауға әкелуі мүмкін қайталанатын идентификациялау процесі.

Бағалаушы жалпы қолжетімді ақпараттағы әлеуетті осалдықтарды идентификациялау үшін қандай әрекеттер жасалғанын көрсетуге тиіс. Алайда, бағалаушы мұндай іздеу әдісі кезінде әдіс іздеу уақытында алынған нәтижеде анықталуы мүмкін болғандықтан, зерттеуді бастар алдында әлеуетті осалдықтарды идентификациялау бойынша операцияны сипаттай алмайды.

Бағалаушы зерттелген куәліктерді әлеуетті осалдықтарды іздеуді аяқтаған кезде көрсетеді.

Куәліктердің осы таңдамасы бұзушының қол жеткізуі мүмкін куәліктермен байланысты немесе бағалаушы ұсынатын басқа қисынды негіздемелерге сәйкес бағалаушының белгілі бір көздерден алуы мүмкін.

Алдын ала анықталған ортада қатыстырылатын нақты қатерлерге байланысты, бағалаушы осалдықтарды тәуелсіз талдау кезінде мынадай тараулардың бірінің әрқайсысына тән осалдықты қарастыруы керек:

а) сертификаттау жөніндегі орган көрсетуі мүмкін бағаланатын БО нақты типіне тән осалдықтар;

б) аралау;

в) қол сұғу;

г) тура шабуылдар;

д) қадағалау;

е) дұрыс емес қолдану.

б) - е) тармақтары В қосымшасында барынша толық түсіндіріледі.

Қауіпсіздік құрылымын сипаттаулар жоғарыда аталған ерекше әлеуетті осалдықтарға қатысты зерттелуге тиіс. Әрбір әлеуетті осалдық ОФҚ қорғауды аралау және ОФҚ қиратылатын кезде ықтимал жолдардың болу мәнін зерттеуге тиіс.

13.2.3.6.2 AVA_VAN.3-5 операциясы

Бағалаушы БТЕ тестілеуге кандидат болып табылатын және оның алдын ала анықталған ортасында БО қолданылатын идентификацияланған әлеуетті осалдықтарды көрсетуге тиіс.

Мүмкін, егер бағалаушы шаралардың не алдын ала анықталған ортада, не АТ, не АТ емес ортада алдын ала анықталған ортадағы осалдықтарды пайдалануды болдырмайтынын идентификацияласа, әлеуетті осалдықтарды одан әрі зерттеудің қажеті жоқтығы анықталатын болады. Мысалы, тек уәкілетті пайдаланушыларға ғана БО жеке қол жеткізуін шектей отырып, пайдалану үшін жарамсыз қол сұғуға БО осалдығын нақты жасауға болады

Егер бағалаушы әлеуетті осалдықтың алдын ала анықталған ортада жарамсыздығын анықтайтын болса, бағалаушы әлеуетті осалдықты зерттеуден бас тартуға арналған толық себепті көрсетеді.

Қалған жағдайларда, бағалаушы одан әрі зерттеулер үшін әлеуетті осалдықтарды көрсетеді.

БО оның алдын ала анықталған ортасында жарамды және енгізу тестілерін орындау үшін пайдаланылуы мүмкін әлеуетті осалдықтар тізімін бағалаушы БТЕ көрсетуге тиіс.

13.2.3.7 AVA_VAN.3.4E әрекеті

13.2.3.7.1 AVA_VAN.3-6 операциясы

Бағалаушы әлеуетті осалдықтарды тәуелсіз іздеуге негізделген енгізу тестілерін әзірлеуге тиіс.

Бағалаушы өту тестілеуіне жалпы қолжетімді ақпарат көздерінде іздеу барысында идентификацияланған әлеуетті осалдықтарға БО оның алдын ала анықталған ортасында қабылдағыштығын анықтау үшін жеткілікті түрде дайындалуға тиіс. Бағалаушыға белгілі әлеуетті осалдықтарға қатысты үшінші тараптан (мысалы, сертификаттау жөніндегі орган) ұсынылатын кез келген ағымдағы ақпаратты бағалаушы бағалау бойынша басқа әрекеттерді орындау барысында анықталатын кез келген әлеуетті осалдықпен қатар зерттеуі қажет.

Бағалаушыға осалдықтарды іздеуде қауіпсіздік құрылымын сипаттауды талдау үшін (AVA_VAN.3-4 нақтыланған сияқты), тестілеудің құрылым қасиеттерін растаумен жүргізілу керектігі хабарланады. Егер АТЕ_DPT болатын талаптар ФҚТ қамтылса, куәлікті тестілейтін әзірлеуші қауіпсіздік құрылымын сипатталып нақтыланған барлық арнайы құрылғылардың тиісінше көрсетілуін растайтын тестілеуді қосады. Алайда әзірлеушінің тестілерінде ОФҚ қорғайтын құрылымдардың барлық аспектілерін тестілеуді қамтуы міндетті емес, мұндай тестілеу қаншалықты теріс болатындықтан, шын мәнінде қасиеттерін теріске шығаруға тырысу керек. Бағалаушы енуді тестілеу стратегиясын әзірлеуде қауіпсіздік құрылымын сипаттайтын барлық аспектілердің қолданылуын тестілеу (13 зерттелгендей) және бағалаушының енуді тестілеуі сияқты тестіленгеніне көз жеткізуге тиіс.

Бағалаушының әрбір тестілер жиынтығы нақты осалдықты тестілеу үшін пайдаланылатын жерде бірқатар тестілер жиынтығын пайдалана отырып, өтуді тестілеуді орындау мақсатқа сәйкес деп санауы ықтимал.

Бағалаушының осалдық болатын затты шабуылды іске асыру үшін төмен әлеует талап етілетіндерден басқа, тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеулер нәтижесінде төменгіге қарағанда, жоғары шабуыл әлеуетімен ғана бұзушы пайдалануға жарамды болып табылатын кезде ол БТЕ қалдық осалдық сияқты беріледі.

Әлеуетті осалдықты пайдалану үшін қажетті шабуылдың қажетті әлеуетін анықтау бойынша нұсқау В қосымшасында болады.

Төмен, орташа немесе жоғары шабуыл әлеуетіне ие бұзушылар ғана пайдалануы үшін жарамды болып болжанатын осалдықтар бағалаушының осы әрекеті бойынша теріс қорытындыға әкелмейді. Талдау материалдары

осы гипотезаны растайтын кезде, онда тиісті осалдықтар енуді тестілеуге арналған бастапқы деректер ретінде қарастырылмайды. Алайда осындай осалдықтар БТЕ қалдық осалдықтар ретінде келтіріледі.

Төмен, орташа немесе жоғары шабуыл әлеуетіне ие бұзушылар ғана пайдалануы үшін жарамды болып болжанатын және қауіпсіздік мақсаттарының бұзылуына әкелетін осалдықтарды БО енуді тестілеуге арналған нұсқау үшін пайдаланылатын тізбеде болатын аса жоғары басымдықты әлеуетті осалдыққа жатқызуға болады.

13.2.3.7.2 AVA_VAN.3-7 операциясы

Бағалаушы тестілердің өндірімділігін қамтамасыз ету үшін жеткілікті нақтылаудың әлеуетті осалдықтары тізіміне негізделген ену тестілеріне арналған тестілеу құжаттамасын әзірлеуге тиіс.

Тестілеу құжаттамасында қамтылуы керек:

- а) тестіленетін БО осалдығын идентификациялау;
- б) нақты енгізу тестісін өткізу үшін талап етілетін сияқты талап етілетін барлық тестілеу жабдықтарын қосу және орнату жөніндегі нұсқаулықтар;
- в) енгізу тестісін орындаудың барлық алғы шарттарын белгілеу жөніндегі нұсқаулықтар;
- г) ОФҚ инициирлеу жөніндегі нұсқаулықтар;
- д) ОФҚ орындау режимін қадағалау жөніндегі нұсқаулықтар;
- е) күтілетін нәтижелермен салыстыру үшін ОФҚ қадағаланатын орындау режиміне қатысы бойынша орындалатын күтілетін барлық нәтижелерді және қажетті талдауды сипаттау;
- ж) БО жай-күйін тестілеуден кейінгі қажетті тестілеу және орнатуды аяқтау жөніндегі нұсқаулықтар.

Бағалаушы жалпы қолжетімді орындардан іздеу және бағалау куәліктерін талдау барысында идентификацияланған әлеуетті осалдықтар тізбесіне негізделген енуді тестілеуге дайындалады.

Бағалаушының осалдық болатын затты шабуылды іске асыру үшін төмен әлеует талап етілетіндерден басқа, тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеулер нәтижесінде төменгіге қарағанда, жоғары шабуыл әлеуетімен ғана бұзушы пайдалануға жарамды болып табылатын кезде ол БТЕ қалдық осалдық сияқты беріледі.

Бағалаушы болжанатын осалдықты түсініп, БО қабылдағыштығын қолайлы тестілеу тәсілін анықтайды. Атап айтқанда, бағалаушы мынаны қарастырады:

- а) ОФҚ орындау және олардың реакцияларын қадағалауды инициирлеу үшін пайдаланылатын ОФҚИ немесе басқа БО интерфейстері (Бағалаушыға қауіпсіздік құрылымын сипаттауда суреттелетін ОФҚ қасиеттерін көрсету үшін басқа ОФҚ емес, БО арналған интерфейс талап етіледі (ADV_ARC

талап ететін сияқты)). Бұл БО осы интерфейстері ОФҚ қасиеттерін тестілеу тәсілдерін болжайтындығымен ескерілгенмен, олар тестілеу объектісі болып табылмайды;

б) тестіні орындау үшін қажет болатын бастапқы шарттар (яғни, қажет болатын қандай да бір нақты объектілер немесе субъектілер және оларда болуы қажет қауіпсіздік атрибуттары);

в) ОФҚИ инициирлеу, не ОФҚИ қадағалау үшін қажет болатын тестілеуге арналған арнайы жабдық (дегенмен, арнайы жабдықтың айқын осалдықты пайдалану үшін қажет болуы екіталай);

г) жеке тестілеуді теориялық талдаумен ауыстыру, әсіресе, бастапқыда талдау нәтижелері қайталанатын шабуыл әрекеттерінің белгілі бір әрекеттер санынан кейін сәтті болу ықтималдығын көрсету үшін сыртқа таратылғаны маңызды.

Бағалаушының әрбір тесті жинағы нақты осалдықты тестілеу үшін пайдаланылатын жерде бірқатар тестілер жинағын пайдалана отырып, енуді тестілеуді орындау мақсатқа сәйкес деп санауы ықтимал.

Тестілеу құжаттамасында осы нақтылау деңгейін белгілеу мақсаты – басқа бағалаушыға тестіні қайталауға және балама нәтиже алуға мүмкіндік беру.

13.2.3.7.3 AVA_VAN.3-8 операциясы

Бағалаушы енуді тестілеуді жүргізуге тиіс.

Бағалаушы AVA_VAN.3-6 операциясында әзірленген ену тестілеріне арналған құжаттаманы ену тестілерін БО қатысы бойынша орындауға арналған негіз ретінде пайдаланады, бірақ бұл бағалаушыға қосымша арнайы ену тестілерін орындауға кедергі жасамайды. Егер қажет болса, бағалаушы енуді тестілеу процесінде ақпаратты зерделеу нәтижесінде арнайы тестілер ойлап таба алады, егер бағалаушы орындаса, ену тестілеріне арналған құжаттамаға кіргізіледі. Мұндай тестілер күтпеген нәтижелер немесе қадағалауларды түсіну немесе бағалаушы алдын ала жоспарланған тестілеу уақытында болатынын аңғарған әлеуетті осалдықтарды зерттеу үшін қажет болуы мүмкін.

Егер енгізу тестісі болжанатын әлеуетті осалдықтың болмайтынын көрсетсе, бағалаушы бағалаушының өзінің талдауының дұрыс болмағанын немесе дайындалған бағалаудың дұрыс емес немесе жеткіліксіз екенін анықтауға тиіс.

Шабуылды іске асыру үшін төменгі әлеует талап етілетіндерден басқа, бағалаушының осалдық болатын затты тестілеуі болжанбайды (оның ішінде жалпы қолжетімді көздерден белгілісі). Алайда кейбір жағдайларда талап етілетін шабуыл әлеуеті анықталғаннан бұрын тестіні орындау қажет болады. Бағалаушы бағалау барысында зерттеу нәтижесінде төменгі шабуыл әлеуетіне қарағанда, бұзушының үлкен әлеуетті пайдалануы үшін ғана

жарамды болып табылатын әлеуетті осалдықты байқаған кезде, ол БТЕ-де қалдық осалдық ретінде келтіріледі.

13.2.3.7.4 AVA_VAN.3-9 операциясы

Бағалаушы ену тестілерінің нақты нәтижелерін белгілеуге тиіс.

Дегенмен, тестілерді орындаудың нақты нәтижелерінің кейбір өзгеше бөлшектері күтілетіннен ерекшеленуі мүмкін (мысалы, аудит жазбасындағы уақыт өрісі және күні), жалпы нәтиже бірдей болуы қажет. Кез келген айырмашылықты қатаң түрде негіздеу керек.

13.2.3.7.5 AVA_VAN.3-10 операциясы

Бағалаушы БТЕ тестілеу тәсілін, тестіленетін пішін үйлесімін, тестілеу белгілемесі мен тестілеу нәтижелерін қысқаша баяндап, енуді тестілеу бойынша бағалаушының шарттары туралы ақпаратты келтіруге тиіс.

Бағалаушының БТЕ келтіретін тестілеу туралы ақпараты тестілеу бойынша қызмет түрін бағалау барысында жұмсалған күшті және тестілеуге арналған жалпы тәсілді беруге мүмкіндік жасайды. Осы ақпаратты ұсыну мәні тестілеу бойынша күшке қысқаша мазмұнды шолу жасау. БТЕ тестілеу туралы ақпараттың жеке тестілердің нақты тестілеу операциялары немесе нәтижелерінің дәл туындысы болуы міндетті емес. Әзірлеушінің БТЕ тестілеу туралы ақпаратының нақты тестілеу операциясының немесе жеке тестілер нәтижелерінің дәлме-дәл көшірмесі болуының мәні жоқ. Басқа бағалаушылар мен сертификаттау жөніндегі қызметкерлерге әзірлеушінің тестілеу тәсіліне қатысты орындалған тестілеу, БО тестіленетін пішін үйлесімдері көлемін және әзірлеушінің жалпы тестілеу нәтижелерін кейбір түсіну үшін мүмкіндік беретін жеткілікті нақтылаулар ұсыну мақсат болып табылады.

Әзірлеушінің енуді тестілеу жөніндегі ақпаратты, әдетте, БТЕ тиісті бөлімінен табуға болады, ол мынаны қамтиды:

а) БО тестіленетін пішін үйлесімдері. Енуді тестілеуге түсетін БО нақты пішін үйлесімдері;

б) Енуді тестілеуге түсетін ОФҚИ. Енуді тестілеу бағытталатын ОФҚИ және БО басқа интерфейстерінің қысқаша тізбесі;

в) Қызметтің осы ішкі түрі бойынша ұйғарым. Енуді тестілеу нәтижелері бойынша жалпы шешім.

Осы тізбе ешқандай жағдайда да БТЕ ұсынылуға тиіс бағалау барысында бағалаушы орындайтын енуді тестілеуге қатысты ақпарат типі туралы кейбір түсінік беру үшін ғана тағайындалған және жан-жақты болып табылмайды.

13.2.3.7.6 AVA_VAN.3-11 операциясы

Бағалаушы барлық тестілеу нәтижелерін өзінің алдын ала анықталған ортасында болатын БО төменгі шабуыл әлеуетіне ие бұзушыға орнықты болып табылатынын анықтау үшін зерттеуге тиіс. Егер нәтижелер өзінің алдын ала анықталған ортасында болатын БО орташа шабуыл әлеуетіне

қарағанда аз әлеуетке ие бұзушының пайдалануы үшін жарамды осалдығы болатынын көрсетсе, онда осы әрекет бойынша бағалаушы теріс қорытынды жасайды.

Нақты осалдықты пайдалану үшін қажетті шабуыл әлеуетін және осының салдарынан берілген ортада оның пайдаланылуын анықтау үшін нұсқаудың В қосымшасының В.4 тармағы пайдаланылуға тиіс. Орташаға қарағанда әлеуеті аз болатын бұзушының осалдықты пайдалана ма немесе жоқ па деген күдіктер болатын жағдайда қоспағанда, әр жолы шабуыл әлеуетін есептеп қажеті жоқ.

13.2.3.7.7 AVA_VAN.3-12 операциясы

Бағалаушы БТЕ әрбіреуі үшін нақтыланатын барлық пайдалануға жарамды осалдықтар мен қалдық осалдықтар туралы ақпаратты келтіруге тиіс:

- а) оның көзі (мысалы, бағалау бойынша әрекеттерді орындаған кезде белгілі болған, бағалаушыға белгілі, жарияланымда оқылды);
- б) ФҚТ жауап бермейтін;
- в) сипаттау;
- г) алдын ала анықталған ортада ол пайдаланыла ма, жоқ па (яғни, не пайдалану үшін жарамды немесе қалдық осалдық болып табылады);
- д) В қосымшасының В.2 және В.3 кестесін пайдалана отырып, осалдықты және тиісті мәндерді идентификациялауды орындау үшін қажетті уақыт көлемі, талдау деңгейі, БО білу деңгейі, мүмкіндіктер деңгейі және жабдық.

13.2.4 (AVA_VAN.4) қызметінің ішкі түрін бағалау

13.2.4.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты БО-ның өзінің алдын ала анықталған ортасында төменгі шабуыл әлеуеті болатын бұзушыға осалдықтың жарамды екенін анықтау.

13.2.4.2 Бастапқы деректер

- а) ҚТ;
- б) функционалдық сипаттізім;
- в) БО жобасы;
- г) қауіпсіздік құрылымын сипаттау;
- д) таңдалған ішжиынды жүзеге асыру;
- е) нұсқау;
- ж) тестілеу үшін жарамды БО;
- и) әлеуетті осалдықтарды идентификациялауды қамтамасыз ететін жалпы қолжетімді ақпарат.

Қызметтің осы ішкі түрі үшін қалған болжанатын бағалау куәліктері сенім пакетінде қамтылатын құрауыштарға тәуелді болады. Әрбір құрауышты қамтамасыз ететін куәліктер қызметтің осы ішкі түрінде бастапқы ретінде пайдаланылады.

Қызметтің осы ішкі түрі үшін айқын осалдықтарға қатысты ағымдағы ақпарат қосымша бастапқы материал болып табылады (мысалы, сәйкестікті растау жөніндегі органнан болатын).

13.2.4.3 Қолдану бойынша ескертулер

Жүйелік талдау әдісі куәліктерді құрылымдық талдау формасын қабылдайды. Осы әдіс бағалаушыдан өткізілетін талдаудың құрылымы мен формасын дәл сипаттауды талап етеді (яғни, мамандандырылған талдауға қарағанда, талдау жүргізілген тәсіл ертерек алдын ала анықталады). Әдіс талданатын және олардың қалай/не үшін талданатыны туралы деректер арқылы белгіленеді. Жүйелік талдауға арналған кезекті нұсқаулар В қосымшасында көрсетілген.

13.2.4.4 AVA_VAN.4.1Е әрекеті

БО тестілеу үшін жарамды болуға тиіс.

13.2.4.4.1 AVA_VAN.4-1 операциясы

Бағалаушы БО тестіленетін пішін үйлесімінің ҚТ анықталған бағалау пішін үйлесімімен келісілгені туралы қорытынды жасау үшін зерттеуге тиіс.

Бағалаушының тестілеу үшін пайдаланатын БО УК қызметінің ішкі түрінің мүмкіндіктерімен белгіленетін дәл сондай бірегей таңбалауы болуы және ҚТ кіріспе бөлімінде идентификациялануы керек.

ҚТ бағалануға тиіс бірнеше пішін үйлесімі анықталуға тиіс. БО ҚТ сәйкестігіне тестіленуге тиіс әр түрлі бірқатар аппараттық және программалық жүзеге асырулардан тұруы мүмкін.

Бағалаушы тестілеу ортасына қатысы болуы мүмкін БО қауіпсіздік ортасының аспектілеріне қатысты ҚТ сипатталған болжамдарды қарастыруы керек. ҚТ тестілеу ортасына қатысы болмайтын басқа да болжамдар болуы мүмкін. Мысалы, пайдаланушылардың рұқсатнамасына қатысты болжам тестілеу ортасына қатысты болмауы мүмкін, алайда, желіге қосылатын бірыңғай нүктеге қатысты болжам, әдетте, тестілеу ортасына қатысты болады.

Қандай да болмасын тестілеу құралдарын пайдаланған кезде (мысалы, өлшеуіштер, талдағыштар) осы құралдардың дұрыс калибрленуін қамтамасыз ету бағалаушының міндеті болады.

13.2.4.4.2 AVA_VAN.4-2 операциясы

Бағалаушы БО оның дұрыс орнатылғаны және белгілі күйінде болатыны туралы қорытынды жасау үшін зерттеуге тиіс.

Бағалаушының бірнеше тәсілдермен БО жай-күйі туралы қорытынды жасауға мүмкіндігі бар.

Мысалы, осының алдындағы (AGD_PRE.1) қызметінің ішкі түрін сәтті аяқтау тестіленетін БО егер тиісті түрде орнатылғанына және белгілі жағдайда екендігіне бағалаушы әлі сенімді болмаса, осы операцияны орындалған деп санауға мүмкіндік береді. Егер бұл бұлай болмаса, онда бағалаушыға жеткізілген нұсқауды ғана пайдалана отырып, БО орнату,

өндіру және іске қосу үшін әзірлеушінің процедураларын басшылыққа алу ұсынылады.

Егер бағалаушыға БО белгісіз жай-күйде болуы салдарынан орнату процедураларын орындауға тура келсе, онда сәтті аяқтаған кезде осы операция AGD_PRE.1-3 операциясын қанағаттандырған болар еді.

13.2.4.5 AVA_VAN.4.2E әрекеті

13.2.4.5.1 AVA_VAN.4-3 операциясы

Бағалаушы БО әлеуетті осалдықтарын идентификациялау үшін жалпы қолжетімді ақпарат көздерін зерттеуге тиіс.

Бағалаушы БО әлеуетті осалдықтарын идентификациялау үшін жалпы қолжетімді ақпаратты зерттеуге тиіс.

Бағалаушы, мысалы, бүкіләлемдік өрмекте қолжетімді ақпаратты пайдалана отырып зерттеуге тиіс жалпы қолжетімді ақпарат көздері болады, мыналарды қоса алғанда:

- а) мамандандырылған басылымдар (журналдар, кітаптар);
- б) ғылыми мақалалар.
- в) конференция хаттамалары.

Бағалаушы өзінің жалпы қолжетімді ақпаратты зерттеулерін жоғарыда аталған көздермен шектемеуге тиіс, кез келген маңызды қолжетімді ақпаратты зерттеуі қажет.

Бағалаушы ұсынылатын куәліктерді талдаумен қатар, кезекті іздеу үшін жалпы қолжетімді ақпарат көздеріндегі ақпаратты пайдаланатын болады. Бағалаушы қызықты саланы анықтаған кезде, бағалаушы қызықты салаға қатысты жалпы қолжетімді ақпаратты зерттеуге тиіс.

Оңай қол жеткізетін ақпаратқа қол жеткізу бұзушыға идентификациялауға көмектеседі және шабуылға ықпал етеді, осы бұзушының шабуыл әлеуетін арттыра отырып елеулі әрекет етеді. Ғаламтордағы осалдықтар және жетік бұзу құралдары туралы ақпаратқа қол жеткізу осы ақпараттың БО әлеуетті осалдығын идентификациялау және оларды пайдалану әрекетінде пайдаланатындығы туралы ықтималдықты арттырады.

Осындай ақпаратты уақытылы іздеу құралдары оны бағалаушы үшін оңай қол жететін етеді және жарияланған әлеуетті осалдықтарға және жақсы белгілі қарапайым шабуылдарға қарсы әрекетті анықтауға жоғары тиімді тәсілмен қол жеткізуге болады.

Жалпы қолжетімді ақпаратты іздеу типіне БО жататын өнімдермен айналысатын ресурстарда топталуға тиіс. Осындай іздеудің ұлғаюы мынадай факторлармен анықталуға тиіс: ОО типі, бағалаушының осындай типтегі БО жұмыс тәжірибесі, әлеуетті шабуылдар ықтималдығы және қолда бар куәліктер бойынша ADV деңгейі.

Бір әлеуетті осалдықты идентификациялау одан әрі зерттеуді қажет ететін басқа мүдделі саланы идентификациялауға әкелуі мүмкін қайталанатын идентификациялау процесі.

Бағалаушы әлеуетті осалдықтарды іздеуді аяқтаған кезде зерттелген куәліктерді көрсетеді. Аталған куәліктер таңдамасы бұзушының қолы жетуі мүмкін болып саналатын куәліктермен байланысты немесе бағалаушы ұсынатын қисынды негіздемелерге сәйкес бағалаушы анықтайтын көздерден алынуы мүмкін.

Алайда осындай іздеу түрі кезінде іздеу барысында алынған деректер нәтижесінде әдіс жүйелі дамуы мүмкін екені белгілі. Бағалаушы сондай-ақ әлеуетті осалдықтарға әкеледі деп саналатын мәселені одан әрі осы зерттеу әдісінде сипатталғанға алдын ала қолданылғанға қосымша барлық әрекетті көрсетеді және әлеуетті осалдықтарды іздеуді аяқтаған соң зерттелген куәліктерді атайды.

13.2.4.6 AVA_VAN.4.3E әрекеті

13.2.4.6.1 AVA_VAN.4-4 операциясы

Бағалаушы ҚТ әдіснамалық талдауын, құжаттама, нұсқаулар, функционалдық сипаттізім, БО жобасы, қауіпсіздік құрылымын сипаттау және жүзеге асыру жұмыстарын БО-дағы ықтимал әлеуетті осалдықтарды тану үшін жүргізуге тиіс.

Осалдықты жүйелік талдау жөніндегі жалпы нұсқаулар Б қосымшасында ұсынылған.

Әлеуетті осалдықты танудың осы әдісі реттелген және жоспарланған болуы керек. Мұндай жүйе қарау кезінде қолданылады. Бағалаушы осы ақпарат ескерілетін және жорамал жасалатын ерекше сипат жағдайында пайдаланылатын әдісті сипаттайды.

Бағалаушы ҚТ арқылы кемшілік жорамалы әдіснамасын пайдалануға, әзірлеу куәлігі (функционалдық сипаттізім, БО жобасы және жұмысты жүзеге асыру) мен жалпы нұсқауды талдауға тура келеді, ал содан соң БО-дағы осалдық туралы жорамал жасауы немесе жай ғана ойлануы қажет.

Ол БО әзірлемесінің әлеуетті ақауларын тану және кемшілігіне жорамал жасау үшін БО жеткізуден алынған БО жобасы мен жұмыстарының табыстарын және БО пайдаланудың нақты әдісіндегі әлеуетті қателіктерді пайдаланады.

Қауіпсіздік құрылымын сипаттау әзірлеушіге ол ОФҚ қауіпті объектілердің кедергісінен сақтайтыны және қауіпсіз ескертудің қолданылуын оңайлатудың алдын алатыны туралы хабарлайтындықтан, осалдықты талдауды береді. Сондықтан бағалаушы куәлікті талдау кезінде алынған ОФҚ қорғауына негізделеді, ал содан соң бұны ADV куәліктерінің басқа әзірлемелерінің тәжірибесінде дайындайды.

Осалдықты әдіснамалық зерттеуде пайдаланылатын әдіс бағалаушының әзірлемесін бағалау нәтижесінде танылатын барлық саланы және

куәліктердің жалпы нұсқауларын ескереді. Дегенмен, бағалаушы сондай-ақ ОФҚ қорғауы үзілетін жердегі мезетте болу үшін қауіпсіздік құрылымын талдаудың әрбір аспектісін ескеруге тиіс. Әдіснамалық талдау құрастырылымы тиісті ADV куәліктерінің мүддесін ұсынуға мүмкіндік беретін қауіпсіздік құрылымын сипаттау материалдары негізінде пайдалы болуы мүмкін. Талдау одан әрі ADV басқа барлық куәлік материалдарының ескерілетініне кепілдік берілген кезде әзірлене алады.

Куәлікті қарау кезінде мынадай жорамалдар жасалуы мүмкін:

а) сыртқы қауіпсіздік функцияларында шабуыл жасаушының қолы жететін қауіпсіздік функциялары үшін пішіні өзгерген қауіпсіздік функцияларын қарастыру;

б) бөлу сапасының төмендеуіне әкелуі мүмкін процесті бөлу, ішкі резервтің артықшылығы бойынша жорамал жасау сияқты қауіпсіздік құрылымын сипаттауда тартылатын негізгі қауіпсіздік механизмін қарау;

в) бақылауда толығымен болмайтын және ФҚТ қауіпсіздік механизмін үзу үшін шабуыл жасаушылардың пайдалануы мүмкін БО жұмыстарын жүзеге асыруда объектілерді тану.

Мысалға, бағалаушы қауіпсіздік функцияларының БО әлеуетті осалдық саласы болып табылатынын және куәліктің қауіпсіздік функцияларының барлық бөлшектерін зерделейтін іздеуге арналған әдісті анықтайтынын, әлеуетті осалдық бойынша жорамал жасайтынын және онда пайдаланылатын әдістерді түсіндіретінін таниды.

Бағалаушы қосымша бағалау қызметін жүргізу кезінде куәлікті қарау ішінде мүдделі саланы белгілейді. Мүдде салалары сондай-ақ еруге жүргізілетін тестілерді әзірлеу және орындау зерттеу мүддесінің немесе әлеуетті осалдықтың одан арғы салаларын анықтайтын жерде, атап айтқанда, AVA_VAN.4-7, AVA_VAN.4-5 және AVA_VAN.4-6 аталған құрауышымен бірге басқа операцияларды орындаған кезде байқалуы мүмкін.

Алайда аталған қатаң шаралар кезінде әзірлеу куәліктерінің ішжиыны мен жалпы нұсқауларды немесе олардың мазмұнын қарауға рұқсат етілмейді. Сипаттау әдісі осы әдіснамалық тәсілдің аяқталғанын дәлелдейді және әдісте сол жеткізулерде ұсынылатын барлық ақпараттың сақталатынына кепілдік береді.

Әлеуетті осалдықты танудың осы әдісі реттелуге және жоспарлануға тиіс; жүйені қарау кезінде қолдану қажет. Бағалаушы ескерілетін ақпарат және жасалатын жорамал ерекшелігін куәландыруды қарау жағдайында пайдаланылатын әдісті суреттеуге тиіс. Осы әдіс бағалау жұмыстарының басшылығымен келісілуге тиіс, басшылық сондай-ақ осалдықты талдауға арналған кез келген қосымша әдістер нақтылауын және бағалаушының қарауына қосымша ақпаратты ұсына алады. Әлеуетті осалдықты тану жүйесі алдын ала анықталғанымен, идентификациялау процесі бірнеше реттік болып

қалуы мүмкін, яғни әлеуетті осалдық өз кезегінде одан әрі зерттеуді қажет ететін басқа салаға әкелуі ықтимал.

ФҚТ жағдайында БО бағалаушының осалдықты тәуелсіз талдауы әрбір мынадай тақырыпқа сәйкес ерекше әлеуетті осалдықты ескеруге тиіс жердегі операциялық ортада қолданылады:

а) ерекше әлеуетті осалдық БО бағалау типі үшін релевантты, сондай-ақ бағалау басшылығы өзгертуі мүмкін;

б) жіберілген қате;

в) бұрмалау;

г) тура шабуылдар;

д) мониторинг;

е) теріс пайдалану.

б)-е) тармақтары Б қосымшасында түсіндіріледі.

Қауіпсіздік құрылымын сипаттауды ерекше әлеуетті осалдықтың жоғарыда аталған тармақтары бойынша ескеру керек. Әрбір әлеуетті осалдық ОФҚ және ұзу ОФҚ қорғауды жоюдың ықтимал жолдарын іздеу үшін қарастырылуға тиіс.

13.2.4.6.2 AVA_VAN.4-5 операциясы

Бағалаушы тестіге үміткер және БО операциялық ортасында қолданылатын БТЕ әлеуетті осалдықтарымен танылған жазбаны жүргізуі қажет.

Егер бағалаушы, мысалы, осы шараларды немесе АТ алдыңғы пайдалану немесе АТ емес әлеуетті осалдықты пайдалануды операциялық ортада байқаса, әлеуетті осалдықты одан әрі қарастыру қажет еместігі анықтала алады. Мысалы, БО өкілетті пайдаланушылардың жеке қол жеткізуін шектеу әлеуетті осалдықты ғана көрсетуі мүмкін.

Егер бағалаушы әлеуетті осалдықты операциялық ортада қолданылмайды деп шешсе, онда ол одан әрі қарастырудан әлеуетті осалдықты алып тастау себептерінің тізімін құрайды.

Басқаша жағдайда қарастырады.

Ену тестісінің қызметіне енгізу үшін пайдаланылатын БО әлеуетті осалдықтарының тізбесін БТЕ бағалаушылары ұсына алады.

13.2.4.7 AVA_VAN.4.4E әрекеті

13.2.4.7.1 AVA_VAN.4-6 операциясы

Бағалаушы осалдықты тәуелсіз іздеуге негізделген пенетрацияға арналған тестіні әзірлеуге тиіс.

Бағалаушы тестіні әзірлеген кезде, жалпы қолжетімді ақпарат ортасында танылған әлеуетті осалдықтың БО қабылдағыштығын анықтауы қажет. Үшінші тұлғадан (мысалы, Бағалау басшылығы) бағалау қызметінің кез келген басқа ақпаратымен бірге алынған кез келген ағымдағы ақпаратты бағалаушы ескеруге тиіс.

Бағалаушы қауіпсіздікті сипаттау құрылымын сипаттауды ескере отырып (AVA_VAN.4-3 жазылған сияқты), тестінің құрылым қасиеттерін растайтынын біледі. Егер АТЕ_DPT талаптары ТҚА қосылған болса, онда әзірлеуші тестісінің куәлігінде қауіпсіздік құрылымында сипатталатын кез келген нақты механизмнің дұрыс пайдаланылуын растайтын тесті болады. Алайда, аталған тестілердің көп саны өз мәнінде барлық қасиеттерді теріске шығаратын жағымсыз болып табылатындықтан, құрылым қасиеттерінің барлық аспектілеріне арналған тестінің болуы міндетті емес. Бағалаушы пенетрацияға арналған тестімен жұмыс жасай отырып, не функционалдық тестіде, не пенетрацияға арналған тестіде қауіпсіздік құрылымын сипаттайтын барлық аспектілерді тексеруге кепілдік береді.

Бағалаушыға әрбір бақылау үлгісінің нақты әлеуетті осалдығын тексеретін жерде бақылау үлгілерінің сериясын пайдалана отырып, пенетрацияға арналған тесті жүргізуге ыңғайлы болады.

Бағалаушының Орташа шабуылдар әлеуетінде көрсетілмеген әлеуетті осалдыққа тесті жүргізуі міндетті емес (қоғамдық домендегілерді қоса алғанда). Кейбір жағдайларда пайдаланар алдында тесті жүргізу қажет. Бағалаушы бағалау сараптамасы нәтижесінде Орташа шабуыл әлеуетінен тыс осалдықтың болатынын тапқан жерде, бұл осалдық элементінің қалдығы ретінде хабарланады.

Б.4 қосымшасында әлеуетті осалдықты пайдалану үшін қажетті ықтимал шабуылды анықтау жөніндегі нұсқауларды табуға болады.

Әлеуетті осалдық Орташа шабуыл әлеуеті болатын шабуылдаушы пайдаланатын жорамал бойынша және мақсаттардың бұзылуын көрсете отырып, БО қарсы бағытталған тізбені қамтитын артықшылығы болуы керек.

13.2.4.7.2 AVA_VAN.4-7. операциясы.

Бағалаушы әлеуетті осалдықтардың жан-жақты жазылған тізіміне негізделген басқа тестілердің бірнеше дүркіндігін пенетрациялауға арналған тесті құжаттамасын ұсынуға тиіс. Тесті құжаттамасында мыналар қамтылуға тиіс:

а) БО тексерілуге тиіс әлеуетті осалдыққа арналған идентификациялау парағы;

б) пенетрацияға арналған тесті жүргізу үшін қажетті барлық жабдықты қосуға және орнатуға арналған нұсқаулық;

в) барлық бастапқы жағдайды анықтау жөніндегі нұсқаулық;

г) ОФҚ қызметін күшейту жөніндегі нұсқаулық;

д) ОФҚ қызметін қадағалау жөніндегі нұсқаулық;

е) күтілетін нәтижені және қажетті талдауды сипаттау, оларды бір-бірімен салыстыру;

ж) тестіні қорытындылау және тексеруден кейінгі БО қажетті жағдайын анықтау жөніндегі нұсқаулық.

Бағалаушы тестіні қоғамдық домен және бағалау куәлігін іздеу кезінде танылған әлеуетті осалдық тізімі негізінде пенетрациялауға арналған тестіні дайындайды.

Бағалаушының Орташа шабуыл әлеуетіне әсер етуі қажеттіден басқа әлеуетті осалдықты пайдалану функциясын анықтауы екіталай. Дегенмен, бағалаушы бағалау сараптамасы нәтижесінде Орташа шабуыл әлеуетіне қарағанда барынша елеулі шабуылдаушының әлеуетті осалдықты пайдалануын байқай алады. Мұндай осалдықтар туралы БТЕ қалдық осалдықтар ретінде хабарлау керек.

Бағалаушы әлеуетті осалдықпен қатар, БО қабылдағыштығын тексерудің барынша ықтимал жолдарын анықтайды.

Бағалаушы, әсіресе, мынаны ескереді:

а) ОФҚІ қауіпсіздік функциялары немесе ОФҚ жұмысын ынталандыру және реакцияларды қадағалау үшін пайдаланылатын БО (ОФҚ қасиеттерін көрсетуге арналған ОФҚІ қарағанда, БО қауіпсіздік функцияларының пайдаланылуы мүмкін (ADV_ARC көрсетілгендей). БО қауіпсіздік функцияларының ОФҚ қасиеттерін тексеру құралын анықтайтынын және тестінің басты мақсаты болып табылмайтынын айтып кету керек);

б) тесті жүргізу үшін қажетті бастапқы шарттар (нақты объектілер немесе субъектілер, 3 қауіпсіздік атрибуттары);

в) ОФҚІ жұмысын ынталандыруға арналған сияқты, ОФҚІ қадағалауға арналған арнайы тестілеу жабдығы;

г) теориялық талдаулар іс жүзінде тексеруді ауыстыра ала ма, атап айтқанда, бірнеше реттік талпынысты көрсетуге арналған бастапқы тесті нәтижелері сыртқа таратылатын жерде.

Бағалаушы үшін бақылау үлгілері сериясын пайдалана отырып, тесті өткізгені барынша қолайлы, әр үлгі нақты әлеуетті осалдық үшін тағайындалатын болады.

Құжаттамада осы нақтылау деңгейінің мақсаты осы тәрізді тестілер өткізуде және балама нәтижелер алуда көмек болып табылады.

13.2.4.7.3 AVA_VAN.4-8 операциясы

Бағалаушы пенетрациялауға арналған тесті өткізуге тиіс.

Бағалаушы пенетрацияға арналған тестіні орындау үшін AVA_VAN.4-6 операциясы нәтижесінде алынған құжаттаманы негіз ретінде пайдаланады, бірақ тіпті бұл да оған арнайы қосымша тестіні орындауға кедергі жасамайды. Қажет болған жағдайда, бағалаушы пенетрацияға арналған тесті уақытында зерделенген ақпарат нәтижесінде арнайы тестілер әзірлейді және қажет болса, пенетрацияға арналған тесті құжаттамасында барлығын жазады. Осындай түрдегі тестілер күтпеген нәтижелер алу немесе қадағалау кезінде немесе бағалаушыға тестілерді жоспарлау уақытында ұсынылатын әлеуетті осалдықты зерттеу үшін қажет болуы ықтимал.

Егер пенетрацияға арналған тестіде әлеуетті осалдықтың болуы байқалмаса, бағалаушы оның өзіндік талдауларының дұрыс немесе бағалау жеткізулерінің қате немесе аяқталмағанын анықтауы керек.

Бағалаушының Әлеуетті шабуыл модераторында көрсетілгендерден басқа әлеуетті осалдықты пайдалану функциясын анықтауы екіталай. Дегенмен, бағалаушы бағалау сараптамасы нәтижесінде Әлеуетті шабуыл модераторына қарағанда барынша елеулі шабуылдаушының әлеуетті осалдықты пайдалануын байқай алады. Мұндай осалдық БТЕ қалдық болып саналады.

13.2.4.7.4 AVA_VAN.4-9 операциясы

Бағалаушы пенетрацияға арналған тестілердің нақты нәтижелер жазбасын жүргізуге тиіс. Нақты нәтижелердің белгілі бір нақтылауларының күтілетіннен ерекшеленетініне қарамастан (мысалы, тексеру уақыты және күні), қорытынды нәтиже бірдей болуы қажет. Кез келген күтпеген нәтиже зерделенуге тиіс. Бағалауға әсері тіркелген және негізделген болуға тиіс.

13.2.4.7.5 AVA_VAN.4-10 операциясы

Бағалаушы есепте БТЕ тесті әдісін, пішін үйлесімін, белгілемесі мен нәтижелеріне көңіл аудара отырып, пенетрацияға арналған тесті жұмыстарының нәтижелері туралы хабарлауға тиіс.

Осы ақпарат пенетрацияға арналған барлық тесті әдісін және қызметтің осы ішкі түріндегі жұмыстар нәтижесін беруге мүмкіндік береді. Осы ақпараттың мақсаты жұмыстар көшірмесін немесе дербес ену тестісінің нақты тесті нәтижелерін емес, бағалаушы жұмысының елеулі нәтиже көрсету болып табылады. Негізгі ой басқа бағалаушыларға немесе бағалау басшылығына пенетрация үшін таңдалған тесті әдісін, орындалатын тестілер санын, БО тестісінің пішін үйлесімін және тестінің қызметі бойынша толық нәтижені түсінуге мүмкіндік беретін жеткілікті толық ақпаратты қамтамасыз ету. БТЕ бөліміндегі ақпарат бағалаушының тесті жұмыстарының нәтижелері бойынша былай болады:

а) БО тестісінің пішін үйлесімі. Ену тестісімен тексерілген БО нақты пішін үйлесімдері;

б) пенетрацияға тексерілген ОФҚІ. Ену тестісінде тоғысталған ОФҚІ және БО қауіпсіздік функцияларының қысқаша тізбесі;

в) Қызметтің ішкі түріне арналған қорытынды. Қорытынды шешім және пенетрацияға арналған тесті нәтижелері.

Осы тізбе толық және БТЕ бағалау уақытындағы пенетрация тестісіне қатысты ұсынылуға тиіс ақпараттың нақты контекстін қамтамасыз ету ғана көзделген.

13.2.4.7.6 AVA_VAN.4-11 операциясы

Бағалаушы Орташа шабуыл әлеуетіне талпынысты өз ортасында БО орнықтылығын анықтау үшін, пенетрацияға арналған тестінің барлық нәтижесін қарауы керек. Егер нәтижелерде БО операциялық ортасында

Жоғары болмайтын шабуыл әлеуеті талпынысының пайдаланылатын осалдықтары байқалса, онда бағалаушының барлық әрекеті сәтсіз болады. Б.4 нұсқау нақты осалдықты пайдалану үшін қажетті әлеуетті шабуылды, сондай-ақ оның қажетті ортада пайдалану жарамдылығын анықтауға көмектеседі. Жоғары болмайтын шабуылға талпыныста пайдаланылатын осалдық күдігін қоспағанда, әрбір үлгіде шабуыл әлеуетін есептеудің қажеті жоқ.

13.2.4.7.7 AVA_VAN.4-12 операциясы

Бағалаушы БТЕ мыналар туралы нақтылауды көрсете отырып, барлық пайдаланылатын және қалдық осалдықтар туралы хабарлауға тиіс:

- а) дереккөз (мысалы, бағалау әдіснамасының қызметі бағалаушыға белгілі болды, жарияланымда оқылды);
- б) ФҚТ(s) сәйкессіздігі;
- в) сипаттау;
- г) операциялық ортада пайдаланылуы;
- д) уақыт мөлшері, сараптама деңгейі, БО туралы таным деңгейі, мүмкіндік деңгейі және осалдықты тануға арналған жабдық, сондай-ақ Б қосымшасының Б.2 және Б.3 кестелерін пайдаланудың тиісті маңыздылығы.

13.2.5 AVA_VAN.5 қызметінің ішкі түрін бағалау

Жалпы нұсқаулар болмайды; қызметтің осы ішкі түрінің нұсқауларына арналған сызбанұсқа талқылануға тиіс.

14 АСО класы: Құрылым

14.1 Кіріспе

Осы қызметтің мақсаты БО арналған ҚТ анықталғандай, қауіпсіздік әдісінде құрауыштардың топтастырылуын анықтау болып табылады. Бұған құрауыштар жобасымен қамтамасыз етілетін құрауыштар арасындағы қауіпсіздік функциясының және осалдыққа талдау жүргізу тестісі мен қарау арқылы қол жеткізуге болады.

14.2 Қолдануға арналған ескертпелер

Тәуелсіз құрауыштар орнықтылығының жиынтығын (ACO_REL) тәуелсіз құрауыш өзінің операциялық ортасында қауіпсіздігін қамтамасыз ету үшін барынша орнықты болатын жерде таниды (БО бағалауда негізгі құрауышпен орындалатын). Осы орнықтылық қауіпсіздік функциясының негізгі құрауышын ұсыну жағдайында танылады. Әзірлеу куәлігі (ACO_DEV) негізгі құрауышты бағалау кезінде негізгі құрауыштың қандай қауіпсіздік функциясын ескеретінін анықтайды.

Тәуелсіз құрауыштар орнықтылығының жиынтығының (ACO_REL) құрамдас құрауыштардың техникалық топтасу проблемасын бағыттау үшін қажетті басқа куәлікті қамтымайтынын айтып кету керек (мысалы,

операциялық жүйенің ОФҚ емес қауіпсіздік функцияларын сипаттау, топтастыру ережелері, т.с.с.). Бұл қауіпсіздік тағайындалымынан тыс функционалдық құрылым мәселесі.

БО құрамдас тестісінің бір бөлігі түрінде (ACO_CTT) бағалаушы құрамдас БО тексеруін БО қауіпсіздік функциясы және олардың тиісті жұмыстарын растауға арналған негізгі құрауыш деңгейінде орындайды. Таңдалған ішжиын БО пайдаланылған негізгі құрауыштың пішін үйлесімінің (пайдалану) өзгеруінің ықтимал әсерін ескеретін болады.

Әзірлеуші негізгі құрауыштың әрбір қауіпсіздік функциясына тексеру куәлігін береді (қамту аймағының талаптары негізгі құрауышты бағалау талаптарымен келісілген).

Құрылымды негіздеу (ACO_COR) бағалаушыдан негізгі құрауышта тиісті кепілдік беру шараларының қолданылғанын және өзінің бағалау пішін үйлесімінде негізгі құрауыштың пайдаланылғанын анықтауды талап етеді. Бұл ОФҚ негізгі құрауышында барлық қауіпсіздік іс-қимылының қамтылғанын анықтауды қамтиды. Құрылымды негіздеу талаптары (ACO_COR) расталған әрбір құрауышты көрсету куәлігінде кездесуі ықтимал.

Осы куәлік қауіпсіздік мақсаты және бағалау құрауышының қоғамдық хаттамасы түрінде болуы мүмкін (мысалы, сертификаттау хаттамасы).

Басқа жағынан, егер жоғарыда аталған құрауыштардың бірі расталмаса, онда бастапқы бағалау кезінде алынған куәліктің түпнұсқалылығы жөнінде күдік пайда болуы мүмкін. Немесе негізгі құрауыштың бұрын қамтылған аспектілеріне қосымша бағалау өткізілетін болады.

Аталған ақпарат Бағалау куәлігіне (ACO_DEV) енгізілетін болады.

Мысалға, бұл тәуелсіз құрауыш негізгі құрауышты бағалау қамтылатын БО көп болатын негізгі құрауыштың қауіпсіздік іс-қимылын қажет ететін жерде, Объектілер (Б.3 қосымшасын қараңыз, ИСО/МЭК 15408-3 АТ құрамдас объектілері арасындағы өзара іс-әрекет) арасындағы өзара әрекеттерде көрсетілетін жағдай болуы мүмкін. Бұл Тәуелсіз құрауыштар орнықтылығы (ACO_REL) және Әзірлеу куәліктері (ACO_DEV) жиынтығын қолдану көлемінде анықталатын болады. Мұндай жағдайда Құрылымды негіздеуге арналған куәлік (ACO_COR) негізгі құрауышты бағалаудың түпнұсқалылығын көрсететін болады. Бұған мыналарды қамтитын құралдар арқылы қол жеткізуге болады:

а) ОФҚ ұзартылған бөлігіндегі куәлікте тоғысталған негізгі құрауышты қайта бағалауды орындау;

б) ОФҚ ұзартылған бөлігінің ОФҚ басқа бөліктеріне әсер етпейтінін көрсету, сондай-ақ ОФҚ қажетті қауіпсіздік іс-қимыл куәлігін ұсыну.

14.3 Тиімді құрылым (ACO_COR)

14.3.1 (ACO_COR.1) қызметінің ішкі түрін бағалау

14.3.1.1 Енгізу

Осы функционалдық шағын топтың бағалау деректері болып табылады:

- а) құрамдас ҚТ;
- б) тиімді салу;
- в) сенім ақпараты;
- г) әзірлеу ақпараты;
- д) бірегей идентификатор.

14.3.1.2 ACO_COR.1.1Е әрекеті

Тиімді құрылым, кем дегенде, өз кезегінде тәуелсіз құрауыштың ОФҚ қажетті қолдауы сияқты соңғы қалыптасқан негізгі құрауышының функционалдық мүмкіндігімен қолдауға ие болған қаншама тәуелсіз құрауыштан соншама жоғары деңгейдегі сенім деңгейін көрсетеді.

14.3.1.2.1 ACO_COR.1-1 операциясы

Бағалаушы әзірлеу ақпаратында жан-жақты нақтыланбаған жорамалданған тәуелсіз құрауыштың қандай интерфейстерде болатынын анықтау үшін әзірлеу ақпараты мен сенім ақпараты арасындағы (бірігу аумақтары) сәйкестікті талдауды қарастырады.

Бағалаушының осы операцияда мынадай мақсаттары болады:

- а) жорамалданатын тәуелсіз құрауышқа қандай интерфейстерді орнату үшін қандай қолайлы сенім шарасы қолданылатынын;
- б) тәуелсіз құрауыш қолданылатын пакетте оны бағалау уақытында сол талаптар немесе иерархиялық жоғары тұратын сенім талаптары болатын негізгі құрауышты бағалау уақытындағы сияқты негізгі құрауышқа қолданылатын пакетті анықтау.

Бағалаушы сенім ақпаратында идентификацияланатын және әзірлеу ақпаратында қарастырылмайтын интерфейстерді анықтауға көмек беру үшін әзірлеу деректері (ACO_DEV) мысалы, ACO_DEV.1-2, ACO_DEV.2-4, ACO_DEV.3-6) пайда болған уақытта жетілдірілетін әзірлеу ақпаратында байқалатын сәйкестікті пайдалана алады.

Бағалаушы сенім ақпаратында сипатталған, бірақ әзірлеу ақпаратында болмайтын ЖІҚ (жүйенің істен шығу қарқындылығы) интерфейстерінің күшеюін жазып алады. Бұл одан әрі сенім талап етілетін негізгі құрауыш бөлігін анықтауға көмектесе отырып, ACO_COR.1-3 операциясына енгізуді қамтамасыз етеді.

Егер негізгі және тәуелді құрауыш та бір ғана сенім пакетіне қарсы бағаланған болса, онда негізгі құрауышты бағалау ішіндегі бөліктердегі сенім деңгейі, кем дегенде, әдеттегі тәуелді құрауышқа қарағанда сонша жоғары. Егер, алайда, құрауыштарды бағалау уақытында құрауышқа қолданылған сенім пакеттері ерекшеленетін болса, онда бағалаушының негізгі құрауышқа қолданылған сенім талаптарының тәуелді құрауышқа қолданылған сенім талаптарынан иерархиялық жоғары екенін анықтауы қажет.

14.3.1.2.2 ACO_COR.1-2 операциясы

Бағалаушы негізгі құрауышқа қосылған және негізгі құрауышты бағалау уақытында тәуелді ОФҚ жорамалданатын интерфейстерді талдауды анықтау үшін тиімді құрылымды қарастырады.

Қауіпсіздік жөніндегі тапсырма, қоғамдық бағалау құрауышының есебі (мысалы, куәлік туралы есеп) және негізгі құрауышты басқару жөніндегі құжаттар олардың барлығы негізгі құрауыш шекарасы шегінде ақпаратпен қамтамасыз етеді. ҚТ бағалаушыға интерфейстің бағалау аумағы шегіндегі өнім бөлігіне жататынын анықтауға мүмкіндік беретін бағалаудың құрамдас объектілерінің қисынды аумағы мен шекараларының бөліктерімен қамтамасыз етеді. Нұсқау жөніндегі құжаттар құрамдас БО барлық интерфейстерін пайдалану бөлшектерімен қамтамасыз етеді. Сондай-ақ нұсқау жөніндегі құжаттар бағалау саласында және одан тыс болатын өнімдегі интерфейстер бөлшектерін қамтуы мүмкін, кез келген мұндай интерфейс не ҚТ ақпаратты қадағалау арқылы, не бағалау пішін үйлесімімен байланысты басқару бөлігі арқылы танылуға тиіс. Қоғамдық бағалау есебі сондай-ақ қажетті атрибут болып табылатын құрамдас БО пайдалануға қойылатын кез келген қосымша шектеуді қамтамасыз етуі мүмкін.

Сондықтан осы енгізулердің құрамдастыруы бағалаушыға тиімді құрылымда сипатталған сонымен байланысты қажетті сенім интерфейсі болатынын немесе одан әрі сену міндетті екенін анықтауға мүмкіндік береді. Бағалаушы ACO_COR.1-3 уақытында талқылау үшін қажетті қосымша уақыт берілетін негізгі құрауыш интерфейстерін жазады.

14.3.1.2.3 ACO_COR.1-3 операциясы

Бағалаушы тиімді құрылымды негізгі құрауышқа қажетті сенім шараларының қалай қолданылатынын анықтау үшін қарастырады. Бағалау ұйғарымы және нәтижесінде алынатын сенім сол бөліктермен қамтамасыз ете отырып, негізгі құрауыш үшін қайта пайдаланылуы ықтимал; құрамдас БО жүйелі пайдаланылады.

Құрауышқа арналған қажетті шаралар және сенім шараларын қолдану үшін әлі қажетті бөліктердің қолданылғанын анықтау үшін, бағалаушы ACO_DEV.*.2E қызметінің өнімін және ACO_COR.1-1 және ACO_COR.1-2 операцияларын пайдалануға тиіс:

а) Сенім ақпаратында (Тәуелді құрауыш сенімі (ACO_REL)) анықталған, бірақ әзірлеу ақпаратында (Даму деректері (ACO_DEV)) талқыланбайтын интерфейстер, қосымша ақпарат талап етіледі (ACO_COR.1-1 идентификацияланған).

б) Бағалау объектісінде негізгі құрауышпен (Даму деректерімен жабдықталған ақпарат арасындағы айырмашылық (ACO_DEV) үйлесімсіз және Тәуелді құрауыш сенімінде (ACO_REL)) пайдаланылған интерфейстер, осы айырмашылықтардың әсері негіздеуді талап етеді. (ACO_DEV.*.2E. идентификацияланған)

в) Алдын ала сенім иеленбеген тиімді құрылымда анықталған интерфейстер, қосымша ақпарат талап етіледі. (ACO_COR.1-1. идентификацияланған)

г) Сенім ақпаратына, тиімді құрылымға және әзірлеу ақпаратына сәйкес сипатталатын интерфейстер, негізгі құрауышты бағалау нәтижелері қайта пайдаланылатындықтан, одан әрі ешқандай әрекеттер талап етілмейді.

Сенім ақпаратын пайдалану үшін қолданылатын, бірақ әзірлеу ақпаратына қосылмаған негізгі құрауыш интерфейстері одан әрі сенім талап етілетін жерде негізгі құрауыштың үлесін көрсетеді.

Интерфейстер негізгі құрауышқа кіретін нүктені анықтайды.

Бағалаушы әзірлеу ақпаратында және негізгі құрауышты бағалаумен байланысты тәсіл бойынша Бағалау объектісінің пайдалануындағы сенім ақпаратында болатын интерфейстерді анықтайды. Интерфейсті пайдалану әдісі екі құрауышта және Бағалау объектісінде интерфейсті пайдалану бірізділігін анықтау үшін, Даму деректерінің (ACO_DEV) қызметі уақытында қарастырылатын болады. Негізгі құрауыш пен Бағалау объектісінің пішін үйлесімдерінің байланысын анықтау қалған әрекет болып табылады. Бағалаушы осыны анықтау үшін, олардың байланыстылығына кепілдік беру үшін әрқайсысының нұсқауы бойынша құжаттарды қарастырады (нұсқау бойынша құжаттардың байланыстылығына қатысты нұсқауды қараңыз. Құжаттамадағы кез келген алдағы уақытта ықтимал ақауларды анықтауға арналған бағалаумен талданады.

Әзірлеу ақпаратында және сенім ақпаратында интерфейстер мақсатқа сәйкес, ал нұсқаудың негізгі құрауышпен және Бағалау объектісімен байланыстылығы сипатталған, қажетті сенім деңгейі өткізілген болып саналады.

Негізгі құрауышта алынған сенім және қарама-қайшылық анықталған жердегі үлгілерде бағалаушы өткізген талдау және бағалау объектісі арқылы алынған деректер арасындағы тізбектілікті анықтау:

а) әзірлеу.

Сенім ақпараты негізгі құрауышпен іріктелген тәуелді құрауыштағы интерфейстерді анықтайды. Егер сенім ақпаратында анықталған интерфейс әзірлеу ақпаратында анықталмаған болса, онда тиімді құрылым негізгі құрауыштың қажетті интерфейстермен қалай қамтамасыз ететіні туралы ережені ұсынады.

Егер сенім ақпаратында анықталған интерфейс әзірлеу ақпаратында анықталса, бірақ сипаттаулар арасында қарама-қайшылық болса, онда одан әрі талдау талап етіледі. Бағалаушы негізгі құрауышты және құрамдас Бағалау объектісін бағалауда қарастырылатын сияқты негізгі құрауышты пайдаланудағы айырмашылықты анықтайды. Бағалаушы интерфейсін тексеруді орындау жоспарын жасайды (құрамдас Бағалау объектісін сынау уақытында (ACO_CTT)).

Құрамдас Бағалау объектісінде пайдаланылған негізгі және тәуелді құрауыштар патчиінің мәртебесі құрауыштар патчиінің мәртебесімен оларды бағалау уақытында салыстырылуға тиіс. Егер құрауыштарға кез келген патчи қолданылған болса, онда тиімді құрылымда ЖІҚ бағалау құрауышының әлеуетті әсерін қоса алғанда, осы патчилердің бөлшектері болуға тиіс. Бағалаушы алынған өзгерістер бөлшектерін қарауға және ЖІҚ құрауышына өзгерістің әлеуетті әсерінің дұрыстығын тексеруге тиіс. Бағалаушы содан соң сынақ барысында патчимен жасалған өзгерістерді тексеру қажеттігін қарастырады және сынақ жүргізу қажеттігін белгілейді. Тексерудің бағалау құрауышы үшін бағалаушы/әзірлеушінің сынақты орындауды қайта қолдану формасын қабылдауы мүмкін немесе ол бағалаушы үшін құрауыш өзгерістерін растаудың жаңа тексерістерін әзірлеу үшін қажет болуы мүмкін.

Егер жеке құрауыштардың кез келгені бағалау құрауышын аяқтаудан бастап әрекеттер қарқынының сенім мәні болса, онда бағалаушы құрамдас бағалау объектісі үшін өткізілген тәуелсіз осал талдау уақытындағы әрекеттер қарқынының сенімінде бағаланған өзгерістерді қарастырады (Осал талдауды құрастыру (ACO_VUL)).

б) нұсқау.

Құрамдас бағалау объектісіне арналған нұсқау жеке құрауыштарға елеулі айналымды іске асырады. Нұсқау минимумына, әсіресе, құрамдас бағалау объектісін орнату уақытында тәуелді және негізгі құрауыштарға нұсқауды қолданғанда тәуелділіктерді кез келген реттеуді қажетті анықтауға жатады.

Құрамдас бағалау объектісіне арналған нұсқауға Дайындау процедураларының топтарын (AGD_PRE) және пайдаланушының операциялық нұсқауын (AGD_OPE) қолдануға қосымша құрауыштарға арналған нұсқаулар мен құрамдас Бағалау объектісі арасындағы байланысты талдау, кез келген ауытқуды анықтау қажет.

Егер құрамдас Бағалау объектісінің нұсқауы негізгі және тәуелді құрауыштар нұсқауынан тыс бағытталатын болса, онда тізбектілікті талқылау құрауыштардың әрқайсысы үшін қолданылған нұсқау бойынша құжаттар арасындағы тізбектілікпен салыстыру бойынша шектелген болып табылады (яғни, негізгі және тәуелді құрауыштар нұсқаулары арасында). Дегенмен, егер құрамдас Бағалау объектісі үшін қолданылатын қосымша нұсқау құрауыштар үшін де пайдаланылатын болса, онда сондай-ақ құрауыштарға арналған нұсқау бойынша құжаттама мен құрамдас Бағалау объектісіне арналған нұсқау бойынша құжаттама арасында байланыстылық болатындықтан, үлкен талдау талап етіледі.

Бұл жағдайда байланыстылық не нұсқаудың бірдей екенін, не болашақта функционалдық/кепілдік құрауыштарды анықтауға арналған осыған ұқсас тәсілмен топтастырылатын дербес құрауыштардың операциясына қосымша қысым беретінін білдіреді.

Бағалаушы қолжетімді ақпаратпен (даму деректеріне (ACO_DEV) арналған енгізу ретінде пайдаланылатын немесе жоғарыда талқыланған даму тәсілдері) бағалау құрауышында көрсетілген негізгі құрауыштың пішін үйлесімінен болатын барлық ықтимал ауытқуларды анықтай алады. Дегенмен, Сенімді бағалаудың жоғары деңгейі үшін (негізгі құрауыштың нақтылы талаптарын бағалау объектісінің жоспарына қосуда (ADV_TDS)) бұл негізгі құрауыштың нақтылы жоспарланған абстракциялары құрамдас бағалау объектісін әзірлеу ақпаратының бөлігі ретінде берілетінін есептемегенде мүмкін, нұсқауға енгізілетін өзгерістердің ықтимал әсері ішкі сала белгісіз болғандықтан, толығымен анықталуы мүмкін емес. Бұндай жағдайда бағалаушы талдаудың қалдық тәуекелін баяндайды.

Осы қалдық тәуекелде құрамдас Бағалау объектісіне арналған кез келген қоғамдық бағалау хабарламалары болады.

Бағалаушы бұл алауыздыққа бағалаушының тәуелсіз сынағын қолданысқа енгізу жөніндегі нұсқауда назар аударады (Құрамдас Бағалау объектісін сынау (ACO_CTT)).

Құрамдас Бағалау объектісіне арналған нұсқау құрауыштарға арналған нұсқауға, әсіресе, тәуелді құрауыштың орнату операциясына қатысы бойынша негізгі құрауыштың белгілеу операцияларын орнату және реттеу жағдайында қосылуы мүмкін. Дербес құрауыштардың белгілеу операцияларының тәртібі өзгермеуге тиіс, алайда олар кезектесе алады. Бағалаушы бұл нұсқауды құрауыштарды бағалау уақытында оның AGD_PRE әрекеті талаптарымен жанасуына кепілдік беру үшін қарастырады.

Бұл сенім ақпараты негізгі құрауыш интерфейстері тәуелді құрауыш сенім туралы ақпаратта анықталады деп жорамалданатын негізгі құрауыштың ОФҚ интерфейстері ретінде анықталғандарға қосымша сенім ақпараты анықтайтын жағдай болуы ықтимал. Нұсқау үшін негізгі құрауыштың осындай кез келген қосымша интерфейстерді пайдалануын қамтамасыз ету қажет болуы мүмкін. Құрамдас Бағалау объектісінің қамтамасыз етілген тұтынушысы негізгі құрауыш нұсқауы жөніндегі құжаттаманы алу үшін қажет, содан кейін негізгі құрауыштың AGD_PRE және AGD_OPE ұйғарымдарының шешімдері негізгі құрауышта қарастырылатын сол интерфейстер үшін қайта пайдаланылуы мүмкін.

Алайда, тәуелді құрауыш жорамалданатын қосымша интерфейстер үшін бағалаушы негізгі құрауыштың нұсқауы жөніндегі құжаттаманың негізгі құрауышты бағалауда қолданылғандай, AGD_PRE және AGD_OPE талаптарымен шектесетінін анықтауға тиіс.

Негізгі құрауышты бағалау уақытында қарастырылатын интерфейстер үшін және сенім ендігі күшейтілгендер үшін де бағалаушы құрамдас Бағалау объектісінің әрбір интерфейсін пайдалану жөніндегі нұсқаудың негізгі құрауыш нұсқауымен байланысты екендігіне көзін жеткізуге тиіс. Бағалаушы құрамдас бағалау объектісі нұсқауының негізгі құрауыш нұсқауымен

байланысты екенін анықтау үшін, құрамдас бағалау объектісінің де және негізгі құрауыштың да нұсқауларында әрбір интерфейсті бейнелеуге тиіс. Бағалаушы содан соң байланыстылығын анықтау үшін нұсқауды салыстыруы қажет.

Негізгі құрауыш нұсқауымен байланысты болатын сияқты қарастырылатын құрамдас Бағалау объектісінің нұсқауында қамтамасыз етілген қосымша байланыстар үлгілері болып табылады (құрауышқа арналған нұсқау қосымша байланыстылық ретінде негізделген құрамдас Бағалау объектісінің нұсқауының үлгісінен кейін беріледі):

Құрауыш: Парольдің ұзындығы алфавиттік және сандық белгілерді қоса алғанда, 8 белгіден кем болмауы керек.

Құрамдас БО: Парольдің ұзындығы алфавиттік және сандық белгілерді қоса алғанда, 10 белгіден және ең аз дегенде мынадай арнайы белгілер жиынтығынан кем болмауы керек: () { } ^ < > - _

ЕСКЕРТПЕ: Егер осындай және одан жоғары ұзындыққа бағалауды күшейту үшін (парольдің бұзылу ықтималдығын ескере отырып) қол жеткізілген болса, құрамдас БО арналған алфавиттік және сандық белгілерді қосуға арналған тапсырманы жоя отырып, сол уақытта парольдің ұзындығын [бүтін сан > 8] белгіге арттыру ғана қабылдауға лайық болады.

Құрауыш: Келесі баптаулар тіркеу баптауларында жарамсыз: WWW Баспа қызметтері және Баяндамашының ICDB қызметтері.

Құрамдас БО: Келесі баптаулар тіркеу баптауларында жарамсыз: Баспа қызметтері, Баяндамашының ICDB қызметтері, Процедураларды қашықтан шақыру хаттамасы (RPC), Локатор және Процедураларды шақыру (RPC) қызметтері.

Құрауыш: Есептік тіркеу журналында болатын мынадай атрибуттарды таңдап аласыз: оқиға күні, уақыты, типі, идентификатор және сәттілік/жеңіліс мәні.

Құрамдас БО: Есептік тіркеу журналында болатын мынадай атрибуттарды таңдап аласыз: оқиға күні, уақыты, типі, идентификатор және сәттілік/жеңіліс мәні, оқиға туралы хабарлама және командалардың тізбектік процесі.

Егер құрамдас бағалау объектісінің нұсқауы негізгі құрауыш нұсқауынан ауытқитын болса (бірақ нақтыланбайды), онда бағалаушы нұсқауды өзгертудің ықтимал тәуекелін бағалайды. Бағалаушы құрамдас Бағалау объектісінің ЖІҚ арналған нұсқауындағы өзгерістердің ықтимал әсерін анықтау үшін қолжетімді ақпаратты пайдаланады (қоғамдық бағалау есебіндегі негізгі құрауыштың қоғамдық доменде қолданылатын архитектуралық сипаттауын қоса алғанда (мысалы, куәлік туралы есепте), нұсқау жөніндегі құжаттамамен бірге нұсқаудың қалдық контексті).

Егер тәуелді құрауышты бағалау барысында сынау қондырғысы тәуелді

құрауышты қамтитын талаптарды қанағаттандыру үшін негізгі құрауышты пайдаланса, онда құрамдас БО арналған осы операция қанағаттанарлық болып саналады. Егер негізгі құрауыш тәуелді құрауышты бағалау уақытында AGD_PRE.1-3 операциясын қанағаттандыру мақсатында пайдаланылмаса, онда бағалаушы AGD_PRE.1-3 көрсетілген нұсқауға сәйкес, құрамдас БО әзірлеу үшін құрамдас БО негізделген пайдаланушы процедураларын қолданады. Бұл бағалаушыға құрамдас БО дайындалған нұсқауының құрамдас БО және қауіпсіздікті қамтитын операциялық талаптарды даярлау үшін жеткілікті болып табылатынын анықтауға мүмкіндік береді.

в) өмірлік цикл.

Жеткізу

Егер құрамдас БО жеткізу үшін пайдаланылатын түрлі жеткізу механизмдері болатын болса (яғни, құрауыштар тұтынушыға құрауыштарды бағалау уақытында анықталған және бағаланған қауіпсіз жеткізу процедурасына сәйкес жеткізілмейді), онда құрамдас БО жеткізу процедурасы құрауыштарды бағалау уақытында қолданылған Жеткізу талаптарына (ALC_DEL) қарсы бағалауды талап етеді.

Құрамдас БО кешенді өнім түрінде жеткізілуі мүмкін немесе жеке жеткізілуі үшін құрауышты талап етуі мүмкін.

Егер құрауыштар жеке жеткізілетін болса, онда негізгі және тәуелді құрауыштарды жеткізу нәтижелері қайта пайдаланылады. Негізгі құрауышты жеткізу мұндайда негізгі құрауыштың нұсқауы жөніндегі құжаттамада сипатталған сияқты, пайдаланушының жауапкершілігі болып табылатын жеткізу аспектілерін тексере және аталған нұсқауды пайдалана отырып, тәуелді құрауышты бағалаушының сынама орнатуы көлемінде тексеріледі.

Егер құрамдас БО қандай да бір жаңа объекті сияқты жеткізілсе, онда осы объектіні жеткізу әдісі құрамдас БО бағалау әрекеттерінде қарастырылуы керек.

Құрамдас БО пункттерін жеткізу процедураларын бағалау кез келген қосымша тармақтардың (яғни, құрамдас БО нұсқауы бойынша қосымша құжаттар) жеткізу процедураларында қаралатынына кепілдік бере отырып, кез келген БО құжаты [құрауыш] сияқты Жеткізу әдіснамасына (ALC_DEL) сәйкес орындалады.

УК жарамдылығы

Құрамдас БО бірегей идентификациялау Функционалдық бағалау ішкі тобын (ALC_CMC.1) қолдану кезеңінде негізделеді және құрамдас БО қамтитын тармақтар Функционалдық бағалау ішкі тобын (ALC_CMC.2) қолдану кезеңінде қарастырылады.

Сондай-ақ қосымша нұсқау құрамдас БО үшін дайындалуы мүмкін, осы нұсқауды бірегей идентификациялау (Функционалдық бағалау ішкі тобын (ALC_CMC.1) қолдану кезеңінде құрамдас БО бірегей идентификациялау

бөлігі ретінде негізделген) нұсқаудың дәлелденген бақылауымен қарастырылады.

ALC класының қалған ұйғарымдары (жоғарыда дәлелденбеген): Өмірлік циклді қолдауды көрсету құрамдас БО топтастыру уақытында одан әрі ешқандай дамыту орындалмайтын болғандықтан, негізгі құрауышты бағалаудан қайта пайдаланылуы ықтимал.

Топтастыру не тұтынушы тарапынан, не әзірлеуші жақтан тәуелді құрауыштың кешенді өнімі ретінде жеткізілгендіктен, дамыту қауіпсіздігін ешқандай қосымша дәлелдеу болмайды. Тұтынушы тарапынан болатын бақылау ИСО/МЭК 15408 дәлелдеуінен тыс болады. Егер топтастыру барлық құрауыштар құрамдас БО пішін үйлесімдері тармақтары сияқты дәлелденетін жағында болатын болса, қосымша талаптар немесе нұсқаулардың қажеті жоқ және сондықтан кез келген жағдайда әзірлеуші қолданатын тәуелді құрауыш деректері қарастырылатын болады.

Топтастыру уақытында игерілген тәсілдер мен техника әзірлеуші қолданатын тәуелді құрауыш деректерімен қарастырылатын болады. Негізгі құрауыштың кез келген маңызды тәсілдері/техникасы негізгі құрауышты бағалау уақытында қаралатын болады. Мысалы, егер негізгі құрауыш бастапқы код ретінде жеткізілсе және тұтынушының құрастыруын талап етсе (мысалы, топтастыруды орындайтын тәуелді құрауыш әзірлеушісі), онда құрастырғыш құрастырушы негізгі құрауышты бағалау уақытында тиісті аргументке параллель көрсетілетін және бағаланатын болады.

Тармақтарды бұдан әрі дамыту болмайтындықтан, құрауыш БО қолданылатын өмірлік циклді анықтаудың қажеті жоқ.

Құрауыштың ақауларын түзету нәтижелері құрамдас БО үшін қолданылмайды. Егер ақауды түзету құрамдас БО сенім пакетіне кіретін болса, онда ақауды түзету талаптары (ALC_FLR) құрамдас БО бағалау көлемінде қолданылады (кез келген арттыру үшін).

г) тексеріс.

Құрамдас БО АТЕ класын басқару уақытында сыналатын болады: Тәуелді құрауышты тексеру үшін пайдаланылатын пішін үйлесімі кезінде тәуелді құрауышты бағалауды тексеру әрекеті операциялық шеңберде Ақпараттық технология талаптарын қанағаттандыру үшін негізгі құрауышты қамтуы керек. Егер негізгі құрауыш тәуелді құрауышты бағалауды тексеру үшін пайдаланылмаса немесе құрауыштың пішім үйлесімі оларды бағалау пішін үйлесімінен ерекшеленсе, онда тәуелді құрауышты бағалау үшін негізделген тексеріс әзірлеушісі АТЕ класын қанағаттандырады. Талап етілетін тексерістер құрамдас бағалау объектісі үшін қайталанатын болады.

14.4 Әзірleme деректері (ACO_DEV)

14.4.1 (ACO_DEV.1) қызметінің ішкі түрін бағалау

14.4.1.1 Мақсаты

Осы функционалдық ішкі топтың мақсаты қолайлы қауіпсіздік тиімділігінің тәуелді құрауышты қолдауда негізгі құрауышпен қолданылатынын анықтау болып табылады. Бұған тәуелді құрауышпен қолданылатын сенім ақпаратында көрсетілетін интерфейстермен олардың байланысын анықтау үшін негізгі құрауыш интерфейстерін зерттеу арқылы қол жеткізілетін болады.

Негізгі құрауыштар интерфейстерін сипаттау Функционалдық ішкі топты бағалаумен (ADV_FSP.2) болатын жан-жақты байланыс деңгейінде, сондай-ақ Функционалдық ішкі топты бағалауды (ACO_DEV.1) қанағаттандыру үшін талап етілетін барлық аспектілерге қолданылады, Функционалдық ішкі топты бағалау (ADV_FSP.2) үшін талап етіледі; интерфейс анықталды және қалған бөлшекті, интерфейс сипаттізімдерін сипаттайтын мақсат негізгі құрауышты пайдаланғанда қайталануы мүмкін.

14.4.1.2 Енгізу

Осы функционалдық ішкі топтың бағалау деректері болып табылады:

- а) құрамдас ҚТ;
- б) әзірлеу ақпараты;
- в) сенім ақпараты.

14.4.1.3 ACO_DEV.1.1E әрекеті

Әзірлеу ақпараты құрамдас БО пайдаланылатын негізгі құрауыштың әрбір интерфейсін мақсатын суреттейді.

14.4.1.3.1 ACO_DEV.1-1 операциясы

Бағалаушы әзірлеу ақпаратын оның әрбір интерфейсін мақсатын сипаттайтынын анықтау үшін қарастырады.

Негізгі құрауыш тәуелді ОФҚ қамтамасыз етуде тәуелді құрауышпен болатын өзара әрекетті қолдауда интерфейстерді қамтамасыз етеді. Әрбір интерфейсін мақсаты – бұл оны БО жоспарындағы (Функционалдық ішкі топты бағалау (ADV_TDS.1)) ішкі жүйелер арасында қолданылатын сияқты ОФҚ тәуелді құрауышы интерфейстерін сипаттау сияқты деңгейде сипаттау. Осы сипаттау ОФҚ тәуелді құрауышы талап ететін қызметтерді қамтамасыз ететін негізгі құрауыш ретінде оқырманның оны түсінуі үшін қолданылады.

Бұл операция негізгі құрауыштың ОФҚ Интерфейстері болып табылатын интерфейстер үшін негізгі құрауыштың функционалдық сипаттізімін қамтамасыз етумен қанағаттандырылуы мүмкін.

Әзірлеу ақпараты тәуелді құрауыштың ОФҚ қолдауда құрамдас БО пайдаланылатын интерфейстер мен тәуелді құрауыштар арасындағы сәйкестікті көрсетеді.

14.4.1.3.2 ACO_DEV.1-2 операциясы

Бағалаушы әзірлеу ақпаратын тәуелді құрауыш дұрыс болып

болжанатын интерфейстер мен негізгі құрауыш интерфейстері арасындағы сәйкестікті анықтау үшін қарастырады.

Тәуелді құрауыш дұрыс болып болжанатын интерфейстер мен негізгі құрауыш интерфейстері арасындағы сәйкестік матрица немесе кесте формасын қабылдауы мүмкін. Тәуелді құрауыш болжанатын интерфейстер сенім ақпаратында анықталады (Тәуелді құрауыш сенімін (ACO_REL) көрсету барысында қарастырылған сияқты).

Осы әрекет барысында тәуелді құрауыш болжануы мүмкін интерфейстердің қолданылу аясының толықтығын анықтаудың ешқандай талабы жоқ, тек сәйкестік дұрыс және әрқашан мүмкін тәуелді құрауышпен талап етілетін интерфейстермен көрсетілетін негізгі құрауышының интерфейстерінің дұрыстығына кепілдік беріледі.

Қолданылу саласының толықтығы Тиімді құрылым (ACO_COR) қолданысында қарастырылады.

14.4.1.4 ACO_DEV.1.2E әрекеті

14.4.1.4.1 ACO_DEV.1-3 операциясы

Бағалаушы әзірлеу ақпараты мен сенім ақпаратын интерфейстердің жүйелі сипатталғанын анықтау үшін қарастырады.

Бағалаушының осы операциядағы мақсаты негізгі құрауышқа арналған әзірлеу ақпаратында және тәуелді құрауышқа арналған сенім ақпаратында сипатталатын интерфейстердің жүйелі ұсынылғанын анықтау болып табылады.

14.4.2 (ACO_DEV.2) қызметінің ішкі түрін бағалау

14.4.2.1 Мақсаты

Осы функционалдық ішкі топтың мақсаты қолайлы функционалдық қауіпсіздіктің тәуелді құрауышты қолдауда негізгі құрауышпен қамтамасыз етілгенін анықтау болып табылады. Бұған интерфейстерді зерттеу және тәуелді құрауышпен қолданылатын сенім ақпаратында көрсетілген интерфейстермен оның байланыстылығын анықтау үшін қауіпсіз бейнесімен байланысты негізгі құрауыш әрекеті арқылы қол жеткізілетін болады.

14.4.2.2 Енгізу

Осы функционалдық ішкі топтың бағалау деректері болып табылады:

- а) құрамдас ҚТ;
- б) әзірлеу ақпараты;
- в) сенім ақпараты.

14.4.2.3 ACO_DEV.2.1E әрекеті

Әзірлеу жөніндегі ақпарат құрамдас БО базалық құрауыштың әрбір функциясының мақсаты мен әдісін сипаттауға тиіс.

14.4.2.3.1 ACO_DEV.2-1 операциясы

Бағалаушы әзірлеу жөніндегі ақпаратты онда әрбір функцияның мақсаты дәл сипатталғанын анықтау үшін тексеруге тиіс.

Базалық құрауыш тәуелді ОФҚ қамтамасыз етуде тәуелді құрауыштармен өзара әрекетті қолдауға арналған қауіпсіздік функцияларын ұсынады. Әрбір функцияның мақсаты қауіпсіздік функциясын БО жобасындағы ішкі жүйелер арасындағы деңгейдегі тәуелді құрауыш сияқты деңгейде сипаттауға бағытталған (ADV_TDS.1 қызметінің ішкі түрін бағалау). Осы сипаттау оқырманға базалық құрауыштың ОФҚ тәуелді құрауышы үшін қажетті функциялармен қалай қамтамасыз ететінін түсінуге мүмкіндік береді.

Осы әрекетті орындау ОФҚІ базалық құрауышына арналған функционалдық сипаттізім арқылы жүргізілуі мүмкін.

14.4.2.3.2 АСО_DEV.2-2 операциясы

Бағалаушы әзірлеу жөніндегі ақпаратты онда әрбір функцияны пайдалану әдісінің дәл сипатталғанын анықтау үшін тексеруге тиіс.

Қауіпсіздік функциясын пайдалану әдісі операцияны белсендіру және нәтижелер алуға арналған функцияның қалай қолданылатындығы туралы түйіндейді. Бағалаушы әзірлеу туралы берілген материалдан болатын функцияның пайдаланылатынын өздігінен түсінуге тиіс. Әрбір функцияны пайдалану үшін жеке тәсілдердің болуы, сондай-ақ оларды жалпы стильді қолдана отырып тану мүлде міндетті емес.

Осы әрекетті орындау ОФҚІ базалық құрауышына арналған функционалдық сипаттізім арқылы жүргізілуі мүмкін.

Әзірлеу жөніндегі ақпаратта ФҚТ тәуелді құрауышына арналған қысымды қолдайтын базалық құрауыштың тәртібінің толық сипаттауы болуға тиіс.

14.4.2.3.3 АСО_DEV.2-3 операциясы

Бағалаушы әзірлеу жөніндегі ақпаратты онда ФҚТ тәуелді құрауышына арналған қысымды қолдайтын базалық құрауыштың тәртібінің дәл сипатталатынын анықтау үшін тексеруге тиіс. Тәуелді құрауыш қажетті функцияларды қамтамасыз ету үшін базалық құрауыштың қауіпсіздік функциясын белсендіреді. Әзірлеу жөніндегі ақпарат белсендірілген базалық құрауыштың қауіпсіздік функциясы үшін базалық құрауыштың қауіпсіз тәртібін толық сипаттауды қамтиды. Базалық құрауыштың қауіпсіз тәртібін сипаттау қауіпсіздік функциясын шақыру кезінде осы құрауыштың қажетті функцияларын көрсетеді. Аталған сипаттау ADV_TDS.1.4C арналған деңгейге сәйкес болуы қажет. Сондықтан БО жобасының куәлігін қауіпсіздік функциялары ОФҚІ тәуелді құрауышымен белсендірілетін жерде осы операция орындайды. Егер белсендіру базалық құрауыштың ОФҚІ арқылы жүргізілмесе, онда қауіпсіз тәртібін БО жобасының куәлігінде сипаттау міндетті емес.

Әзірлеу жөніндегі ақпаратта тәуелді құрауыштың ОФҚ қолдау үшін құрамдас БО пайдаланылатын базалық құрауыш және тәуелді құрауыштың қауіпсіздік функциялары арасындағы сәйкестік көрсетілуге тиіс.

14.4.2.3.4 ACO_DEV.2-4 операциясы

Бағалаушы дамыту туралы ақпаратты тәуелді құрауыш сүйенетін интерфейстер мен базалық құрауыш интерфейстері арасындағы сәйкестік дәлдігін анықтау үшін тексеруге тиіс.

Тәуелді құрауыш сүйенетін интерфейстер мен базалық құрауыш интерфейстері арасындағы сәйкестік матрица немесе кесте формасында болуы мүмкін. Тәуелді құрауыш сүйенетін интерфейстер тәуелділік ақпаратында байқалады (Тәуелді құрауыштың тәуелділігі (ACO_REL) уақытында тексерілгендей).

Осындай әрекетті орындаған уақытта сәйкестік дәлдігін тексеру талаптары және тәуелді құрауыштар үшін қажетті интерфейстерде базалық құрауыштың интерфейстерінің қажет кезде түрленгенін растаудан басқа, тәуелді құрауыш сүйенетін интерфейстің толық қамтылғанын тексерудің өзге талаптары туындамайды.

Қамту толықтығы құрамды қисынды негіздеу операцияларында (ACO_COR) ескеріледі.

14.4.2.4 ACO_DEV.2.2E әрекеті

14.4.2.4.1 ACO_DEV.2-5 операциясы

Бағалаушы дамыту туралы ақпаратты, сондай-ақ тәуелділік туралы ақпаратты интерфейстердің жүйелі сипатталатынын анықтау үшін тексеруге тиіс.

Жұмыстың осы бірлігіндегі есептегіш мақсаты базалық құрауышқа арналған дамыту туралы ақпаратта және тәуелді құрауышқа арналған тәуелділік туралы ақпаратта сипатталатын интерфейстердің жүйелі сипатталғанын анықтау болып табылады.

14.4.3 (ACO_DEV.3) қызметінің ішкі түрін бағалау

14.4.3.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты базалық құрауыштың тәуелді құрауышты қолдау үшін тиісті қауіпсіздіктің функционалдық мүмкіндігімен қамтамасыз етілгенін анықтау болып табылады. Бұған тәуелді құрауыш үшін қажетті тәуелділік туралы ақпаратта көрсетілген интерфейстермен олардың келісілетінін анықтау үшін базалық құрауыштың қауіпсіз тәртібінің интерфейстерін тексеру арқылы қол жеткізіледі.

Сондай-ақ интерфейсті сипаттаудан басқа, бағалаушының сол интерфейстің базалық құрауыштың ОФҚ бөлігін құрайтынын анықтауы үшін тәуелді құрауыш үшін қажетті қауіпсіздіктің функционалдық мүмкіндігімен қамтамасыз ететін базалық құрауыштың ішкі жүйелері сипатталатын болады.

14.4.3.2 Бастапқы деректер

Әрекеттің осы түрінің бағалау куәлігі болып табылады:

- а) құрамдас ҚТ;
- б) дамыту туралы ақпарат;
- в) тәуелділік туралы ақпарат.

14.4.3.3 АСО_DEV.3.1Е әрекеті

Дамыту туралы ақпаратта құрамдас БО пайдаланылатын базалық құрауыштың әрбір интерфейсіне арналған қолданылу мақсаты мен әдісі сипатталуға тиіс.

14.4.3.3. АСО_DEV.3-1 операциясы

Бағалаушы дамыту туралы ақпаратты оның әрбір интерфейсін мақсатын сипаттайтынын анықтау үшін тексеруге тиіс.

Базалық құрауыш тәуелді ОФҚ қамтамасыз етуде тәуелді құрауышпен болатын өзара әрекетті қолдауға арналған интерфейстерді ұсынады. Әрбір интерфейсін мақсаты оны БО жобасындағы ішкі жүйелер арасында қамтамасыз етілуі мүмкін ОФҚ тәуелді құрауышының функционалдық мүмкіндіктері арналған интерфейстерді сипаттау деңгейіндегі сияқты деңгейде сипаттауды білдіреді (Қосымша әрекетті бағалау (ADV_TDS.1)). Осы сипаттау есептеушіге ОФҚ тәуелді құрауышы талап ететін қызметтерді базалық құрауыштың қалай ұсынатынын түсінуді көрсетуге тиіс.

Жұмыстың мұндай бірлігі базалық құрауыштың ОФҚІ болып табылатын осындай интерфейстері үшін базалық құрауыштың функционалдық сипаттізімімен қамтамасыз етіліп орындалуы мүмкін.

14.4.3.3.2 АСО_DEV.3-2 операциясы

Бағалаушы дамыту туралы ақпаратты оның әрбір интерфейске арналған қолдану әдісін сипаттайтынын анықтау үшін тексеруге тиіс.

Интерфейске арналған қолдану әдісі интерфейсін операцияларды қарқындату және интерфейспен байланысты нәтижелер алу үшін өңделетіні туралы қорытынды жасайды. Бағалаушы дамыту туралы ақпаратта осы материалды санаудан бастап интерфейсін қолдану тәсілін анықтай білуі керек. Бұл, мысалы, APIA қалай белсенетіні және содан соң жалпы стильді қолдана отырып, әрбір интерфейсін анықтаудың жалпы сипаттауын беретін болғандықтан, әрбір интерфейсін қолданудың жеке әдісінде болуы қажет екенін білдіруі міндетті емес.

Мұндай жұмыс бірлігі базалық құрауыштың ОФҚІ болып табылатын интерфейстер үшін базалық құрауышқа арналған функционалдық сипаттізіммен қамтамасыз етіліп орындалуы мүмкін.

Дамыту туралы ақпаратта құрамдас БО пайдаланылатын базалық құрауыш интерфейстерін қамтамасыз ететін базалық құрауыштың ішкі жүйелері анықталуға тиіс.

14.4.3.3.3 АСО_DEV.3-3 операциясы

Бағалаушы дамыту туралы ақпаратты тәуелді құрауышқа арналған интерфейстермен қамтамасыз ететін базалық құрауыштың барлық ішкі жүйелерінің табылғанын анықтау үшін тексеруге тиіс.

Базалық құрауыштың ОФҚІ құрайтын болып саналатын осындай интерфейстері үшін интерфейстермен байланысты ішкі жүйелер базалық құрауышты бағалау уақытында БО жобаланатын процесінде (ADV_TDS)

қарастырылатын ішкі жүйелер болады. Тәуелді құрауыш сүйенетін және базалық құрауыштың ОФҚІ құрамайтын интерфейстер базалық құрауыштың ОФҚ шегіндегі ішкі жүйелерге түрлендірілетін болады.

Дамыту туралы ақпаратта тәуелді құрауыштардың ФҚТ мәжбүрлеуін қолдайтын базалық құрауыштың ішкі жүйелерінің тәртібі жоғары деңгейде сипатталып ұсынылуы керек.

14.4.3.3.4 АСО_DEV.3-4 операциясы

Бағалаушы дамыту туралы ақпаратты оның тәуелді құрауыштың ФҚТ мәжбүрлеуін қолдайтын базалық құрауыштың ішкі жүйелерінің тәртібін сипаттайтынын анықтау үшін тексеруге тиіс.

Тәуелді құрауыш базалық құрауыш қызметтер ұсынуы үшін базалық құрауыш интерфейстерін жандандырады. Базалық құрауыштың жандандырылатын интерфейстері үшін дамыту туралы ақпаратта базалық құрауыш тәртібінің қауіпсіздігімен байланысты жоғары деңгейлі сипаттау болуға тиіс. Базалық құрауыш тәртібінің қауіпсіздігін сипаттау базалық құрауыштың интерфейсті шақыру жүргізілген кезде қажетті қызметті қалай ұсынатынын бейнелейді. Мұндай сипаттау ADV_TDS.1.4C арналған сияқты деңгейде болуға тиіс. Сондықтан, базалық құрауышты бағалаудан БО есептік куәлігін қамтамасыз ету егер тәуелді құрауыштар белсендіретін интерфейстер базалық құрауыштың ОФҚІ болып табылатын болса, жұмыс бірлігін қанағаттандырады. Егер тәуелді құрауыштар белсендіретін интерфейстер базалық құрауыштың ОФҚІ болып табылмайтын болса, онда тәртіптің байланысқан қауіпсіздігі базалық құрауыштың БО есептік куәлігінде сипатталмауы да мүмкін.

Дамыту туралы ақпаратта базалық құрауыштың ішкі жүйелеріне интерфейстерден болатын түрлендіру болуы керек.

14.4.3.3.5 АСО_DEV.3-5 операциясы

Бағалаушы дамыту туралы ақпаратты базалық элементтің интерфейстері мен ішкі жүйелері арасындағы сәйкестік дәлдігін анықтау үшін тексеруге тиіс.

Егер базалық құрауышты бағалаудан соң БО есептік куәлігі және функционалдық мүмкіндіктің сипаттізім куәлігі қолжетімді болса, онда олар құрамдас БО пайдаланылған сияқты, базалық құрауыш интерфейстері мен ішкі жүйелері арасындағы сәйкестік дәлдігін тексеру үшін пайдаланылуы ықтимал. Базалық құрауыштың ОФҚІ бөлігін құраған базалық құрауыштың сол интерфейстері базалық құрауыштың функционалдық мүмкіндік сипаттізімінде сипатталатын және байланысты ішкі жүйелер базалық құрауыштың есептік куәлігінде суреттелетін болады.

Егер, дегенмен, базалық құрауыш интерфейсі базалық құрауыштың ОФҚІ бөлігін құрамаған болса, онда дамыту туралы ақпаратта болатын ішкі жүйелер тәртібін сипаттау сәйкестік дәлдігін тексеру үшін пайдаланылатын болады.

Дамыту туралы ақпаратта базалық құрауыштың құрамдас БО және тәуелді құрауыштың ОФҚ қолдауға арналған тәуелді құрауышында пайдаланылатын интерфейстер арасындағы сәйкестікті көрсетуге тиіс.

14.4.3.3.6 ACO_DEV.3-6 операциясы

Бағалаушы дамыту туралы ақпаратты базалық құрауыштың интерфейстері мен тәуелді құрауыш сүйенетін интерфейстер арасындағы сәйкестік дәлдігін анықтау үшін тексеруге тиіс.

Базалық құрауыштың интерфейстері мен тәуелді құрауыш сүйенетін интерфейстер арасындағы сәйкестік матрица немесе кесте түрінде болуы мүмкін. Тәуелді құрауыш сүйенетін интерфейстер тәуелділік ақпаратында байқалады (Тәуелді құрауыштың тәуелді (ACO_REL) уақытында тексерілгендей).

Осындай әрекетті орындаған уақытта сәйкестік дәлдігін тексеру талаптары және тәуелді құрауыштар үшін қажетті интерфейстерде базалық құрауыштың интерфейстерінің қажет кезде түрленгенін растаудан басқа, тәуелді құрауыш сүйенетін интерфейстің толық қамтылғанын тексерудің өзге талаптары туындамайды.

Қамту толықтығы құрамды қисынды негіздеу операцияларында (ACO_COR) ескеріледі.

14.4.3.4 ACO_DEV.3.2E әрекеті

14.4.3.4.1 ACO_DEV.3-7 операциясы

Бағалаушы дамыту туралы ақпаратты, сондай-ақ тәуелділік туралы ақпаратты интерфейстердің жүйелі сипатталатынын анықтау үшін тексеруге тиіс.

Жұмыстың осы бірлігіндегі есептегіш мақсаты базалық құрауышқа арналған дамыту туралы ақпаратта және тәуелді құрауышқа арналған тәуелділік туралы ақпаратта сипатталатын интерфейстердің жүйелі ұсынылғанын анықтау болып табылады.

14.5 Тәуелді құрауыштың тәуелділігі (ACO_REL)

14.5.1 (ACO_REL.1) қызметінің ішкі түрін бағалау

14.5.1.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты базалық құрауыштағы қажетті функционалдық мүмкіндіктің қолжетімділігін және осындай функционалдық мүмкіндікті жандандыратын құрал арқылы анықтау үшін ақпараттың әзірлеушінің тәуелділік куәлігін жеткілікті түрде ұсынатынын анықтау болып табылады. Мұндай міндет жоғары деңгейде сипаттау жағдайында орындалады.

14.5.1.2 Бастапқы деректер

Қызметтің осы ішкі түрінің бағалау куәлігі болып табылады:

- а) құрамдас ҚТ;
- б) тәуелді құрауыштың функционалдық сипаттізімі;

- в) тәуелді құрауыш жобасы;
- г) тәуелді құрауыш архитектурасын жобалау;
- д) тәуелділік ақпараты.

14.5.1.3 Қолдану бойынша ескертулер

ОФҚ базалық құрауышпен өзара әрекет ететін тәуелді құрауыш базалық құрауыштың осылайша ұсынатын функционалдық мүмкіндігін талап етеді (мысалы, қашықтан түпнұсқаландыру, тексеру деректерін қашықтан сақтау). Мұндай жағдайларда жандандырылатын қызметтерді соңғы пайдаланушылар үшін құрамдас БО пішін үйлесіміне жауап беретіндер үшін сипаттау қажет. Осындай құжаттама талабының қисынды негіздемесі құрамдас БО топтастырушыларына базалық құрауыштың қандай қызметтерінің тәуелді құрауышқа теріс әсері болатынын және Даму куәліктері тобын (ACO_DEV) пайдаланған кезде құрауыштар үйлесімділігі анықталатын ақпаратты қалай ұсынатынын анықтауда көмек беру болып табылады.

14.5.1.4 ACO_REL.1.1E әрекеті

Тиісті ақпаратта аппараттық құралдардың, ОФҚ тәуелді құрауышына болжанатын шағын программалар және (немесе) программалық қамтудың базалық құрауыштарының функционалдық тағайындалымының сипаттауы болуға тиіс.

14.5.1.4.1 ACO_REL.1-1 операциясы

Бағалаушы ақпараттың сәйкестігін онда аппараттық құралдардың, ОФҚ тәуелді құрауышына болжанатын шағын программалар және (немесе) программалық қамтудың базалық құрауыштарының функционалдық тағайындалымының сипаттауы болатынын анықтау үшін тексереді.

Бағалаушы аппараттық құралдар, шағын программалар және программалық қамтудың базалық құрауыштармен қамтамасыз етілетінін қоса алғанда, ОФҚ тәуелді құрауышы талап ететін қауіпсіздік функцияларының сипаттауын бағалайды. Осы жұмыстық құрылғының акценті ақпараттық дәлдікті бағалауға емес, осы сипаттау бөлшектерінің деңгейіне жасалады.

(Ақпараттың дәлдігін бағалау келесі жұмыстық құрылғы мәні болып табылады).

Базалық құрауышты функционалдық тағайындалымды сипаттау БО жобасында (БО жобасы (ADV_TDS) келтірілгендей, ОФҚ құрауышын барынша сипаттау деңгейінде болмауға тиіс.

14.5.1.4.2 ACO_REL.1-2 операциясы

Бағалаушы ақпараттың сәйкестігін онда тәуелді құрауыштың операциялық ортасына арналған мақсаттың дәл бейнеленгенін анықтау үшін тексереді.

Тиісті ақпаратта тәуелді құрауышқа есептелген базалық құрауышты қауіпсіздік функцияларының сипаттауы болуы қажет. Бағалаушы тәуелді құрауыштың операциялық ортасының күтілетін ақпаратының сенімділігінің

сәйкестігін тексеру үшін, сенімділік ақпаратын тәуелді құрауышқа арналған ҚТ ортаның мақсаттарын баяндаумен салыстырады.

Мысалы, егер сенімділік ақпараты басқа бағалау дәлелдемесі ОФҚ тәуелді құрауышының өзінің тексеріс деректерін сақт айтынын және қорғайтынын түсіндірмес бұрын (мысалы, тәуелді құрауышты әзірлеу), ОФҚ тәуелді құрауышы тексеріс деректерін сақтау және қорғауы үшін базалық құрауышқа болжанғанын талап етеді, бұл қателікті көрсетеді.

Операциялық орта міндеттерінде ІТ емес шамасына сәйкес келмейтін мақсаттар болатынын айтып кету керек. Базалық құрауышты ортаның қамтамасыз етуі болжанатын қызметтер ҚТ тәуелді құрауышында операциялық ортаға арналған АТ мақсаттарын сипаттауда көрсетілген кезде ортаға қатысты осындай барлық болжамдардың сенімділік ақпаратында көрсетілуі талап етілмейді.

Сенімділік ақпаратында ОФҚ тәуелді құрауышы сол арқылы базалық құрауыш қызметін сұрататын барлық өзара әрекеттер сипатталады.

14.5.1.4.3 ACO_REL.1-3 операциясы

Бағалаушы сенімділік ақпаратын сол арқылы базалық құрауыш қызметін сұрататын тәуелді құрауыш пен базалық құрауыш арасындағы барлық өзара әрекетті оның сипаттайтынын анықтау үшін тексереді.

ОФҚ тәуелді құрауышы базалық құрауыштың шегіне кірмейтін базалық құрауыш қызметтерін сұрата алады (В.3, ҚР СТ ИСО/МЭК 15408-3 АТ құрамдас мәндері арасындағы өзара әрекеттерді қараңыз).

Құрауыштың базалық функционалдық тағайындалымына арналған интерфейстер БО жобасындағы (Функционалдық ішкі топты бағалау (ADV_TDS.1) ішкі жүйелерде қарастырылатын сияқты, ОФҚ құрауышының тәуелді функционалдық тағайындалымындағы интерфейстерінің сипаттауындағы сияқты деңгейде сипатталған.

Тәуелді құрауыштар мен базалық құрауыштардың өзара әрекеттерін сипаттау мақсаты – ОФҚ тәуелді құрауышының тәуелді құрауыштың қауіпсіздік функциясы әрекеттерін қолдау қызметін ұсынуы үшін базалық құрауышқа қалай болжанатынын түсіндіруді қамтамасыз ету. Осы өзара әрекеттер жүзеге асыру деңгейінде сипаттаманы қажетсінбейді (мысалы, құрауыштың бір бағыныңқы программасынан екінші құрауыштың бағыныңқы программасына берілген параметрлер), бірақ басқа құрауыш пайдаланатын белгілі бір құрауыш үшін идентификацияланған деректер элементтерін осы сипаттауға қосу керек. Осы тұжырымдау оқырманға жалпы өзара әрекеттің неліктен қажет екенін түсінуге көмектеседі.

Интерфейстер дәлдігі мен толықтығы ACO_REL.1-1 және ACO_REL.1-2 жұмыстық құрылғыларында белгіленгендей, ОФҚ қажетті базалық құрауыш ұсынатын қауіпсіздік функцияларына негізделген. Осы жұмыстық құрылғыда және керісінше идентификацияланған интерфейстерге арналған бұрынғы жұмыстық құрылғыларда сипатталған барлық функционалдық

тағайындауларды бейнелеу мүмкін болуы керек. Сондай-ақ сипатталған функционалдық тағайындалымға сәйкес келмейтін интерфейс сәйкессіздікті көрсетуге тиіс.

Сенімділік ақпараты тәуелді ОФҚ базалық құрауыштың кедергісі мен көшірмелерінен өзін қалай қорғайтынын сипаттайды.

14.5.1.4.4 ACO_REL.1-4 операциясы

Бағалаушы сенімділік ақпаратын онда тәуелді ОФҚ базалық құрауыштың кедергісі мен көшірмелерінен өзін қалай қорғайтынын сипатталатынын растау үшін тексереді.

Тәуелді ОФҚ базалық құрауыштың кедергісі мен көшірмелерінен өзін қалай қорғайтынын сипаттау ADV_ARC.1-4 үшін қажет сияқты бөлшектер деңгейінде келтірілуі керек.

14.5.2 (ACO_REL.2) қызметінің ішкі түрін бағалау

14.5.2.1 Мақсаты

Осы функционалдық ішкі топтың мақсаты әзірлеушінің сол арқылы функционалдық тағайындау іске қосылатын базалық құрауышта және құралдарда қажетті функционалдық тағайындауға рұқсат етілетінін анықтау үшін ақпараттың қолжетімділігін бағалау дәлелдемесімен қамтамасыз ететінін анықтау болып табылады. Бұл тәуелді және базалық құрауыш арасындағы интерфейстер жағдайында қамтамасыз етіледі және сол интерфейстердің қайтарылатын мәндері тәуелді құрауышпен шақырылады.

14.5.2.2 Бастапқы деректер

Осы функционалдық ішкі топтың бағалау дәлелдемесі болып табылады:

- а) құрамдас ҚТ;
- б) тәуелді құрауыштың функционалдық сипаттізімі;
- в) тәуелді құрауышты әзірлеу;
- г) тәуелді құрауышты жүзеге асыруды көрсету;
- д) тәуелді құрауышты архитектуралық әзірлеу;
- е) сенімділік ақпараты.

14.5.2.3 Қолдану бойынша ескертулер

Кімнің ОФҚ базалық құрауышпен өзара әрекет ететін тәуелді құрауыш осы базалық құрауышпен қарастырылатын функционалдық тағайындауды талап етеді (мысалы, қашықтан түпнұсқаландыру, тексеру деректерін қашықтан сақтау). Мұндай жағдайларда іске қосылған қызметтер соңғы пайдаланушылар үшін құрамдас БО пішін үйлесімдерін жоспарлауға жауаптылар үшін суреттелуі қажет. Құжаттама талаптарының қисынды негіздемесі құрамдас БО топтастырушыларын қолдауда базалық құрауышта қандай қызметтердің топ әзірлемесінің дәлелдемесін (ACO_DEV) қолданған кезде құрауыштардың үйлесімділігін анықтау және ақпарат ұсынуға қарсы тәуелді құрауышқа жағымсыз әсері болатынын анықтауды білдіреді.

14.5.2.4 АСО_REL.2.1Е әрекеті

Сенімділік ақпараты базалық құрауышты аппараттық құралдардың, ОФҚ тәуелді құрауышы болжанатын шағын программа және (немесе) программалық қамтудың функционалдық тағайындалымын сипаттайды.

14.5.2.4.1 АСО_REL.2-1 операциясы

Бағалаушы ақпараттың сәйкестігін онда базалық құрауышты аппараттық құралдардың, ОФҚ тәуелді құрауышы болжанатын шағын программа және (немесе) программалық қамтудың функционалдық тағайындалымын сипаттау болатынын анықтау үшін тексереді.

Бағалаушы апараттық құралдар, шағын программалар және программалық қамтудың базалық құрауыштармен қамтамасыз етілетінін қоса алғанда, ОФҚ тәуелді құрауышы талап ететін қауіпсіздік функцияларының сипаттауын бағалайды. Осы жұмыстық құрылғының акценті ақпараттық дәлдікті бағалауға емес, осы сипаттау бөлшектерінің деңгейіне жасалады.

Ақпараттың дәлдігін бағалау келесі жұмыстық құрылғы мәні болып табылады.

Базалық құрауышты функционалдық тағайындалымды сипаттау БО жобасында (БО жобасы (ADV_TDS) келтірілгендей, ОФҚ құрауышын барынша сипаттау деңгейінде болмауға тиіс.

14.5.2.4.2 АСО_REL.2-2 операциясы

Бағалаушы ақпараттың сәйкестігін онда тәуелді құрауыштың операциялық ортасына арналған мақсаттың дәл бейнеленгенін анықтау үшін тексереді.

Тиісті ақпаратта тәуелді құрауышқа есептелген базалық құрауышты қауіпсіздік функцияларының сипаттауы болуы қажет. Бағалаушы тәуелді құрауыштың операциялық ортасының күтілетін ақпаратының сенімділігінің сәйкестігін тексеру үшін, сенімділік ақпаратын тәуелді құрауышқа арналған ҚТ ортаның мақсаттарын баяндаумен салыстырады.

Мысалы, егер сенімділік ақпараты басқа бағалау дәлелдемесі ОФҚ тәуелді құрауышының өзінің тексеріс деректерін сақт айтынын және қорғайтынын түсіндірмес бұрын (мысалы, тәуелді құрауышты әзірлеу), ОФҚ тәуелді құрауышы тексеріс деректерін сақтау және қорғауы үшін базалық құрауышқа болжанғанын талап етеді, бұл қателікті көрсетеді.

Операциялық орта міндеттерінде ІТ емес шамасына сәйкес келмейтін мақсаттар болатынын айтып кету керек. Базалық құрауышты ортаның қамтамасыз етуі болжанатын қызметтер ҚТ тәуелді құрауышында операциялық ортаға арналған АТ мақсаттарын сипаттауда көрсетілген кезде ортаға қатысты осындай барлық болжамдардың сенімділік ақпаратында көрсетілуі талап етілмейді.

Сенімділік ақпаратында ОФҚ тәуелді құрауышы сол арқылы базалық құрауыш қызметін сұрататын барлық өзара әрекеттер сипатталады.

14.5.2.4.3 ACO_REL.2-3 операциясы

Бағалаушы сенімділік ақпаратын сол арқылы базалық құрауыш қызметін сұрататын тәуелді құрауыш пен базалық құрауыш арасындағы барлық өзара әрекетті оның сипаттайтынын анықтау үшін тексереді.

ОФҚ тәуелді құрауышы базалық құрауыштың шегіне кірмейтін базалық құрауыш қызметтерін сұрата алады (В.3, ҚР СТ ИСО/МЭК 15408-3 АТ құрамдас мәндері арасындағы өзара әрекеттерді қараңыз).

Құрауыштың базалық функционалдық тағайындалымына арналған интерфейстер БО жобасындағы (Функционалдық ішкі топты бағалау (ADV_TDS.1) ішкі жүйелерде қарастырылатын сияқты, ОФҚ құрауышының тәуелді функционалдық тағайындалымындағы интерфейстерінің сипаттауындағы сияқты деңгейде сипатталған.

Тәуелді құрауыштар мен базалық құрауыштардың өзара әрекеттерін сипаттау мақсаты – ОФҚ тәуелді құрауышының тәуелді құрауыштың қауіпсіздік функциясы әрекеттерін қолдау қызметін ұсынуы үшін базалық құрауышқа қалай болжанатынын түсіндіруді қамтамасыз ету. Осы өзара әрекеттер жүзеге асыру деңгейінде сипаттаманы қажетсінбейді (мысалы, құрауыштың бір бағыныңқы программасынан екінші құрауыштың бағыныңқы программасына берілген параметрлер), бірақ басқа құрауыш пайдаланатын белгілі бір құрауыш үшін идентификацияланған деректер элементтерін осы сипаттауға қосу керек. Осы тұжырымдау оқырманға жалпы өзара әрекеттің неліктен қажет екенін түсінуге көмектеседі.

Интерфейстер дәлдігі мен толықтығы ACO_REL.2-1 және ACO_REL.2-2 жұмыстық құрылғыларында белгіленгендей, ОФҚ қажетті базалық құрауыш ұсынатын қауіпсіздік функцияларына негізделген. Осы жұмыстық құрылғыда және керісінше идентификацияланған интерфейстерге арналған бұрынғы жұмыстық құрылғыларда сипатталған барлық функционалдық тағайындауларды бейнелеу мүмкін болуы керек. Сондай-ақ сипатталған функционалдық тағайындалымға сәйкес келмейтін интерфейс сәйкессіздікті көрсетуге тиіс.

Сенімділік ақпараты тәуелді ОФҚ базалық құрауыштың кедергісі мен көшірмелерінен өзін қалай қорғайтынын сипаттайды.

14.5.2.4.4 ACO_REL.2-4 операциясы

Сенімділік ақпаратында пайдаланылатын интерфейс және сол интерфейстерден қайтарылатын мәндер тұрғысынан алғандағы әрбір өзара әрекет сипатталады.

Базалық құрауыштың қызметтері туралы сұраныстарды дайындаған кезде ОФҚ тәуелді құрауышы пайдаланатын интерфейстерді идентификациялау топтастырушыға базалық құрауыштың барлық қажетті тиісті интерфейстерді қамтамасыз ететінін анықтауға мүмкіндік береді. Бұл ұғым бұдан әрі тәуелді құрауыштан күтілетін қайтымды мәндер сипаттізімі

арқылы күшейтіледі. Бағалаушы интерфейстердің әрбір анықталған өзара әрекет үшін сипатталғанын тексереді (ACO_REL.2-3 талданған сияқты).

Сенімділік ақпараты тәуелді ОФҚ базалық құрауыштың кедергісі мен көшірмелерінен өзін қалай қорғайтынын сипаттайды.

14.5.2.4.5 ACO_REL.2-5 операциясы

Бағалаушы сенімділік ақпаратын онда тәуелді ОФҚ базалық құрауыштың кедергісі мен көшірмелерінен өзін қалай қорғайтынын сипатталатынын растау үшін тексереді.

Тәуелді ОФҚ базалық құрауыштың кедергісі мен көшірмелерінен өзін қалай қорғайтынын сипаттау ADV_ARC.1-4 үшін қажет сияқты бөлшектер деңгейінде келтірілуі керек.

14.6 TOE құрамдас тестілеуі (ACO_CTT)

14.6.1 (ACO_CTT.1) қызметінің ішкі түрін бағалау

14.6.1.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты әзірлеушінің тәуелді құрауыш болжанатын базалық құрауышты интерфейстердің әрқайсысын сынауды дұрыс орындағанын және құжатпен рәсімдегенін анықтау болып табылады. Бағалаушы осы анықтаудың бөлігі ретінде әзірлеуші орындаған үлгілерді сынауды қайталайды және ФҚТ құрамдас БО және тәуелді құрауыш болжанатын базалық құрауыш интерфейстерінің күтілетін тәртібіне кепілдік беру үшін қажетті кез келген қосымша сынақтарды орындайды.

14.6.1.2 Бастапқы деректер

Осы функционалдық ішкі топқа арналған бағалау дәлелдемесі:

- а) сынақ үшін қолайлы құрамдас TOE;
- б) құрамдас TOE құрауышын сынау дәлелдемесі;
- в) сенімді ақпарат;
- г) әзірлеу туралы ақпарат.

14.6.1.3 ACO_CTT.1.1E әрекеті

Құрамдас TOE базалық құрауыш интерфейсінің сынақ құжаттамасы сынақ жоспарынан, күтілетін сынақ нәтижелерінен және нақты сынақ нәтижелерінен тұрады.

14.6.1.3.1 ACO_CTT.1-1 операциясы

Бағалаушы құрамдас TOE сынақ хаттамасын оған сынақ құжаттамасы сынақ жоспарынан, күтілетін сынақ нәтижелерінен және нақты сынақ нәтижелері кіретінін анықтау үшін тексереді.

Осы жұмыстық құрылғы егер базалық құрауыш тәуелді құрауыштың операциялық ортасында АТ арналған талаптарды қанағаттандыру үшін пайдаланылған болса, тәуелді құрауышты бағалауға қарамастан, сынақ дәлелдемелерін ұсынумен қанағаттандырылуы мүмкін.

ATE_FUN.1.1E қанағаттандыру үшін қажетті барлық жұмыстық құрылғылар:

- а) сынақ құжаттамасының сынақ хаттамасын оған сынақ құжаттамасы сынақ жоспарынан, күтілетін сынақ нәтижелерінен тұратынын;
- б) сынақ құжаттамасында сынақтардың қайталануына кепілдік беру үшін қажетті ақпарат болатынын;
- в) базалық құрауышты сынауға жұмсалған әзірлеуші күшінің деңгейін анықтау үшін қолданылады.

14.6.1.3.2 АСО_СТТ.1-2 операциясы

Сарапшы базалық құрауыш интерфейсінің мәтіндік құжаттамасын оның тестілеу жүргізу жоспарынан, күтілетін тестілеу нәтижелерінен және нақты тестілеу нәтижелерінен тұратынын анықтау үшін зерделеуге тиіс.

Осы операция сәтті бағаланған базалық құрауыштың ОФҚИ болып табылатын тәуелді құрауыштың құрылған БО болжанатын интерфейстерге арналған базалық құрауышты бағалау негізінде сынақ дәлелдемесін ұсыну арқылы қанағаттандырылуы мүмкін. Бағаланған негізгі құрауыштың ОФҚИ, тәуелді құрауышқа негізделген негізгі құрауыштың нақты интерфейстері болып табылатынын анықтау АСО_COR қызметі уақытында жасалады.

ATE_FUN.1.1E қанағаттандыру үшін қажетті барлық операциялар:

- а) тесті құжаттамасының тестілеуді жүргізу жоспарынан, күтілетін тестілеу нәтижелері мен нақты тестілеу нәтижелерінен тұратынын;
- б) тестілеу құжаттамасында тестілердің қайта жүргізілуі мүмкін екендігіне кепілдік беретін қажетті ақпарат болатынын;
- в) әзірлеушінің негізгі құрауышты тестілеуге қолданған күшінің деңгейін анықтау үшін қолданылатын болады.

Әзірлеушінің БО құрастырылған тестілерін орындау жөніндегі тесті құжаттамасы ОФҚ белгіленгендей жұмыс істейтінін көрсетуге тиіс.

14.6.1.3.3 АСО_СТТ.1-3 операциясы

Сарапшы тестілеу құжаттамасын әзірлеушінің БО құрастырылған тестілерін орындау жөніндегі тесті құжаттамасы ОФҚ белгіленгендей жұмыс істейтінін көрсететінін анықтау үшін зерттеуге тиіс.

Сарапшы әзірлеушінің қандай ФҚТ тексергенін идентификациялау үшін, құрамдас БО үшін анықталған ФҚТ тестілеу жоспарында сипатталған тестілер арасындағы графикалық бейнелеуді жасауға тиіс.

Осы операция бойынша нұсқау 12.2.1 т. және 12.2.2 т. болады.

ATE_FUN.1.3C анықталғандай, тестілерді сәтті орындаудан шығатын тұжырымдар әзірлеуші тексергендей, құрамдас БО ФҚТ күтілгендей жұмыс істейтінін шешу үшін графикалық бейнелеумен салыстырылуы мүмкін.

Әзірлеушінің базалық құрауыштың интерфейсін орындау жөніндегі тесті құжаттамасы тәуелді құрауыш болжанатын базалық құрауыш интерфейсінің белгіленгендей жұмыс істейтінін көрсетуге тиіс.

14.6.1.3.4 АСО_СТТ.1-4 операциясы

Сарапшы тесті құжаттамасын әзірлеуші орындаған базалық құрауыштар интерфейстерінің тестісі тәуелді құрауыш болжанатын базалық құрауыштар

интерфейстерінің өздерін белгіленгендей ұстайтынын көрсетуге тиіс екендігін белгілеу үшін зерделеуге тиіс.

Сарапшы әзірлеушінің базалық құрауыштың қандай интерфейстерін тексергенін идентификациялауы үшін, тәуелді құрауыш (ACO_REL сенімді ақпарат көздерінде анықталғандай) болжанатын базалық құрауыш интерфейстерінде және тестілеу жөніндегі жоспарда сипатталған тестілер арасындағы графикалық бейнелеуді жасауға тиіс.

Осы операция бойынша нұсқау 12.2.1 т. және 12.2.2 т. болады.

ATE_FUN.1.3C үшін бағаланған сияқты тестілерді сәтті орындаудан жасалатын тұжырымдар әзірлеушінің тексерген базалық құрауыш интерфейстерінің күтілгендей жұмыс істейтінін анықтау үшін графикалық бейнелеумен салыстырылуы мүмкін және базалық құрауыш тестілеу үшін қолайлы болуға тиіс.

14.6.1.3.5 ACO_CTT.1-5 операциясы

Сарапшы құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін зерделеуге тиіс.

Құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін, құрастырылған БО ATE_IND.2-1 және ATE_IND.2-2 операциялары қолданылатын болады.

14.6.1.3.6 ACO_CTT.1-6 операциясы

Сарапшы әзірлеуші ұсынатын ресурстар жиынтығын олардың базалық құрауышты функционалдық тексеру үшін базалық құрауышты әзірлеуші пайдаланатын ресурстар жиынтығына балама екенін анықтау үшін зерделеуге тиіс.

Құрастырылған БО пайдаланылатын базалық құрауышты функционалдық тексеру үшін, ұсынылатын ресурстар жиынтығының пайдаланылатындарға балама екенін анықтау үшін ATE_IND.2-3 операциясы қолданылатын болады.

14.6.1.4 ACO_CTT.1.2E әрекеті

14.6.1.4.1 ACO_CTT.1-7 операциясы

Сарапшы тестілеуді әзірлеушінің тестілеу нәтижелерін тексеру үшін, құрастырылған қауіпсіздік тапсырмасында анықталған ФҚТ ішжиынына арналған ATE_IND.2.2E сәйкес орындауға тиіс.

Сарапшы ілеспе операциялармен айтып жаздырылғандай, барлық талдаулар, нәтижелер мен қорытындыларды құрастырылған БО үшін БТЕ жинақтайтын ATE_IND.2.2E қанағаттандыру үшін қажетті барлық операцияны қолдануға тиіс.

14.6.1.5 ACO_CTT.1.3E әрекеті

14.6.1.5.1 ACO_CTT.1-8 операциясы

Сарапшы тестілеуді ОФҚ белгіленгендей жұмыс істейтінін растау үшін, құрастырылған қауіпсіздік тапсырмасында анықталған ФҚТ ішжиынына арналған ATE_IND.2.3E сәйкес орындауы керек.

Сарапшы барлық талдаулар, нәтижелер мен қорытындыларды құрастырылған БО үшін БТЕ жинақтайтын АТЕ_IND.2.3Е қанағаттандыру үшін қажетті барлық операцияны операциялармен айтып жаздырылғандай қолдануға тиіс.

Құрастырылған БО ОФҚ интерфейстерін тестілеу үшін тандай отырып, сарапшы бағаланған нұсқа немесе пішін үйлесімінің құрауыштарының кез келген түрленуіне назар аударуға тиіс. Бағаланған құрауыштардың түрленуі өзгертілген жетекші құжаттама нәтижесінде енгізілген түзетулер, түрлі пішін үйлесімдерін, ОФҚ құрауышы шегінде болмаған құрауыштың қосымша бөліктерін пайдалану деңгейін қамтуы мүмкін.

Аталған түрлендірулер негіздемені құрастыру жөніндегі қызмет уақытында идентификацияланатын болады (АСО_COR).

14.6.2 (АСО_СТТ.2) қызметінің ішкі түрін бағалау

14.6.2.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты әзірлеушінің тәуелді құрауыш болжанатын базалық құрауыштың әрбір интерфейсіне арналған тестілерді дұрыс орындағанын және тіркегенін анықтаудан тұрады. Сарапшы осы анықтаудың бөлігі ретінде әзірлеуші орындаған тестілер таңдамасын қайталайды және құрастырылған БО күтілетін жұмыс режимін және тәуелді құрауыш болжанатын базалық құрауыш интерфейстерін толық көрсету үшін талап етілетін кез келген қосымша тестіні орындайды.

14.6.2.2 Бастапқы деректер

Қызметтің осы ішкі түрінің бағалау деректері болып табылады:

- а) тестілеу үшін қолайлы құрастырылған БО;
- б) деректерді тексеретін құрастырылған БО;
- в) сенімді ақпарат;
- г) әзірлеу ақпараты.

15.6.2.3 АСО_СТТ.2.1Е әрекеті

ҚР СТ ИСО/МЭК 15408-3 АСО_СТТ.2.1С: құрастырылған БО және базалық құрауыш интерфейсін тестілеу құжаттамасы тестілеуді өткізу жоспарлары, күтілетін тестілеу нәтижелері және нақты тестілеу нәтижелерінен тұруға тиіс.

14.6.2.3.1 АСО_СТТ.2- 1 операциясы

Сарапшы базалық құрауыш интерфейсінің мәтіндік құжаттамасын оның тестілеу жүргізу жоспарынан, күтілетін тестілеу нәтижелерінен және нақты тестілеу нәтижелерінен тұратынын анықтау үшін зерделеуге тиіс.

Егер тәуелді құрауыштың операциялық ортасында АТ арналған талаптарды қанағаттандыру үшін базалық құрауыш пайдаланылса, осы операция тәуелді құрауышты бағалаудың тестілеу дәлелдемесін ұсынумен қанағаттандырылуы мүмкін.

АТЕ_FUN.1.1Е қанағаттандыру үшін қажетті барлық операциялар:

а) тесті құжаттамасының тестілеуді жүргізу жоспарынан, күтілетін тестілеу нәтижелері мен нақты тестілеу нәтижелерінен тұратынын;

б) тестілеу құжаттамасында тестілердің қайта жүргізілуі мүмкін екендігіне кепілдік беретін қажетті ақпарат болатынын;

в) әзірлеушінің базалық құрауышты тестілеуге қолданған күшінің деңгейін анықтау үшін қолданылатын болады.

14.6.2.3.2 АСО_СТТ.2-2 операциясы

Сарапшы базалық құрауыш интерфейсінің тестілеу құжаттамасын оның тестілеу жүргізу жоспарынан, күтілетін тестілеу нәтижелерінен және нақты тестілеу нәтижелерінен тұратынын анықтау үшін зерделеуге тиіс.

Осы операция сәтті бағаланған базалық құрауыштың ОФҚИ болып табылатын тәуелді құрауыштың құрылған БО болжанатын интерфейстерге арналған базалық құрауышты бағалау негізінде сынақ дәлелдемесін ұсыну арқылы қанағаттандырылуы мүмкін.

Бағаланған негізгі құрауыштың ОФҚИ, тәуелді құрауышқа негізделген негізгі құрауыштың нақты интерфейстері болып табылатынын анықтау АСО_COR қызметі уақытында жасалады.

ATE_FUN.1.1E қанағаттандыру үшін қажетті барлық операциялар:

а) тесті құжаттамасының тестілеуді жүргізу жоспарынан, күтілетін тестілеу нәтижелері мен нақты тестілеу нәтижелерінен тұратынын;

б) тестілеу құжаттамасында тестілердің қайта жүргізілуі мүмкін екендігіне кепілдік беретін қажетті ақпарат болатынын;

в) әзірлеушінің негізгі құрауышты тестілеуге қолданған күшінің деңгейін анықтау үшін қолданылатын болады.

Әзірлеушінің БО құрастырылған тестілерін орындау жөніндегі тесті құжаттамасы ОФҚ белгіленгендей жұмыс істейтінін және аяқталатынын көрсетуге тиіс.

14.6.2.3.3 АСО_СТТ.2-3 операциясы

Сарапшы тестілеу құжаттамасын әзірлеушінің БО құрастырылған тестілерін орындау жөніндегі тесті құжаттамасы ОФҚ белгіленгендей жұмыс істейтінін көрсететінін анықтау үшін зерделеуге тиіс.

Қарапайым түйісу кестесі тестілеу арақатынасын көрсету үшін жеткілікті болуы мүмкін. Тестілеу құжаттамасында ұсынылатын тестілер мен ФҚТ арасындағы арақатынасты идентификациялау дәл өрнектелуге тиіс.

14.6.2.3.4 АСО_СТТ.2-4 операциясы

Сарапшы тестілеу құжаттамасын әзірлеушінің БО құрастырылған тестілерін орындау жөніндегі тесті құжаттамасы ОФҚ белгіленгендей жұмыс істейтінін көрсететінін анықтау үшін зерттеуге тиіс.

Осы операция бойынша нұсқау 12.2.1 т. және 12.2.2 т. болады.

ATE_FUN.1.3C анықталғандай, тестілерді сәтті орындаудан шығатын тұжырымдар әзірлеуші тексергендей, құрамдас БО ФҚТ күтілгендей жұмыс істейтінін шешу үшін графикалық бейнелеумен салыстырылуы мүмкін.

Әзірлеушінің базалық құрауыштың интерфейсін орындау жөніндегі тесті құжаттамасы тәуелді құрауыш болжанатын базалық құрауыш интерфейсінің белгіленгендей жұмыс істейтінін және аяқталатынын көрсетуге тиіс.

14.6.2.3.5 АСО_СТТ.2-5 операциясы

Сарапшы тестілеу құжаттамасын оның сенімді ақпарат көздерінде анықталған тәуелді құрауыш және интерфейстер болжанатын базалық құрауыш интерфейстерін тестілеуге қатысты тестілеу құжаттамасындағы тестілер арасындағы дәл арақатынасты қамтамасыз ететінін белгілеу үшін зерделеуге тиіс.

Қарапайым түйісу кестесі тестілеу арақатынасын көрсету үшін жеткілікті болуы мүмкін. Тестілеу құжаттамасында ұсынылатын тестілер мен ФҚТ арасындағы арақатынасты идентификациялау дәл өрнектелуге тиіс.

14.6.2.3.6 АСО_СТТ.2-6 операциясы

Сарапшы тесті құжаттамасын әзірлеуші орындаған базалық құрауыштар интерфейстерінің тестісі тәуелді құрауыш болжанатын базалық құрауыштар интерфейстерінің өздерін белгіленгендей ұстайтынын көрсетуге тиіс екендігін белгілеу үшін зерделеуге тиіс.

Осы операция бойынша нұсқау 12.2.1 т. және 12.2.2 т. болады.

ATE_FUN.1.3C үшін бағаланған сияқты тестілерді сәтті орындаудан жасалатын тұжырымдар әзірлеушінің тексерген базалық құрауыш интерфейстерінің күтілгендей жұмыс істейтінін анықтау үшін графикалық бейнелеумен салыстырылуы мүмкін.

Базалық құрауыш тестілеу үшін қолайлы болуға тиіс.

14.6.2.3.7 АСО_СТТ.2-7 операциясы

Сарапшы құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін зерделеуге тиіс.

Құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін, құрастырылған БО ATE_IND.2-1 және ATE_IND.2-2 операциялары қолданылатын болады.

14.6.2.3.8 АСО_СТТ.2-8 операциясы

Сарапшы әзірлеуші ұсынатын ресурстар жиынтығын олардың базалық құрауышты функционалдық тексеру үшін базалық құрауышты әзірлеуші пайдаланатын ресурстар жиынтығына балама екенін анықтау үшін зерделеуге тиіс.

Құрастырылған БО пайдаланылатын базалық құрауышты функционалдық тексеру үшін, ұсынылатын ресурстар жиынтығының пайдаланылатындарға балама екенін анықтау үшін ATE_IND.2-3 операциясы қолданылатын болады.

14.6.2.4 АСО_СТТ.2.2Е әрекеті

14.6.2.4.1 АСО_СТТ.2-9 операциясы

Тестілер құрастырылған БО қауіпсіздік тапсырмасында анықталған ФҚТ дұрыс жұмыс режимін көрсету үшін, АТЕ_IND.2.2Е сәйкес таңдалуы және орындалуы керек.

Сарапшы ілеспе операциялармен айтып жаздырылғандай, барлық талдаулар, нәтижелер мен қорытындыларды құрастырылған БО үшін БТЕ жинақтайтын АТЕ_IND.2.2Е қанағаттандыру үшін қажетті барлық операцияны қолданады.

14.6.2.5 АСО_СТТ.2.3Е әрекеті

14.6.2.5.1 АСО_СТТ.2-10 операциясы

Сарапшы тестілеуді ОФҚ белгіленгендей жұмыс істейтінін растау үшін, құрастырылған қауіпсіздік тапсырмасында анықталған ФҚТ ішжиынына арналған АТЕ_IND.2.3Е сәйкес орындауы керек.

Сарапшы барлық талдаулар, нәтижелер мен қорытындыларды құрастырылған БО үшін БТЕ жинақтайтын АТЕ_IND.2.3Е қанағаттандыру үшін қажетті барлық операцияны операциялармен айтып жаздырылғандай қолданады.

Құрастырылған БО ОФҚ интерфейстерін тестілеу үшін таңдай отырып, сарапшы бағаланған нұсқа немесе пішін үйлесімінің құрауыштарының кез келген түрленуіне назар аударуға тиіс. Бағаланған құрауыштардың түрленуі өзгертілген жетекші құжаттама нәтижесінде енгізілген түзетулер, түрлі пішін үйлесімдерін, ОФҚ құрауышы шегінде болмаған құрауыштың қосымша бөліктерін пайдалану деңгейін қамтуы мүмкін.

Аталған түрлендірулер негіздемені құрастыру жөніндегі қызмет уақытында идентификацияланатын болады (АСО_COR).

14.6.2.5.2 АСО_СТТ.2-11 операциясы

Сарапшы тестілеуді олардың белгіленгендей дұрыс жұмыс істейтінін анықтау үшін негізгі құрауышқа дейінгі интерфейстер ішжиыны үшін (АТЕ_IND.2) қызметінің ішкі түрін бағалауға сәйкес орындауға тиіс.

Сарапшы барлық талдаулар, нәтижелер мен қорытындыларды құрастырылған БО үшін БТЕ жинақтайтын АТЕ_IND.2.3Е қанағаттандыру үшін қажетті барлық операцияны операциялармен айтып жаздырылғандай қолданады.

Құрастырылған БО ОФҚ интерфейстерін тестілеу үшін таңдай отырып, сарапшы бағаланған нұсқа немесе пішін үйлесімінің құрауыштарының кез келген түрленуіне назар аударуға тиіс. Атап айтқанда, сарапшы тестілер әзірлемесінің базалық құрауышты бағалау уақытында қарастырылмаған базалық құрауыш интерфейстерінің дұрыс тәртібін көрсететін жорамалдауға тиіс. Осы қосымша интерфейстер және базалық құрауыштың басқа түрлендірулері негіздемені құрастыру (АСО_COR) жөніндегі қызмет уақытында идентификацияланатын болады.

14.7 Осалдық талдауын құру (ACO_VUL)

14.7.1 (ACO_VUL.1) қызметінің ішкі түрін бағалау

14.7.1.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты құрастырылған БО операциялық ортасында оңай пайдаланылатын осалдықтың болатынын анықтаудан тұрады.

Әзірлеуші құрауыштарды бағалаудан ұсынылатын кез келген қалдық осалдықтың бөлшектерін ұсынады. Сарапшы берілетін қалдық осалдықтың диспозициясын талдауды орындайды, сондай-ақ құрауыштарда кез келген жаңа әлеуетті осалдықты идентификациялау үшін жалпы доменді қарауды орындайды (яғни, базалық құрауышты бағалаудан бастап хабарлаған қоғамдық пайдаланыстағы проблемалар). Сарапшы содан соң БО әлеуетті осалдықтың операциялық ортасында шабуылшының негізгі шабуылдау мүмкіндіктерін пайдалана алмайтынын көрсету үшін, қорғауға шыдайтын тестілеуді орындайды.

14.7.1.2 Бастапқы деректер

Қызметтің осы ішкі түрінің бағалау деректері болып табылады:

- а) тестілеу үшін қолайлы құрамдас БО;
- б) құрастырылған ҚТ;
- в) негіздемені құру;
- г) жетекші құжаттама;
- д) ықтимал қауіпсіздік осалдығын идентификациялауды қолдауға арналған жалпы қолжетімді ақпарат;
- е) әрбір құрауышты бағалау уақытында ұсынылатын қалдық осалдық.

14.7.1.3 Қолдану бойынша ескертулер

Қызметтің осы ішкі түрін бағалау үшін қолдану бойынша ескертпелерді қараңыз (AVA_VAN.1).

14.7.1.4 ACO_VUL.1.1E әрекеті

Құрастырылған БО тестілеу үшін қолайлы болуға тиіс.

14.7.1.4.1 ACO_VUL.1-1 операциясы

Сарапшы құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін зерделеуге тиіс.

Құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін, құрастырылған БО ATE_IND.2-1 және ATE_IND.2-2 операциялары қолданылатын болады. Егер кепілдік пакетінде ACO_CTT тобынан болатын құрауыштар қамтылатын болса, онда сарапшы осы жағдайдың қанағаттандырылғанын көрсету үшін ACO_CTT*-1 операциясының нәтижесіне жүгіне алады.

14.7.1.4.2 ACO_VUL.1-2 операциясы

Сарапшы құрастырылған БО пішін үйлесімін АТ объектілеріне қатысты ҚТ құрауыштарындағы кез келген болжамдар мен мақсаттардың басқа құрауыштармен орындалғанын белгілеу үшін зерделеуге тиіс.

Құрауышқа арналған ҚТ, мысалы, пайдаланылатын операциялық жүйеге арналған ҚТ базалық құрауыш операциялық жүйеге жүктелмеген кез келген қосымшаның артықшылығы болатын режимде жұмыс істемейтін болжамын қамтуы мүмкін болғандықтан, ҚТ қатынасы болатын құрауышты пайдалануы мүмкін басқа құрауыштар туралы болжамдарды қамтуы мүмкін.

14.7.1.5 АСО_VUL.1.2Е әрекеті

14.7.1.5.1 АСО_VUL.1-3 операциясы

Сарапшы базалық құрауышты бағалаудан болатын қалдық осалдықтарды олардың құрастырылған БО операциялық ортасында пайдалану үшін жарамды болып табылмайтынын белгілеу үшін зерделеуге тиіс.

Базалық құрауышта пайдалану үшін жарамсыздығын көрсететін базалық құрауышты бағалау уақытында өнімдегі идентификацияланбаған осалдықтар тізімі осы қызметке енгізу ретінде пайдаланылуға тиіс. Сарапшы құрамдас БО пайдалану үшін жарамсыз деп саналған осалдық бойынша алғышарттардың немесе қайта енгізілген әлеуетті осалдық құрамдастыруының болатынын анықтайды. Мысалы, егер базалық құрауышты бағалау уақытында құрамдас БО бағалауға қолданылған операциялық жүйенің ерекше сервисі бұғатталған деп болжанса, онда бұрын таңдалған сол сервиске қатысты кез келген әлеуетті осалдықты енді қарастыру қажет.

Одан басқа, базалық құрауышты бағалаудан алынған осалдықты пайдалану үшін жарамсыз, белгілі осы тізімді құрастырылған БО шегінде басқа құрауыштар (мысалы, тәуелді құрауыш) үшін осалдықты пайдалану үшін жарамсыз кез келген белгілі индикаторда қарастыру қажет. Әлеуетті осалдық оқшаулауда пайдалану үшін жарамсыз болып табылатын жерде басқа әлеуетті осалдық болатын АТ объектісімен топтастырылған кезде пайдалану үшін жарамды болып табылатын жағдайды қарау керек.

14.7.1.5.2 АСО_VUL.1-4 операциясы

Сарапшы тәуелді құрауышты бағалаудан алынатын қалдық осалдықтарды олардың құрамдас БО операциялық ортасында пайдалану үшін жарамды болып табылмайтынын белгілеу үшін зерделеуге тиіс.

Тәуелді құрауышта пайдалану үшін жарамсыздығын көрсететін базалық құрауышты бағалау уақытында өнімдегі идентификацияланбаған осалдықтар тізімі осы қызметке енгізу ретінде пайдаланылуға тиіс. Сарапшы құрамдас БО пайдалану үшін жарамсыз деп саналған осалдық бойынша алғышарттардың немесе қайта енгізілген әлеуетті осалдық құрамдастыруының болатынын анықтайды. Мысалы, егер тәуелді құрауышты бағалау уақытында ортаның операциялық талаптарына жауап беретін АТ құрастырылған БО бағалауда базалық құрауышпен ұсынылатын сервис сұранысына жауап ретінде анықталған мәнді қайтармайтыны

болжанса, онда бұрын таңдалған қайтымды мәнге қатысты кез келген әлеуетті осалдықты енді қарастыру қажет.

Одан басқа, тәуелді құрауышты бағалаудан алынған осалдықты пайдалану үшін жарамсыз, белгілі осы тізімді құрастырылған БО шегінде басқа құрауыштар (мысалы, тәуелді құрауыш) үшін осалдықты пайдалану үшін жарамсыз кез келген белгілі индикаторда қарастыру қажет. Әлеуетті осалдық оқшаулауда пайдалану үшін жарамсыз болып табылатын жерде басқа әлеуетті осалдық болатын АТ объектісімен топтастырылған кезде пайдалану үшін жарамды болып табылатын жағдайды қарау керек.

14.7.1.6 ACO_VUL.1.3E әрекеті

14.7.1.6.1 ACO_VUL.1-5 операциясы

Сарапшы қолжетімді ақпарат көздерін базалық құрауышты бағалауды аяқтаудан бастап белгілі болған базалық құрауыштағы ықтимал қауіпсіздік осалдығын идентификациялауды қолдау үшін ашық зерделеуге тиіс.

Сарапшы жалпы домендегі ақпаратты базалық құрауышты осалдықты табу үшін AVA_VAN.1-2 сипатталғандай етіп пайдаланатын болады.

Базалық құрауышты бағалауға дейін жұрт алдында рұқсат етілген әлеуетті осалдық егер сарапшы үшін бұзушы әлеуетті осалдықты пайдалану үшін талап ететін шабуыл мүмкіндігі елеулі түрде азайтылғаны анық болмаса, одан әрі зерделенбеуі керек. Бұл әлеуетті осалдықты пайдаланудың ықшамдалғанын білдіретін базалық құрауышты бағалаудан бастап, кейбір жаңа технологияларды енгізу арқылы болуы мүмкін.

14.7.1.6.2 ACO_VUL.1-6 операциясы

Сарапшы қолжетімді ақпарат көздерін тәуелді құрауышты бағалауды аяқтаудан бастап белгілі болған тәуелді құрауышты ықтимал қауіпсіздік осалдығын идентификациялауды қолдау үшін ашық зерделеуге тиіс.

Сарапшы жалпы домендегі ақпаратты тәуелді құрауышты осалдықты табу үшін AVA_VAN.1-2 сипатталғандай етіп пайдаланатын болады.

Тәуелді құрауышты бағалауға дейін жұрт алдында рұқсат етілген әлеуетті осалдық егер сарапшы үшін бұзушы әлеуетті осалдықты пайдалану үшін талап ететін шабуыл мүмкіндігі елеулі түрде азайтылғаны анық болмаса, одан әрі зерделенбеуі керек. Бұл әлеуетті осалдықты пайдаланудың ықшамдалғанын білдіретін базалық құрауышты бағалаудан бастап, кейбір жаңа технологияларды енгізу арқылы болуы мүмкін.

14.7.1.6.3 ACO_VUL.1-7 операциясы

Сарапшы тестілеуге үміткер болып табылатын БТЕ идентификацияланған және құрастырылған БО оның операциялық ортасында қолданылатын әлеуетті қауіпсіздік осалдықтары жазбасын жасауға тиіс.

ҚТ, жетекші құжаттама және функционалдық сипаттізім осалдықтың құрамдас БО оның операциялық ортасында қатысы болатынын анықтау үшін пайдаланылады.

Егер сарапшы осалдықтың операциялық ортада қолданылмайтынын анықтаса, сарапшы осалдықты одан әрі қарастырудан алып тастау үшін кез келген негіздеме жазбасын жасайды. Сарапшы одан әрі қарастыру үшін әлеуетті осалдық жазбасын басқаша жасайды.

Құрамдас БО оның қорғауға шыдайтын тесті әрекеттеріне (яғни ACO_VUL.1.4E) үлес ретінде пайдаланылуы мүмкін операциялық ортасында қолданылатын әлеуетті осалдықтар тізімі БТЕ сарапшыларға берілетін болады.

14.7.1.7 ACO_VUL.1.4E әрекеті

14.7.1.7.1 ACO_VUL.1-8 операциясы

Сарапшы қорғауға шыдау тестілеуін AVA_VAN.1.3E үшін жан-жақты айтылғандай етіп өткізуі керек.

Сарапшы AVA_VAN.1.3E сарапшысының әрекетін қанағаттандыру үшін қажетті барлық операцияны құрастырылған БО арналған барлық талдаулар мен қорытындыларды операциялармен айтып жазылғандай етіп қолданады.

Сарапшы сондай-ақ AVA_VAN.1.1E сарапшысының барлық әрекетіне арналған операцияларды тестілеу үшін қолайлы болып табылатын әзірлеуші ұсынатын құрастырылған БО анықтау үшін қолданатын болады.

14.7.2 (ACO_VUL.2) қызметінің ішкі түрін бағалау

14.7.2.1 Мақсаты

Қызметтің осы ішкі түрінің мақсаты құрамдастырылған БО операциялық ортасында бұзушының негізгі шабуыл әлеуетін пайдалану үшін жарамды осалдықтың болатынын анықтаудан тұрады.

Әзірлеуші базалық және тәуелді құрауыштар киыстыруы арқылы енгізілген құрауыштар және кез келген осалдықтар үшін алынған кез келген қалдық осалдықтың диспозициясына талдауды ұсынады. Сарапшы құрауыштарда кез келген жаңа әлеуетті осалдықты идентификациялау үшін жалпы доменді қарауды іске асырады (яғни, базалық құрауышты бағалаудан бастап хабарлаған қоғамдық пайдаланыстағы проблемалар). Сарапшы сондай-ақ құрастырылған БО осалдығын тәуелсіз талдауды және қорғауға шыдамды тестілеуді орындайды.

14.7.2.2 Бастапқы деректер

Қызметтің осы ішкі түрінің бағалау деректері болып табылады:

- а) тестілеу үшін қолайлы құрастырылған БО;
- б) құрамдас ҚТ;
- в) негіздемені құру;
- г) сенімді ақпарат;
- д) жетекші құжаттама;
- е) ықтимал қауіпсіздік осалдығын идентификациялауды қолдау үшін қолжетімді ашық ақпарат;
- ж) әрбір құрауышты бағалау уақытында берілетін қалдық осалдықтар.

14.7.2.3 Қолдану бойынша ескертулер

Қызметтің осы ішкі түрін бағалау үшін қолдану бойынша ескертпелерді қараңыз (AVA_VAN.2).

14.7.2.4 АСО_VUL.2.1Е әрекеті

Құрастырылған БО тестілеу үшін қолайлы болуға тиіс.

14.7.2.4.1 АСО_VUL.2-1 операциясы

Сарапшы құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін зерделеуге тиіс.

Құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін, құрастырылған БО ATE_IND.2-1 және ATE_IND.2-2 операциялары қолданылатын болады.

Егер кепілдік пакетінде АСО_СТТ тобынан болатын құрауыштар қамтылатын болса, онда сарапшы осы жағдайдың қанағаттандырылғанын көрсету үшін АСО_СТТ*-1 операциясының нәтижесіне жүгіне алады.

14.7.2.4.2 АСО_VUL.2-2 операциясы

Сарапшы құрастырылған БО пішін үйлесімін АТ объектілеріне қатысты ҚТ құрауыштарындағы кез келген болжамдар мен мақсаттардың басқа құрауыштармен орындалғанын белгілеу үшін зерделеуге тиіс.

Құрауышқа арналған ҚТ, мысалы, пайдаланылатын операциялық жүйеге арналған ҚТ базалық құрауыш операциялық жүйеге жүктелмеген кез келген қосымшаның артықшылығы болатын режимде жұмыс істемейтін болжамын қамтуы мүмкін болғандықтан, ҚТ қатынасы болатын құрауышты пайдалануы мүмкін басқа құрауыштар туралы болжамдарды қамтуы мүмкін. Осы болжамдар мен мақсаттар құрамдас БО басқа құрауыштармен орындалуға тиіс.

14.7.2.5 АСО_VUL.2.2Е әрекеті

14.7.2.5.1 АСО_VUL.2-3 операциясы

Сарапшы базалық құрауышты бағалаудан болатын қалдық осалдықтарды олардың құрастырылған БО операциялық ортасында пайдалану үшін жарамды болып табылмайтынын белгілеу үшін зерделеуге тиіс.

Базалық құрауышта пайдалану үшін жарамсыздығын көрсететін базалық құрауышты бағалау уақытында өнімдегі идентификацияланбаған осалдықтар тізімі осы қызметке енгізу ретінде пайдаланылуға тиіс. Сарапшы құрамдас БО пайдалану үшін жарамсыз деп саналған осалдық бойынша алғышарттардың немесе қайта енгізілген әлеуетті осалдық құрамдастыруының болатынын анықтайды. Мысалы, егер базалық құрауышты бағалау уақытында құрамдас БО бағалауға қолданылған операциялық жүйенің ерекше сервисі бұғатталған деп болжанса, онда бұрын таңдалған сол сервиске қатысты кез келген әлеуетті осалдықты енді қарастыру қажет.

Одан басқа, базалық құрауышты бағалаудан алынған осалдықты пайдалану үшін жарамсыз, белгілі осы тізімді құрастырылған БО шегінде басқа құрауыштар (мысалы, тәуелді құрауыш) үшін осалдықты пайдалану үшін жарамсыз кез келген белгілі индикаторда қарастыру қажет. Әлеуетті осалдық оқшаулауда пайдалану үшін жарамсыз болып табылатын жерде басқа әлеуетті осалдық болатын АТ объектісімен топтастырылған кезде пайдалану үшін жарамды болып табылатын жағдайды қарау керек.

14.7.2.5.2 ACO_VUL.2-4 операциясы

Сарапшы тәуелді құрауышты бағалаудан алынатын қалдық осалдықтарды олардың құрамдас БО операциялық ортасында пайдалану үшін жарамды болып табылмайтынын белгілеу үшін зерделеуге тиіс.

Тәуелді құрауышта пайдалану үшін жарамсыздығын көрсететін базалық құрауышты бағалау уақытында өнімдегі идентификацияланбаған осалдықтар тізімі осы қызметке енгізу ретінде пайдаланылуға тиіс. Сарапшы құрамдас БО пайдалану үшін жарамсыз деп саналған осалдық бойынша алғышарттардың немесе қайта енгізілген әлеуетті осалдық құрамдастыруының болатынын анықтайды. Мысалы, егер тәуелді құрауышты бағалау уақытында ортаның операциялық талаптарына жауап беретін АТ құрастырылған БО бағалауда базалық құрауышпен ұсынылатын сервис сұранысына жауап ретінде анықталған мәнді қайтармайтыны болжанса, онда бұрын таңдалған қайтымды мәнге қатысты кез келген әлеуетті осалдықты енді қарастыру қажет.

Одан басқа, тәуелді құрауышты бағалаудан алынған осалдықты пайдалану үшін жарамсыз, белгілі осы тізімді құрастырылған БО шегінде басқа құрауыштар (мысалы, базалық құрауыш) үшін осалдықты пайдалану үшін жарамсыз кез келген белгілі индикаторда қарастыру қажет. Әлеуетті осалдық оқшаулауда пайдалану үшін жарамсыз болып табылатын жерде басқа әлеуетті осалдық болатын АТ объектісімен топтастырылған кезде пайдалану үшін жарамды болып табылатын жағдайды қарау керек.

14.7.2.6 ACO_VUL.2.3E әрекеті

14.7.2.6.1 ACO_VUL.2-5 операциясы

Сарапшы қолжетімді ақпарат көздерін базалық құрауышты бағалауды аяқтаудан бастап белгілі болған базалық құрауыштағы ықтимал қауіпсіздік осалдығын идентификациялауды қолдау үшін ашық зерделеуге тиіс.

Сарапшы жалпы домендегі ақпаратты базалық құрауыштағы осалдықты табу үшін AVA_VAN.1-2 сипатталғандай етіп пайдаланатын болады.

Базалық құрауышты бағалауға дейін жұрт алдында рұқсат етілген әлеуетті осалдық егер сарапшы үшін бұзушы әлеуетті осалдықты пайдалану үшін талап ететін шабуыл мүмкіндігі елеулі түрде азайтылғаны анық болмаса, одан әрі зерделенбеуі керек. Бұл әлеуетті осалдықты пайдаланудың ықшамдалғанын білдіретін базалық құрауышты бағалаудан бастап, кейбір жаңа технологияларды енгізу арқылы болуы мүмкін.

14.7.2.6.2 ACO_VUL.2-6 операциясы

Сарапшы қолжетімді ақпарат көздерін тәуелді құрауышты бағалауды аяқтаудан бастап белгілі болған тәуелді құрауыштағы ықтимал қауіпсіздік осалдығын идентификациялауды қолдау үшін ашық зерделеуге тиіс.

Сарапшы жалпы домендегі ақпаратты тәуелді құрауышты бағалауды осалдықты табу үшін AVA_VAN.1-2 сипатталғандай етіп пайдаланатын болады.

Тәуелді құрауышты бағалауға дейін жұрт алдында рұқсат етілген әлеуетті осалдық егер сарапшы үшін бұзушы әлеуетті осалдықты пайдалану үшін талап ететін шабуыл мүмкіндігі елеулі түрде азайтылғаны анық болмаса, одан әрі зерделенбеуі керек. Бұл әлеуетті осалдықты пайдаланудың ықшамдалғанын білдіретін базалық құрауышты бағалаудан бастап, кейбір жаңа технологияларды енгізу арқылы болуы мүмкін.

14.7.2.6.3 ACO_VUL.2-7 операциясы

Сарапшы тестілеуге үміткер болып табылатын БТЕ идентификацияланған және құрастырылған БО оның операциялық ортасында қолданылатын әлеуетті қауіпсіздік осалдықтары жазбасын жасауға тиіс.

ҚТ, жетекші құжаттама және функционалдық сипаттізім осалдықтың құрамдас БО оның операциялық ортасында қатысы болатынын анықтау үшін пайдаланылады.

Егер сарапшы осалдықтың операциялық ортада қолданылмайтынын анықтаса, сарапшы осалдықты одан әрі қарастырудан алып тастау үшін кез келген негіздеме жазбасын жасайды. Сарапшы одан әрі қарастыру үшін әлеуетті осалдық жазбасын басқаша жасайды.

Құрамдас БО оның қорғауға шыдайтын тесті әрекеттеріне (яғни ACO_VUL.1.4E) үлес ретінде пайдаланылуы мүмкін операциялық ортасында қолданылатын әлеуетті осалдықтар тізімі БТЕ сарапшыларға берілетін болады.

14.7.2.7 ACO_VUL.2.4E әрекеті

14.7.2.7.1 ACO_VUL.2-8 операциясы

Сарапшы құрастырылған БО ықтимал қауіпсіздік осалдығын идентификациялау үшін ҚТ, жетекші құжаттама, сенімді ақпарат және құрастырылған БО негіздемесінің құрылуын қарауды жүргізуге тиіс.

Осалдықты тәуелсіз талдауда құрастырылған БО құрауыштарын қарастыру ол дұрыстық пакетіне қатысты әзірлеу абстракцияларының барлық деңгейін міндетті түрде ескермейтін болғандықтан, құрауышты бағалау үшін AVA_VAN.2.3E тіркелгеннен ерекше біраз басқа форманы қабылдайды. Оларды енді құрауыштарды бағалау уақытында қарастырады, бірақ мәліметтер құрастырылған БО бағалау үшін қолжетімді болмауы мүмкін. Алайда, AVA_VAN.2.3E байланысты операцияларда сипатталған жалпы тәсіл қолданылады және ол құрастырылған БО-да сарапшының әлеуетті осалдықты іздеуінен негіздеме жасауға тиіс.

Құрастырылған БО-да пайдаланылатын жеке құрауыштардың осалдығын талдау жеке құрауыштарды бағалау уақытында орындалатын болады. Құрастырылған БО-ны бағалау уақытында осалдықты талдау фокусы құрастырылған БО пішін үйлесіміне қатысты бағаланған құрауыштың пішін үйлесімі арасындағы құрауыштарды пайдаланғанда құрауыштар немесе кез келген өзгерістерді топтастыру нәтижесінде енгізілген кез келген осалдықты идентификациялауға тиіс.

Сарапшы құрауыш құрастырылымының түсінігін тәуелді құрауышқа арналған дұрыс ақпаратта нақтыланған сияқты пайдаланатын болады және базалық құрауышқа арналған негіздемені әзірлеу және жасау ақпараты тәуелді құрауышпен бірге ақпаратты жобалайды. Осы ақпарат бағалаушыға базалық құрауыш пен тәуелді құрауыштың қалай өзара әрекет ететінін және осы өзара әрекет нәтижесінде енгізілуі мүмкін әлеуетті осалдықты қалай идентификациялайтынын түсінуге мүмкіндік береді.

Сарапшы осы қайта қаралған нұсқау арқылы енгізілген кез келген әлеуетті осалдықты идентификациялау үшін, құрастырылған БО орнату, іске қосу және жұмыс істеуі үшін қарастырылған кез келген жаңа нұсқауды қарастыратын болады.

Егер жеке құрауыштардың әрқайсысы құрауышты бағалауды аяқтаудан бастап дұрыстықтың үздіксіз әрекеті арқылы болса, онда сарапшы осалдықты тәуелсіз талдауда түзету(лер)ді қарастырады.

Дұрыстықтың үздіксіз әрекетінің ашық есебінде ұсынылатын өзгеріспен байланысты ақпарат (мысалы, техникалық қызмет көрсету нәтижелері туралы есеп) өзгеріске арналған кіріс материалының негізгі көзі болатын болады. Бұл жалпы пайдалануда қолжетімді өзгеріске қатысты кез келген ақпарат және өзгерістен алынатын жетекші құжаттаманың кез келген жаңартуларымен толықтырылатын болады, мысалы, өндірушінің вебсайты.

Бағаланған пішін үйлесімінің құрауыш пішін үйлесімінде кез келген түзету немесе ауытқудың толық әсерін белгілеуге арналған деректердің жетіспеушілігінен идентификацияланатын кез келген тәуекел сарапшының осалдықты талдауына тіркелген болуға тиіс.

14.7.2.8 ACO_VUL.2.5E әрекеті

14.7.2.8.1 ACO_VUL.2-9 операциясы

Сарапшы қорғауға шыдау тестілеуін AVA_VAN.2.4E үшін толық айтылғандай өткізуге тиіс.

Сарапшы операциялармен айтылып жазылғандай, барлық талдаулар мен қорытындыларды құрастырылған БО арналған БТЕ хабарлайтын AVA_VAN.2.4E сарапшысының әрекетін қанағаттандыру үшін қажетті барлық операцияны қолдануға тиіс.

Сарапшы сондай-ақ әзірлеуші ұсынатын құрастырылған БО тестілеу үшін қолайлы болып табылатынын анықтау үшін AVA_VAN.2.1E сарапшысының әрекетіне арналған операцияны қолданатын болады.

14.7.3 (АСО_VUL.3) қызметінің ішкі түрін бағалау

14.7.3.1 Мақсаты

Қызметтің осы ішкі қызметінің мақсаты құрастырылған БО оның операциялық ортасында шабуылдың жақсартылған әлеуетін бұзушының пайдалануы үшін жарамды осалдықтың болатынын анықтаудан тұрады.

Әзірлеуші базалық және тәуелді құрауыштар қиыстыруы арқылы енгізілген құрауыштар мен кез келген қалдық осалдықтар үшін алынған диспозиция талдауын ұсынады. Сарапшы құрауыштардағы кез келген жаңа әлеуетті осалдықтарды идентификациялау үшін жалпы доменді қарауды іске асырады (яғни, құрауыштарды бағалауды аяқтаудан бастап алынған жалпы домендегі проблемалар). Сарапшы сондай-ақ құрастырылған БО осалдығын тәуелсіз талдауды және қорғауға шыдамды тестілеуді орындайды.

14.7.3.2 Бастапқы деректер

Қызметтің осы ішкі түріне арналған бағалау деректері болып табылады:

- а) тестілеу үшін қолайлы құрастырылған БО;
- б) құрастырылған ҚТ;
- в) негіздемені құрастыру;
- г) сенімді ақпарат;
- д) жетекші құжаттама;
- е) ықтимал қауіпсіздік осалдығын идентификациялауды қолдауға арналған қолжетімді ашық ақпарат;
- ж) әрбір құрауышты бағалау уақытында берілетін қалдық осалдықтар.

14.7.3.3 Қолдану бойынша ескертулер

Қызметтің осы ішкі түрін бағалау үшін қолдану бойынша ескертпелерді қараңыз (AVA_VAN.3).

14.7.3.4 АСО_VUL.3.1Е әрекеті

Құрастырылған БО тестілеу үшін қолайлы болуға тиіс.

14.7.3.4.1 АСО_VUL.3-1 операциясы

Сарапшы құрастырылған БО ол тиісті түрде орнатылуы және белгілі режимде болуын анықтау үшін зерделеуге тиіс.

Құрастырылған БО оның тиісті түрде орнатылғанын және белгілі режимде болатынын анықтау үшін, құрастырылған БО ATE_IND.2-1 және ATE_IND.2-2 операциялары қолданылатын болады.

Егер кепілдік пакетінде АСО_СТТ тобынан болатын құрауыштар қамтылатын болса, онда сарапшы осы жағдайдың қанағаттандырылғанын көрсету үшін құрастырылған БО (АСО_СТТ) - бір операциясының нәтижесіне жүгіне алады.

14.7.3.4.2 АСО_VUL.3-2 операциясы

Сарапшы құрастырылған БО пішін үйлесімін басқа құрауыштармен орындалған РТ объектілеріне қатысты ҚТ құрауыштарында кез келген болжамдар мен мақсаттарды анықтау үшін зерделеуге тиіс.

Құрауышқа арналған ҚТ, мысалы, пайдаланылатын операциялық жүйеге арналған ҚТ базалық құрауыш операциялық жүйеге жүктелмеген кез келген қосымшаның артықшылығы болатын режимде жұмыс істемейтін болжамын қамтуы мүмкін болғандықтан, ҚТ қатынасы болатын құрауышты пайдалануы мүмкін басқа құрауыштар туралы болжамдарды қамтуы мүмкін. Осы болжамдар мен мақсаттар құрамдас БО басқа құрауыштармен орындалуға тиіс.

14.7.3.5 ACO_VUL.3.2E әрекеті

14.7.3.5.1 ACO_VUL.3-3 операциясы

Сарапшы базалық құрауышты бағалаудан болатын қалдық осалдықтарды олардың құрастырылған БО операциялық ортасында пайдалану үшін жарамды болып табылмайтынын белгілеу үшін зерделеуге тиіс.

Базалық құрауышта пайдалану үшін жарамсыздығын көрсететін базалық құрауышты бағалау уақытында өнімдегі идентификацияланбаған осалдықтар тізімі осы қызметке енгізу ретінде пайдаланылуға тиіс. Сарапшы құрамдас БО пайдалану үшін жарамсыз деп саналған осалдық бойынша алғышарттардың немесе қайта енгізілген әлеуетті осалдық құрамдастыруының болатынын анықтайды. Мысалы, егер базалық құрауышты бағалау уақытында құрамдас БО бағалауға қолданылған операциялық жүйенің ерекше сервисі бұғатталған деп болжанса, онда бұрын таңдалған сол сервиске қатысты кез келген әлеуетті осалдықты енді қарастыру қажет.

Одан басқа, базалық құрауышты бағалаудан алынған осалдықты пайдалану үшін жарамсыз, белгілі осы тізімді құрастырылған БО шегінде басқа құрауыштар (мысалы, тәуелді құрауыш) үшін осалдықты пайдалану үшін жарамсыз кез келген белгілі индикаторда қарастыру қажет. Әлеуетті осалдық оқшаулауда пайдалану үшін жарамсыз болып табылатын жерде басқа әлеуетті осалдық болатын АТ объектісімен топтастырылған кезде пайдалану үшін жарамды болып табылатын жағдайды қарау керек.

14.7.3.5.2 ACO_VUL.3-4 операциясы

Сарапшы тәуелді құрауышты бағалаудан алынатын қалдық осалдықтарды олардың құрамдас БО операциялық ортасында пайдалану үшін жарамды болып табылмайтынын белгілеу үшін зерделеуге тиіс.

Тәуелді құрауышта пайдалану үшін жарамсыздығын көрсететін базалық құрауышты бағалау уақытында өнімдегі идентификацияланбаған осалдықтар тізімі осы қызметке енгізу ретінде пайдаланылуға тиіс. Сарапшы құрамдас БО пайдалану үшін жарамсыз деп саналған осалдық бойынша алғышарттардың немесе қайта енгізілген әлеуетті осалдық құрамдастыруының болатынын анықтайды. Мысалы, егер тәуелді құрауышты бағалау уақытында ортаның операциялық талаптарына жауап беретін АТ құрастырылған БО бағалауда базалық құрауышпен ұсынылатын

сервис сұранысына жауап ретінде анықталған мәнді қайтармайтыны болжанса, онда бұрын таңдалған қайтымды мәнге қатысты кез келген әлеуетті осалдықты енді қарастыру қажет.

Одан басқа, тәуелді құрауышты бағалаудан алынған осалдықты пайдалану үшін жарамсыз, белгілі осы тізімді құрастырылған БО шегінде басқа құрауыштар (мысалы, базалық құрауыш) үшін осалдықты пайдалану үшін жарамсыз кез келген белгілі индикаторда қарастыру қажет. Әлеуетті осалдық оқшаулауда пайдалану үшін жарамсыз болып табылатын жерде басқа әлеуетті осалдық болатын АТ объектісімен топтастырылған кезде пайдалану үшін жарамды болып табылатын жағдайды қарау керек.

14.7.3.6 АСО_VUL.3.3Е әрекеті

14.7.3.6.1 АСО_VUL.3-5 операциясы

Сарапшы қолжетімді ақпарат көздерін базалық құрауышты бағалауды аяқтаудан бастап белгілі болған базалық құрауыштағы ықтимал қауіпсіздік осалдығын идентификациялауды қолдау үшін ашық зерделеуге тиіс.

Сарапшы жалпы домендегі ақпаратты базалық құрауыштағы осалдықты табу үшін AVA_VAN.3-2 сипатталғандай етіп пайдаланатын болады.

Базалық құрауышты бағалауға дейін жұрт алдында рұқсат етілген әлеуетті осалдық егер сарапшы үшін бұзушы әлеуетті осалдықты пайдалану үшін талап ететін шабуыл мүмкіндігі елеулі түрде азайтылғаны анық болмаса, одан әрі зерделенбеуі керек. Бұл әлеуетті осалдықты пайдаланудың ықшамдалғанын білдіретін базалық құрауышты бағалаудан бастап, кейбір жаңа технологияларды енгізу арқылы болуы мүмкін.

14.7.3.6.2 АСО_VUL.3-6 операциясы

Сарапшы қолжетімді ақпарат көздерін тәуелді құрауышты бағалауды аяқтаудан бастап белгілі болған тәуелді құрауыштағы ықтимал қауіпсіздік осалдығын идентификациялауды қолдау үшін ашық зерделеуге тиіс.

Сарапшы жалпы домендегі ақпаратты тәуелді құрауышты осалдықты табу үшін AVA_VAN.3-2 сипатталғандай етіп пайдаланатын болады.

Тәуелді құрауышты бағалауға дейін жұрт алдында рұқсат етілген әлеуетті осалдық егер сарапшы үшін бұзушы әлеуетті осалдықты пайдалану үшін талап ететін шабуыл мүмкіндігі елеулі түрде азайтылғаны анық болмаса, одан әрі зерделенбеуі керек. Бұл әлеуетті осалдықты пайдаланудың ықшамдалғанын білдіретін базалық құрауышты бағалаудан бастап, кейбір жаңа технологияларды енгізу арқылы болуы мүмкін.

14.7.3.6.3 АСО_VUL.3-7 операциясы

Сарапшы тестілеуге үміткер болып табылатын БТЕ идентификацияланған және құрастырылған БО оның операциялық ортасында қолданылатын әлеуетті қауіпсіздік осалдықтары жазбасын жасауға тиіс.

ҚТ, жетекші құжаттама және функционалдық сипаттізім осалдықтың құрамдас БО оның операциялық ортасында қатысы болатынын анықтау үшін пайдаланылады.

Егер сарапшы осалдықтың операциялық ортада қолданылмайтынын анықтаса, сарапшы осалдықты одан әрі қарастырудан алып тастау үшін кез келген негіздеме жазбасын жасайды. Сарапшы одан әрі қарастыру үшін әлеуетті осалдық жазбасын басқаша жасайды.

Құрамдас БО оның қорғауға шыдайтын тесті әрекеттеріне (яғни ACO_VUL.1.4E) үлес ретінде пайдаланылуы мүмкін операциялық ортасында қолданылатын әлеуетті осалдықтар тізімі БТЕ сарапшыларға берілетін болады.

14.7.3.7 ACO_VUL.3.4E әрекеті

14.7.3.7.1 ACO_VUL.3-8 операциясы

Сарапшы құрастырылған БО ықтимал қауіпсіздік осалдығын идентификациялау үшін ҚТ, жетекші құжаттама, сенімді ақпарат және құрастырылған БО негіздемесінің құрылуын қарауды жүргізуге тиіс.

Осалдықты тәуелсіз талдауда құрастырылған БО құрауыштарын қарастыру ол дұрыстық пакетіне қатысты әзірлеу абстракцияларының барлық деңгейін міндетті түрде ескермейтін болғандықтан, құрауышты бағалау үшін AVA_VAN.3.3E тіркелгеннен ерекше біраз басқа форманы қабылдайды. Оларды енді құрауыштарды бағалау уақытында қарастырады, бірақ мәліметтер құрастырылған БО бағалау үшін қолжетімді болмауы мүмкін. Алайда, AVA_VAN.2.3E байланысты операцияларда сипатталған жалпы тәсіл қолданылады және ол құрастырылған БО-да сарапшының әлеуетті осалдықты іздеуінен негіздеме жасауға тиіс.

Құрастырылған БО-да пайдаланылатын жеке құрауыштардың осалдығын талдау жеке құрауыштарды бағалау уақытында орындалатын болады. Құрастырылған БО-ны бағалау уақытында осалдықты талдау фокусы құрастырылған БО пішін үйлесіміне қатысты бағаланған құрауыштың пішін үйлесімі арасындағы құрауыштарды пайдаланғанда құрауыштар немесе кез келген өзгерістерді топтастыру нәтижесінде енгізілген кез келген осалдықты идентификациялауға тиіс.

Сарапшы құрауыш құрастырылымының түсінігін тәуелді құрауышқа арналған дұрыс ақпаратта нақтыланған сияқты пайдаланатын болады және базалық құрауышқа арналған негіздемені әзірлеу және жасау ақпараты тәуелді құрауышпен бірге ақпаратты жобалайды. Осы ақпарат бағалаушыға базалық құрауыш пен тәуелді құрауыштың қалай өзара әрекет ететінін және осы өзара әрекет нәтижесінде енгізілуі мүмкін әлеуетті осалдықты қалай идентификациялайтынын түсінуге мүмкіндік береді.

Сарапшы осы қайта қаралған нұсқау арқылы енгізілген кез келген әлеуетті осалдықты идентификациялау үшін, құрастырылған БО орнату, іске қосу және жұмыс істеуі үшін қарастырылған кез келген жаңа нұсқауды қарастыратын болады.

Дұрыстықтың үздіксіз әрекетінің ашық есебінде ұсынылатын өзгеріспен байланысты ақпарат (мысалы, техникалық қызмет көрсету нәтижелері

туралы есеп) өзгеріске арналған кіріс материалының негізгі көзі болатын болады. Бұл жалпы пайдалануда қолжетімді өзгеріске қатысты кез келген ақпарат және өзгерістен алынатын жетекші құжаттаманың кез келген жаңартуларымен толықтырылатын болады, мысалы, өндірушінің вебсайты.

Бағаланған пішін үйлесімінің құрауыш пішін үйлесімінде кез келген түзету немесе ауытқудың толық әсерін белгілеуге арналған деректердің жетіспеушілігінен идентификацияланатын кез келген тәуекел сарапшының осалдықты талдауына тіркелген болуға тиіс.

14.7.3.8 ACO_VUL.3.5E әрекеті

14.7.3.8.1 ACO_VUL.3-9 операциясы

Сарапшы қорғауға шыдау тестілеуін AVA_VAN.3.4E үшін толық айтылғандай өткізуге тиіс.

Сарапшы операциялармен айтылып жазылғандай, барлық талдаулар мен қорытындыларды құрастырылған БО арналған БТЕ хабарлайтын AVA_VAN.3.4E сарапшысының әрекетін қанағаттандыру үшін қажетті барлық операцияны қолдануға тиіс.

Сарапшы сондай-ақ әзірлеуші ұсынатын құрастырылған БО тестілеу үшін қолайлы болып табылатынын анықтау үшін AVA_VAN.3.1E сарапшысының әрекетіне арналған операцияны қолданатын болады.

А қосымшасы
(ақпараттық)

Бағалау бойынша жалпы нұсқаулар

А.1 Мақсаты

Осы бөлімнің мақсаты нұсқаудың жалпы мәселелерін қамту үшін бағалау нәтижелерін техникалық растауды қамтамасыз етуден тұрады. Осындай жалпы нұсқауды пайдалану бағалаушы орындайтын жұмыстың әділдігіне, қайталанғыштығы мен өндірімділігіне қол жеткізуге көмектеседі.

А.2 Іріктеу

Осы қосымшада іріктеуді іске асыру бойынша жалпы нұсқаулар болады. Нақты және толық ақпарат іріктемені орындау қажет болатын жерде бағалаушы әрекетінің белгілі бір әрекетіне сәйкес келетін операцияларда берілген. Іріктеу – жалпы алғанда жиынтық үшін зерттелетін және репрезентативті (өкілдік) болжанатын бағалау куәліктерінің жиынтығы талап етілетін кейбір ішжиын арқылы бағалаушы орындайтын белгілі бір процедура. Бұл бағалаушыға нақты бағалау куәлігінің дұрыстығына оны толық көлемде талдаусыз жеткілікті сенімді болуға мүмкіндік береді.

Іріктеу барабар сенім деңгейін қолдау кезінде ресурстарды үнемдеу үшін жүргізіледі. Куәліктерді таңдау мынадай екі ықтимал нәтижеге әкелуі мүмкін.

а) Ішжиында бағалаушыға жиынтықтың жалпы дұрыс екендігіне белгілі бір сенімділік ұялататын ешқандай қате байқалған жоқ;

б) Ішжиында қателер табылды және сол себепті жиынтықтың дұрыстығына жалпы алғанда күдік болады. Тіпті байқалған барлық қатені жою бағалаушыға қажетті сенімділік ұялату үшін жеткіліксіз болып табылуы мүмкін, сондықтан бағалаушыға не ішжиынның көлемін ұлғайту, не осы нақты куәлік үшін іріктеуді пайдалануды тоқтатуға тура келеді.

Іріктеу — бұл куәлік құрамы мәні бойынша салыстырмалы түрде біркелкі болған кезде тұжырымдар сеніміне ие болу үшін пайдаланылуы мүмкін әдіс, мысалы, егер куәлік толық анықталған процесс нәтижесі болып табылса.

Іріктеу БК көрсетілген немесе операцияларда айтылған жағдайларда бағалаушы орындайтын әрекеттерге тиімді тәсіл ретінде танылады. Басқа салаларда іріктеуге нақты қызмет түрін басқа қызмет түрлеріне пропорционал болмайтын күштер талап етілетін жерде және ол сенімге қатысты артпаған жерде ғана рұқсат етіледі. Мұндай жағдайларда осы салада іріктеуді қолдану негіздемесі қажет болады. БО көлемді және күрделі болып табылатын факті, не оның көптеген функционалдық қауіпсіздік талаптары болып табылатыны күрделі және көлемді БО бағалау кезінде жеткілікті негіз

болып табылмайды және біраз күш қажет болуы мүмкін. Дұрысы, осындай әрекет тиісінше сенім деңгейінен асатыны күтілмейтін кезде әдетте тексеру немесе зерттеу қажет болатын жағдайда БО әзірлеуге арналған тәсіл БК нақты талаптарына арналған материалдың көп санын беретін кезде осы ерекшелік осындай жағдайлармен шектеледі.

Іріктеу БО қауіпсіздік мақсаттары мен қатерінің ықтимал әсерін назарға ала отырып, қатаң негіздеуді қажет етеді. Әсер ету іріктеу нәтижесінде жіберілуі мүмкін қателерге байланысты болады. Сондай-ақ іріктеп тексерілетін куәлік сипатын тексеру қажет және талап кез келген қауіпсіздік функцияларын елемеуі және олардың рөлін төмендетпеуі қажет.

БО жүзеге асырумен тікелей байланысты куәліктерден іріктеудің (мысалы, әзірлеуші тестісінің нәтижелері) процестің дұрыс орындалатыны туралы қорытынды шығарумен байланысты іріктеу кезінде қолданылатыннан ерекше тәсілді талап ететінін мойындау керек. Көп жағдайда, бағалаушыдан процестің шын мәнінде орындалатынын анықтау талап етілетін кезде іріктеу стратегиясы ұсынылады. Мұнда тәсіл әзірлеушінің тестілеу нәтижелерін іріктеу кезінде қолданылатыннан ерекшеленеді. Бұл бастапқы жағдайда процестің орындалатыны туралы сенімділік туралы сөз болады, ал екіншісінде біз БО жүзеге асыру дұрыстығын анықтаумен айналысатын боламыз. Әдетте, барынша көлемді іріктеуді процестің орындалатынына көз жеткізу қажеттігіне қарағанда, БО жүзеге асыру дұрыстығымен байланысты жағдайда талдауға тура келеді.

Белгілі бір жағдайда бағалаушы үшін әзірлеуші тестісінің бірнеше реттік ерекше мәнін беруге қолайлы болуы мүмкін. Мысалға, тәуелсіз тестілерді орындау жағдайында онда қосылған тестілердің кеңейтілген жиынтығы сырттай ғана ерекшеленетін болады (ATE_COV және ATE_DPT критерийлеріне сәйкес болуы үшін қажеттіге қарағанда көп тестіні орындаудан болуы ықтимал), одан әрі бағалаушыға тиісінше әзірлеуші тестісінің бірнеше реттігіне тоғысуына тура келеді. Әзірлеуші тестісінің бірнеше реттілігін жоғары пайыздық іріктеуге арналған талапты білдірмейтінін, керісінше, тестілердің аталған кеңейтілген жиынтығының төмен пайыздық іріктеуге негізделгенін айтып кету керек.

Әдетте, функционалдық тестіні орындауға арналған автоматты тесті жиынтығын пайдаланған кезде, бағалаушыға әзірлеушінің тестісін іріктеуді ғана қайталағаннан гөрі жалпы тесті жиынтығын қайта тексерген оңай. Бұған қарамастан, бағалаушының автоматты тестінің дұрыс нәтиже бермейтінін тексеруге міндеттілігі болады. Тұжырым мынадай, автоматты тесті жиынтығын іріктеу басқалардан артығырақ тестіні іріктеу және осы жағдаймен бірдей қолданылатын іріктеудің жеткілікті көлеміне кепілдік беру үшін түбегейлі тексерілуге тиіс.

Іріктеу кезінде мынадай принциптерді әрдайым сақтау ұсынылады:

а) іріктеу кездейсоқ болуы мүмкін емес, керісінше, барлық куәлік үлгілерін таңдайтын сияқты іріктеу керек. Іріктеу көлемі мен құрылымы негізделген болуға тиіс;

б) іріктеу БО дұрыс орындауға негізделетін кезде, іріктеудің оның қолданылу салаларына қатысты барлық аспектілер бойынша репрезентативті болуы керек. Атап айтқанда, іріктеу құрауыштар, қауіпсіздік функциялары, әзірлеу және пайдалану орындарының және аппараттық платформалар типтерінің (егер олар бірнешеу болса) алуан түрлілігін қамтуы керек (егер олар бірнешеу болса).

Іріктеу көлемін бағалау тиімділігімен салыстыру қажет, ол БО кейбір сипаттамаларына (мысалы, БО өлшемдері мен күрделілігі, құжаттаманың көлемі) байланысты болады;

в) сондай-ақ, іріктеу әзірлеушінің тестісі қайталанатын және өндірілетін болып табылатыны туралы куәлікті нақты алуға қатысты болған кезде, пайдаланылатын іріктеу әзірлеушінің әр түрлі тесті режимдері сияқты барлық белгілі бір аспектілеріне сәйкес болуға тиіс. Пайдаланылатын іріктеу әзірлеуші тестісінің функционалдық процесінде кез келген жүйе проблемасын байқауға тиіс. Бағалаушының әрекеті, яғни әзірлеуші тестісінің дүркіндігі және тәуелсіз тестілердің орындалуы БО-да негізгі мәселелерді көрсетуге қатысты дәлелденген болып табылуға тиіс;

г) іріктеу кейбір процесті орындау куәлігін алу үшін іске асыру үшін жерде (мысалы, келушілерді бақылау немесе жобаны талдау) бағалаушы процесті орындауда қабылдауға лайық сенімділікті алу үшін жеткілікті ақпарат көлемін таңдауы керек;

д) өтініш беруші мен әзірлеушіге іріктеудің нақты құрамы туралы күні бұрын хабарламау керек. Сондықтан іріктеу және қосымша материалдардың уақытылы жеткізілу қажеттігі ескерілуі керек, мысалы, бағалаушыға тесті программаларының кешені және жабдықтар бағалау жүргізу кестесіне сәйкес;

е) таңдау кезінде іріктеу мүмкіндігінше қасақана болмауы керек (қашанда тізімдегі бірінші немесе соңғы нөмірді ғана таңдамау қажет). Шындығында іріктеуді бағалаушыға емес, басқа біреуге тапсыру керек.

Таңдауда табылған қателер екі санатқа жатқызылуы мүмкін — жүйелік немесе кездейсоқ. Егер қателік жүйелік болса, оның себебін жойып, жаңа іріктеуді толық орындау қажет. Әзірлеушінің кездейсоқ қателер туралы мәселені тиісті түсіндіруі кезінде мұндай түсіндіруді растау қажет болғанымен, жаңа іріктеудің қажетінсіз шешілуі мүмкін. Бағалаушының анықтау кезінде басқа іріктеуді таңдау немесе пайдалану көлемін арттыру туралы дұрыс мағынаны басшылыққа алғаны жөн.

А.3 Тәуелділіктер

А.3.1 Кіріспе

Жалпы жағдайда бағалау бойынша қызметтер мен әрекеттердің талап етілетін түрлері мен ішкі түрлерін еркін тәртіппен немесе параллель орындау мүмкін. Дегенмен, бағалаушының ескеруге тиіс бірнеше тәуелділік түрлері болады.

Осы ішкі бөлім бағалау бойынша әр түрлі қызмет және әрекет түрлері мен ішкі түрлері арасындағы тіркеу жөніндегі жалпы нұсқауды ұсынады.

А.3.2 Қызмет түрлері арасындағы тәуелділіктер

Кейбір жағдайларда әр түрлі сенім кластары үшін бағалау бойынша сонымен байланысты қызмет түрлерін орындаудың тіпті белгілі бір жүйелілігі ұсынылуы немесе талап етілуі мүмкін. Нақты үлгі – ҚТ бағалау бойынша қызмет түрі. ҚТ бағалау бойынша қызмет түрі алдымен ҚТ оларды орындау негізі мен контексін қамтамасыз ететіндіктен, БО бағалау жөніндегі қандай да бір қызмет түрлерінен басталады. Алайда, БО бағалауды аяқтағанша БО бағалау бойынша қорытынды шешім жасау БО бағалау жөніндегі қызмет нәтижелері ҚТ-да өзгерістерге әкелуі мүмкін болғандықтан, мүмкін емес.

А.3.3 Қызметтің ішкі түрлері арасындағы тәуелділіктер

Бағалаушының БК 3-бөлімінде көрсетілген құрауыштар арасындағы тәуелділікті ескеруі қажет.

Тәуелділіктердің көбі – бір жақты, мысалы, AVA_VAN.1 бағалау қызметінің ішкі түрі ADV_FSP.1 және AGD_OPE.1 бағалау қызметінің ішкі түрін талап етеді. Сонымен бірге екі құрауыш та бір-біріне байланысты болатын өзара тәуелділік үлгілері бар. Бұның үлгісі ATE_FUN.1 бағалау қызметінің ішкі түрі және ATE_COV.1 бағалау қызметінің ішкі түрі болып табылады.

Әдетте, қызметтің ішкі түрі бойынша оң қорытындыны қызметтің осы ішкі түрі байланысты болатын қызметтің сол басқа ішкі түрлерін сәтті аяқтаған кезде ғана қабылдауға болады. Мысалы, әдетте, AVA_VAN.1 бойынша оң қорытынды егер ADV_FSP.1 және AGD_OPE.1 жататын қызметтің ішкі түрлері бойынша ғана шешім, сондай-ақ оң қорытынды қабылданған кезде қабылдануы мүмкін. Өзара тәуелділік жағдайында осы құрауыштарды орындау тәртібін бағалаушы шешеді. Бұл әдетте оң қорытындының қызметтің екі ішкі түрі де сәтті аяқталған кезде анықталуы мүмкін екендігін көрсетеді.

Сондықтан анықтау кезінде қызметтің кейбір ішкі түрінің басқа қызметтің ішкі түріне әсер ететінін, қызметтің осы ішкі түрінің қызметтің кез келген тәуелді ішкі түрін бағалаудың әлеуетті нәтижелеріне байланысты болатынын анықтау керек болады. Шындығында, қызметтің тәуелді ішкі түрінің өзінің қызметтің осы ішкі түріне бұрын аяқталған әрекеттерді қайтадан орындауын талап ете отырып, әсер етуі мүмкін.

Бағалаушы кемшіліктерді байқаған кезде, тәуелділікті алу кезінде елеулі маңызы болады. Егер кемшілік қызметтің тәуелді ішкі түрі бойынша оң қорытынды ол байланысты болатын қызметтің ішкі түріне жататын барлық кемшілікті жойғанша мүмкін болмайды.

А.3.4 Әрекеттер арасындағы тәуелділіктер

Бағалаушының бір әрекеті уақытында алынған нәтижелердің басқа әрекетті орындау кезінде пайдаланылуы мүмкін. Мысалы, толықтық және қарама-қайшы келмеуін талдау бойынша әрекеттер куәліктердің мазмұнын және ұсынылуын тексеру аяқталғанша бітпеуі мүмкін. Бұл мысалға ПП/ҚТ дәлелдеуге арналған бағалауды сол ПП/ҚТ бөліктерінің қайшы келмейтінін бағалаудан кейін ғана орындау керек екенін білдіреді.

А.4 Объектілерді аралау

А.4.1 Кіріспе

АЛС сенім санаты мынадай талаптарды қамтиды:

а) БО бүтіндігінің сақталуын қамтамасыз ететін пішін үйлесімін басқаруды қолдану;

б) БО арналған қауіпсіздік қорғауын қамтамасыз ететін және пайдаланушыға жеткізу кезінде қатерге ұшырамайтын БО қауіпсіз жеткізуге қатысты шаралар, процедуралар және стандарттар;

в) қоршаған ортаның дамуын күзетуді қорғауға арналған қауіпсіздік шаралары.

Әзірлеу объектілерін аралау – бағалаушының құжаттамадағы өз сипаттамасына қайшы келмейтін тәсілмен процедуралардың орындалуын анықтаудың пайдалы тәсілі.

Объектілерді мыналармен танысу үшін аралайды:

а) УК жоспарында суреттелгендей УК жүйесін пайдалану;

б) жеткізу туралы құжаттарда сипатталғандай жеткізу процедураларын іс жүзінде қолдану;

в) әзірлеу қауіпсіздігі жөніндегі құжаттамада сипатталғандай, БО әзірлеу және қолдау уақытында қауіпсіздік шараларын қолдану;

Нақты әрі толық ақпарат осындай аралау қарастырылатын жердегі қызмет түрлерінің операцияларында берілген:

а) УК жарамдылығы $ALC_CMC.n$ с $n \geq 3$ (әсіресе, жұмыс кезеңінде $ALC_CMC.3-10 = ALC_CMC.4-13 = ALC_CMC.5-19$);

б) ALC_DEL жеткізуі (әсіресе, жұмыс кезеңінде $ALC_DEL.1-2$);

в) әзірлеу қауіпсіздігі ALC_DVS (әсіресе, жұмыс кезеңінде $ALC_DVS.1-3 = ALC_DVS.2-4$).

А.4.2 Жалпы әдіс

Бағалау уақытында бағалаушының әзірлеушімен бірнеше жиі кездесуі қажет және әдеттегі тиімді жоспарлау мәселелерінің бірі – шығынды азайту үшін объектілерді бірлесе аралау. Мысалы, объектілерді әзірлеуші

қамтамасыз ететін пішін үйлесімдерін, қауіпсіздікті басқаруды және жеткізулердің орындалуын тексеру үшін аралаумен үйлестіруге болады. Сондай-ақ барлық әзірлеу сатысын тексеру үшін бір ғана объектіні бірнеше рет аралау қажет болуы ықтимал. Әзірлеудің бір аумақта немесе бірнеше жерде орналасқан бір ғимараттың бірнеше үй-жайларында өтуі мүмкін екенін ескеру керек.

Объектіні алғашқы аралауды бағалаудың ерте сатысында жоспарлау керек. БО әзірлеу сатысында басталатын бағалау үшін бұл қажет болған кезде түзетулер енгізуге мүмкіндік береді. БО әзірлеуді аяқтаған соң өткізілетін бағалау үшін ертерек аралау егер қолданылатын процедураларда күрделі дәлсіздіктер байқалатын болса, түзету бойынша шаралар қабылдауға мүмкіндік береді. Бұл бағалау кезінде артық күшті болдырмауға мүмкіндік береді.

Интервью сондай-ақ шын мәнінде не жасалатынын құжатталған процедуралардың бейнелейтінін анықтаудың пайдалы тәсілі болып табылады. Бағалаушы осы тәріздес интервью жүргізген кезде әзірлеу орнында талданатын процедураларды, олардың ұсынылатын бағалау куәліктеріне сәйкес іс жүзінде пайдаланылу және қолданылуын барынша терең түсінуге ұмтылуы қажет. Мұндай интервьюлер бағалау куәлігін зерттеуді толықтырады, бірақ алмастырмайды.

Объектіні аралауға дайындықтың бірінші операциясы бағалаушының объектіні аралау нәтижесін сипаттайтын аспектілерді қоспағанда, АЛС сенім санатына қатысты бағалауды орындауы болып табылады. Әзірлеушінің тиімді құжаттамасының ақпаратын және жауапсыз қалған мәселелерін негізге ала отырып, бағалаушылар объектілерді аралау арқылы шешілуге тиіс мәселелерді тексеру тізбесін жинайды.

АЛС санаты туралы бағалау есебінің бастапқы нұсқасы және тексерістер тізбесі бағалау жұмыстарының нұсқауына сәйкес объектілерді аралауға қатысты кеңеске арналған негіз ретінде қабылданады.

Тексерістер тізбесі объектілерді аралау, тиімді шараларды қарау кезінде жауабы табылуы мүмкін мәселелер, олардың қолданылуы және интервью арқылы жол көрсеткіш болып қолданылады. Іріктеу тиісті жерлерде сенімнің белгілі бір деңгейін қажет етеді (А қосымшасын қараңыз).

Объектілерді аралау нәтижелері жазылып алынады және АЛС сенім санаты туралы бағалау есебінің қорытынды нұсқасы үшін негіз ретінде қолданылады.

Онда балама сенім деңгейін білдіретін сенімділікке ие болу үшін басқа тәсілдерді қарастыру керек (мысалы, бағалау куәлігін талдау). Аралауды өзгерту туралы кез келген шешімді сертификаттау жөніндегі органмен кеңескеннен кейін қабылдау керек. Қауіпсіздіктің қолайлы критерийлері мен әдіснамасы Қауіпсіздік жөніндегі ақпараттық басқару жүйелерінің стандарттарына негізделеді.

А.4.3 Тексерістер тізбесін дайындауға арналған анықтамалық-бағдар

Төменде көрсетіліп анықталған түйінді сөздерді тексеріс уақытында тексеру керек.

А.4.3.1 Пішін үйлесімін басқару аспектілері

Негіз:

- БО, бастапқы код, орындаулар сериясы, жобалық құжаттама, ALC_CMC.3-8 әзірлеу жөніндегі нұсқауды қоса алғанда, пішін үйлесімдері тізбесінің тармақтары;

- жобалық құжаттаманы қостау, бастапқы код, БО әр түрлі нұсқалары бойынша пайдаланушының жол көрсеткіші;

- пішін үйлесімдері жүйесін жобалау және әзірлеу процесіне біріктіру, тесті жоспары, тестіні талдау және сапалық басқару процедуралары.

Тесті талдаулары:

- тесті жоспарларын қолдау және БО белгілі бір пішін үйлесімдері мен нұсқалары бойынша нәтижелер;

- қол жеткізу және тіркеуді бақылау жүйесі;

- қол жеткізу құқығын белгілі бір жобалық тағайындау немесе өзгерту жүйесі.

Рұқсатнама:

- БО қол жеткізу және клиенттерге арналған жол көрсету жүйесі;

- тарату алдында БО үшін және тестілеу және құптау құрауыштарына арналған жүйе.

А.4.3.2 Әзірлеудің қауіпсіздік аспектілері

Инфрақұрылым:

- әзірлеу объектілеріне қол жеткізуді жеке бақылауға арналған қауіпсіздік шаралары және аталған шараларды тиімді негіздеу.

Ұйымдастырушылық іс-шаралар:

- қоршаған ортаны дамыту қауіпсіздігіне қатысты ұйымдастырушылық құрылым;

- әзірлеу, өнім, тесті және сапа кепілдігі арасындағы ұйымдастырушылық сұрыптау.

Дербес іс-шаралар:

- әзірлеу қауіпсіздігіне қатысты жеке құрам құру жөніндегі шаралар;

- ішкі ақпаратты жария етпеу жөніндегі шаралар мен құқықтық келісімдер.

Қол жеткізуді бақылау:

- күзетілетін объектілерді тағайындау (мысалы, БО, бастапқы код, орындау сериялары, жобалық құжаттама, әзірлеу бойынша нұсқау, жол көрсеткіштер) және қауіпсіздік жүйелері;

- қол жеткізуді бақылау және идентификацияланған ақпаратты иеленуге қатысты жүйелер мен міндеттемелер;

- тіркеу деректерін әзірлеу және сақтау объектілеріне кез келген қол жеткізу түрін тіркеу жүйелері. Кіріс, жұмыс процестері мен шығыс деректер;
- шығару және шығару құрылғыларын қорғау бойынша қауіпсіздік шаралары (принтер, плоттер және дисплейлер);
- жергілікті және коммуникациялық байланысты қорғауды ұйымдастыру.

Құжаттарды сақтау, тапсыру және жою және деректер жиынтығы:

- құжаттар және деректерді қолдану жүйелері;
- бөлінген құжаттаманы жою және аталған оқиғаларды тіркеу жүйелері мен міндеттемелері.

Деректерді қорғау:

- деректер мен ақпараттарды қорғау жүйелері мен міндеттемелері (мысалы, резервтік көшірмелер).

Кездейсоқ жағдайдағы оқиғалар жоспары:

- кездейсоқ жағдайлар мен басқа міндеттемелерге жаттығу;
- қол жеткізуді бақылауға қатысты күтпеген жағдайдағы оқиғаларға қолданылатын шаралар бойынша құжаттар;
- төтенше жағдайлардағы қолданылатын жаттығулар туралы жеке құрамның ақпараты.

А.4.4 Бақылау кестесінің үлгісі

Объектілерді қарауға арналған бақылау кестелерінің үлгілері аудитті әзірлеуге арналған және аудит нәтижелерін ұсынуға арналған кестелерден тұрады.

Бақылау кестесінің осы құрылымы бағдарлаушы болып табылады. Жаңа нұсқаудың нақты мазмұнына байланысты өзгерістер талап етілуі мүмкін.

Бақылау кестесі үш тармақшадан тұрады және А.1 кестесінде берілген.

а) жүйенің пішін үйлесімін басқару;

А.1 кестесі – ДОБ 4 бойынша бақылау кестесінің үлгісі (үзінді)

А. Пішін үйлесімдерін басқару жүйелерін тестілеу (ALC_CMC.4 және ALC_CMS.4)					
№	Операция	Әзірлеуші құжаттамасы	Бағалау	Ескертулер мен сұрақтар	Нәтижесі
A.1	ALC_CM C.4- 11, ALC_CM C.4- 12	“Пішін үйлесімін басқару жүйесі”, ch.	Бастапқы кодтар файлдарын автоматты басқаратын, пайдаланушы пішіндерін басқаруға рұқсат беретін және рұқсат беру	Бастапқы код файлын оқу немесе жаңарту үшін түпнұсқалан дыру қажет пе?	Егер пайдаланушының құпия құжатқа рұқсат құқығы болмаса, бұл үшін ол тіпті файлдар тізімінде

			құқығымен сараланған, сондай-ақ пайдаланушыларды идентификациялау және түпнұсқаландыруды тексеру жүйесі.		бейнеленбейді.
...	...	...	...	...	...
В. Жеткізу ережелерін тестілеу (ALC_DEL.1)					
№.	Операция	Әзірлеуші құжаттамасы	Бағалау	Ескертулер мен сұрақтар	Нәтижесі
B.1	ALC_DEL.1-1, ALC_DEL.1-2	“БО жеткізу”, ch. ...	Программалық қамтамасыз етуге қол қойылған және PGP жүйесімен шифрленіп тұтынушыға берілді.	---	Бағалаушылар жеткізу процесін тексерді және оның сипаттауға сәйкестігі туралы қорытындыға келді, бақылау сомасы қосымша беріледі.
...	...	...	...	...	...
С. Әзірлеушінің ұйымдастырушылық және инфрақұрылымдық қауіпсіздігін тестілеу (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)					
№.	Операция	Әзірлеуші құжаттамасы	Бағалау	Ескертулер мен сұрақтар	Нәтижесі
C.1	ALC_DVS.1-1, ALC_DVS.1-2	“Әзірлеу ортасының қауіпсіздігі”, ch. ...	Ғимарат қауіпсіздік қоршауымен қорғалған	Қоршау жеткілікті күшті болып табылады ма?	Бағалаушылар қорғауды санап шықты.
...	...	...	...	...	...
С. Әзірлеушінің ұйымдастырушылық және инфрақұрылымдық қауіпсіздігін тестілеу (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)					
№.	Операция	Әзірлеуші құжаттамасы	Бағалау	Ескертулер мен сұрақтар	Нәтижесі
		(Бастапқы ережелер)		Ғимаратқа оңай кіруді болдырмас үшін биік?	Күшті және биік болу жеткілікті

C.2	ALC_DVS.1-1, ALC_DVS.1-2	“Әзірлеу ортасының қауіпсіздігі”, ch. ... (Ғимарат)	Ғимараттың мынадай қол жеткізу мүмкіндігі бар: қабылдау бөлмесі бақылайтын және жабық тұратын негізгі қол жеткізу, егер қабылдау бөлмесінде қызмет көрсетуші персонал болмаса. Және екі аунақты терезе қақпағымен қорғалатын тауарларды қабылдау бөлмесіне қол жеткізу.	Қол жеткізу мүмкіндіктерінің тізбесі толық болып табылады ма?	Аталған қол жеткізу мүмкіндіктерінен басқа, сыртынан ашылуы мүмкін емес апаттық шығу болады. Алдында айтылған аунақты терезе қақпақтары ішкі жағынан ғана басқарылады.
-----	-----------------------------	--	---	---	--

б) жеткізу ережесі;

в) әзірлеу барысында қауіпсіздік қамтамасыз ету шаралары.

Осы тармақшалар қолданыстағы ҚР СТ ИСО / МЭК 15408 ALC класына, әсіресе, (ALC_CMC).n n> = 3 кезінде пішін үйлесімдерін басқару топтарының мүмкіндіктеріне сәйкес келеді, (ALC_DEL) жеткізу және әзірлеу қауіпсіздігі (ALC_DVS).

Тармақшалар бұдан әрі осы стандартты бағалаудың тиісті белгілі бір операцияларына, жолдарға бөлінеді.

Бақылау кестесінің бағандарында өз кезегінде болады,

- тізбектік нөмірі;
- анықтамалық ақпарат болатын операциялар;
- әзірлеушінің тиісті құжаттамасына арналған сілтемелер;
- әзірлеушінің бағалауларын дәл жасауы;
- қарау кезінде анықталуға тиіс арнайы ескертулер мен мәселелер (бағалаушының аталған шараларды қолданудың дұрыстығын тексеруге беретін стандарттық тапсырмасынан басқа);
- қарау барысындағы тестілеу нәтижелері.

Егер аудит туралы баяндамалар әзірлену және ұсынуға арналған жеке бақылау кестелері болуы керек туралы шешім қабылданса, нәтижелер бағаны әзірлеу кестесінде көрсетілмейді, ал ескертулер мен мәселелер бағаны есеп

беру кестесінде көрсетілмейді. Қалған бағандар екі кестеде бірдей болуға тиіс.

А.5 Міндеттемелер сызбанұсқасы

Осы стандарт қадағалау органдары жүргізетін бағалауды орындауға тиіс минимальды техникалық жұмыстарды сипаттайды (жүйелер). Дегенмен, ол сондай-ақ, (тура және жанама) бағалау нәтижелерін екі жақты тануға байланысты болмайтын қызмет түрлері мен әдістерінің болатынын мойындайды. Айқындық және анықтық мақсатында және осы стандарттың қай жерде аяқталатынын және жеке жүйе әдіснамасының қай жерден басталатынын жақсырақ анықтау үшін мынадай мәселелер жүйенің қарауына қалдырылды. Жүйелер мыналарды көрсетті, дегенмен бір нәрсені көрсетпей кетуі мүмкін. (Осы кестенің толықтығын қамтамасыз ету үшін барлық күш жұмсалды; не осында, не осы стандартта аталмаған субъектімен соқтығысатын бағалаушылар субъектінің неліктен төмен түсетінін анықтау үшін олардың бағалау жүйесіне арналған анықтамаға жүгінуі керек).

Жүйе көрсете алатын мәселелер мынаны қамтиды:

а) жүргізілген бағалаудың жеткіліктілігін қамтамасыз ету үшін не талап етіледі - әрбір жүйенің техникалық біліктілікті верификациялау, жұмысты және оны бағалаушылар жұмысын түсіну, не бағалаушылар талаптарымен қадағалау органдарының бағалаушының жұмысын барлық бағалау органдарының барабарлығы мен салыстырмалылығы туралы жүйені куәландыратын қандай да бір басқа тәсілдермен қайта орындауын талап ете отырып, қадағалау органдарына табылған мәліметтерді ұсыну құралдары болады;

б) бағалауды аяқтаған кезде бағалау куәліктерін жою процесі;

в) кез келген құпиялылық талаптары (бағалаушы тарапынан және бағалау барысында алынатын ақпаратты жария етпеу);

г) бағалау барысында проблемамен соқтығысқан кезде қабылдануға тиіс әрекеттер тәртібі (бағалаудың проблема жойылғаннан кейін жалғасатынына немесе дерек аяқталатынына қарамастан, түзетілген өнім бағалау үшін қайта ұсынылуға тиіс);

д) құжаттама тапсырылуға тиіс кез келген ерекше (табиғи) тіл;

е) техникалық бағалау есебінде ұсынылуға тиіс кез келген жазылған куәліктер - осы стандарт техникалық бағалау есебінде есепке арналған минимумды анықтайды, алайда, жеке жүйелер қосымша ақпараттың қамтылуы талап етуі мүмкін;

ж) бағалаушылардан талап етілетін кез келген қосымша есептер (техникалық бағалау есебінен басқа), мысалы, тестілеу есептері;

и) жүйеде талап етілуі мүмкін қандай да бір нақты талаптар, оның ішінде құрылым, алушылар немесе осындай талаптардың кез келгені;

к) ҚТ бағалау нәтижесінде қандай да бір жазба есеп мазмұнының кез келген нақты құрылымы – жүйенің БО немесе ҚТ бағалауы сияқты бағалау

нәтижелерін толық сипаттайтын барлық өз есептері үшін белгілі бір пішіні болуы мүмкін;

л) ҚП/ҚТ идентификациялаудың кез келген қосымша ақпараты;

м) ҚТ-да анық қалыптасқан талаптардың жарамдылығын анықтауға арналған кез келген қызмет түрлері;

н) куәліктерді қайта бағалау және қайта пайдалануды қолдауда бағалаушы куәліктерін қамтамасыз етуге арналған кез келген талаптар;

о) жүйенің идентификаторлары, логотиптері, тауарлық белгілері және т.с.с. кез келген нақты өңдеуі;

п) криптографияға қатысты кез келген нақты нұсқау;

р) жүйені, ұлттық және халықаралық интерпретацияларды өңдеу және қолдану;

с) тестілеуге жол берілетін жерде, тестілеуге арналған жарамды балама тәсілдер тізбесі немесе сипаттамалары;

т) бағалау органы сол арқылы бағалаушының тестілеу кезінде қандай шаралар қолданғанын анықтай алатын механизм;

у) тестілеу үшін жоғары бағаланатын тәсіл (егер мұндайлар болса): ішкі интерфейс немесе сыртқы интерфейске;

ф) бағалаушының осалдық талдауын өткізуге қолданатын құралдарының тізбесі немесе құралдары (мысалы, кемшіліктер туралы жорамал әдіснамасы);

х) қаралуға тиіс қандай да бір осалдықтар немесе әлсіз орындар туралы мәліметтер.

Б қосымшасы
(ақпараттық)

Осалдықты бағалау (AVA)

Осы қосымшада AVA_VAN критерийлерінің түсінігі және оларды қолдану үлгілері болады. Осы қосымша AVA критерийлерін анықтамайды; бұл анықтайды ИСО / МЭК 15408-3 AVA класының тармақшасынан табуға болады:

Осалдықты бағалау.

Осы қосымша негізгі екі бөліктен тұрады:

а) осалдықты тәуелсіз талдауды аяқтау жөніндегі нұсқау. Б.1 тармақшасында қысқаша баяндалған және Б.2 тармақшасында барынша толық сипатталған. Осы тармақшалар бағалаушының осалдықтың тәуелсіз талдауын жасауға қалай келетінін сипаттайды;

б) қаскүнемнің болжанатын шабуыл әлеуетін қалай сипаттайтынын және пайдаланатынын. Сипаттау Б.3 - Б.5 тармақшаларында. Бұл тармақшаларда шабуыл әлеуетінің қалай сипатталатынын және пайдалануға тиіс екендігін суреттеу үлгісі болады, сондай-ақ үлгілер келтіріледі.

Б.1 Осалдықты талдау

Осалдықты бағалау мақсаты операциялық ортада БО кемшіліктері мен осал жерлерінің болуын және пайдалану мүмкіндігін анықтауды білдіреді. Осы тәуелсіз қорытынды бағалаушы өткізген талдауға негізделеді және бағалаушының тестілеуі қолдайды.

Бағалаушы осалдықты (AVA_VAN) талдаудың ең төменгі деңгейінде жай ғана БО қандай да бір белгілі осалдықтарды табу үшін қоғамдық қолжетімді ақпаратты іздеуді орындайды, бағалаушы барынша жоғары деңгейлерде БО бағалау куәліктерінің құрылымдық талдауын іске асырады.

Осалдық талдауын орындаған кезде негізгі үш фактор қолданылады, атап айтқанда:

а) әлеуетті осалдықтарды идентификациялау;

б) тәуелсіз қорытынды жасауға арналған бағалау, идентификацияланған әлеуетті осалдықтар қаскүнемнің тиісті әлеуетті шабуылмен функционалдық қауіпсіздік талаптарды бұзуына мүмкіндік бере ме;

в) тәуелсіз қорытынды жасау үшін енуді тестілеу, идентификацияланған әлеуетті осалдықтар БО операциялық ортасында пайдаланылатын болып табылады ма.

Осалдықтарды идентификациялау одан әрі қосымша іздеуге арналған куәліктер және әлеуетті осалдықтарды идентификациялау үшін осы куәліктерді іздеу қалай қиын болатынына бөлінуі мүмкін. Осыған ұқсас

тәртіпте енуді тестілеуді шабуылдау әдістерін идентификациялау және оларды көрсету үшін әлеуетті осалдықты талдауға бөлуге болады.

Осы негізгі факторлар, мәні бойынша, итеративті болып табылады, яғни әлеуетті осалдықтарды енуге тестілеу бұдан кейінгі әлеуетті осалдықтарды идентификациялауға әкелуі мүмкін. Осылайша, олар осалдықты бірыңғай талдау түрінде орындалады.

Б.2 Осалдыққа жасалатын талдауды бағалау әдісі

Б.2.1 Кіріспе

Осалдық талдауын бағалау әдісі қаскүнемнің негізгі (AVA_VAN.1 және AVA_VAN.2 үшін), негізгі жоғары (AVA_VAN.3 үшін), орташа (AVA_VAN.4 үшін) немесе жоғары (AVA_VAN.5 үшін) шабуыл әлеуетіне ие болатын шабуылмен енуіне БО орнықтылығын анықтауды білдіреді. Бағалаушы бірінші кезекте барлық идентификацияланған әлеуетті осалдықтарды пайдалану мүмкіндігін бағалайды. Бұған енуге тестілеуді өткізу арқылы қол жеткізіледі.

БО енуге әрекет жасаған кезде, бағалаушы негізгі (AVA_VAN.1 және AVA_VAN.2 үшін), негізгі жоғары (AVA_VAN.3 үшін), орташа (AVA_VAN.4 үшін) немесе жоғары (AVA_VAN.5 үшін) шабуыл әлеуетіне ие болатын қаскүнем рөлін өзіне алуы керек.

Бағалау әдісі бағалаушы бағалау бойынша басқа іс-шараларды өткізген кезде соқтығысатын әлеуетті осалдықтарды ескереді. БО осы әлеуетті осалдықтарға қарсылығын анықтайтын енуге арналған тестілеуді бағалау әдісі негізгі (AVA_VAN.1 және AVA_VAN.2 үшін), негізгі жоғары (AVA_VAN.3 үшін), орташа (AVA_VAN.4 үшін) немесе жоғары (AVA_VAN.5 үшін) шабуыл әлеуетіне ие болатын қаскүнемнің болжанатын рөлімен орындалуға тиіс.

Дегенмен, осалдық талдауы оқшауланған іс-шара өткізілмеуге тиіс. Ол ADV және AGD тығыз байланысты. Бағалаушы бағалау жөніндегі осы шараларды әлеуетті осалдықтарды немесе «проблемалық салаларды» анықтауда тоғыстырумен орындайды. Осылайша, бағалаушының жалпы осалдық нұсқауын (B.2.1 тармақшасында) білуі міндетті.

Б.2.2 Жалпы осалдық нұсқауы

Келесі бес санатта жалпы осалдықтар мәселесін қарастыру болады.

Б.2.2.1 Аралау

Аралау бұзушының мынадай жолдармен қауіпсіздік шараларын іске асыруды болдырмауының кез келген тәсілін қамтиды:

а) БО интерфейстерінің мүмкіндіктерін немесе БО өзара әрекет етуі мүмкін утилитін пайдалану;

б) керісінше тыйым салынуға тиіс артықшылықтар немесе басқа мүмкіндіктерді мұрағаттау;

в) (құпиялылық маңызды болған кезде) жеткіліксіз қорғалған салаларда

сақталатын немесе көшірмеленетін сезімтал деректерді оқу.

Бағалаушы орындайтын осалдықтарды тәуелсіз талдау барысында мынадай аспектілердің әрқайсысын қарастыру керек (бұл орынды болған кезде):

а) БО интерфейстерінің мүмкіндіктерін немесе утилитті, әдетте, осы интерфейстер үшін талап етілетін қауіпсіздік шараларын болдырмау мақсатында пайдаланады. Мысалы, қол жеткізуді басқарумен іске асырылатынға қарағанда, барынша төменгі деңгейде жүзеге асырылатын функционалдық мүмкіндіктерге рұқсат алу. Ықтимал нұсқалар қамтиды:

- 1) функцияны шақырудың алдын ала анықталған тізбектілігін өзгерту;
- 2) қосымша функцияны орындау;
- 3) алдын ала байқалмаған контексте немесе алдын ала болжанбаған мақсатпен кейбір құрауышты пайдалану;
- 4) азырақ абстрактілі көрсетулерде ұсынылатын жүзеге асыру нақтылауларын пайдалану;
- 5) қол жеткізуді тексеру уақыты мен пайдалану уақыты арасындағы кідірісті пайдалану.

б) функцияны шақырудың алдын ала анықталған тізбектілігін өзгертуді кейбір қауіпсіздік функциясын орындау үшін БО интерфейстерін (мысалы, пайдаланушы командасы) шақырудың қарастырылған тәртібі болатын кезде қарау керек (мысалы, қол жеткізу үшін файлды ашу және одан кейін ондағы деректерді оқу). Егер қауіпсіздік функциясы БО интерфейстерінің бірінде шақырылатын болса (мысалы, қол жеткізуді басқаруды тексеру), онда бағалаушының тізбектіліктің барынша кешірек нүктесінде тиісті шақыруды орындау немесе оны тұтасымен өткізу арқылы қауіпсіздік функцияларын аралауы мүмкін екенін қарастыруы керек;

в) қосымша құрауышты орындау (алдын ала анықталған тізбектілікте) жаңа ғана сипатталғанға ұқсас шабуыл формасы болып табылады, бірақ тізбектіліктің кейбір нүктесінде БО кейбір басқа интерфейсін шақыруды қамтиды. Ол сондай-ақ желілік трафик талдауыштарын пайдалану арқылы сезімтал деректер желісі бойынша берілетін қамтуға негізделген шабуылды да қамтуы мүмкін (мұнда қосымша құрауыш желілік трафиктің талдауышы болып табылады);

г) алдын ала байқалмаған контексте немесе алдын ала болжанбаған мақсатпен кейбір құрауышты пайдалану оны ол үшін жоспарланбаған немесе алдын ала анықталмаған мақсатқа қол жеткізу үшін пайдалана отырып, БО интерфейсінің ісіне қатысы болмайтын қауіпсіздік функцияларын аралау үшін пайдалануды қамтиды. Жабық арналар осы типті шабуыл үлгісі болып табылады. Сондай-ақ құжатталмаған интерфейстерді пайдалану (қауіпсіз болуы мүмкін) осы санатқа түседі (қолдау және көмек беру бойынша құжатталмаған мүмкіндіктерді қоса алғанда);

- д) азырақ абстрактілі көрсетулерде ұсынылатын жүзеге асыру

нақтылауларын пайдалану тағы да бұзушының процесті жетілдіру салдары ретінде (мысалы, жабық арна ретінде «бұғаттаудың» ауыспалы типін пайдалану) БО ұсынылатын қосымша функциялар, ресурстар немесе атрибуттарды өз мақсатына пайдалануы арқылы жабық арналарды пайдалануды қамтиды. Сондай-ақ қосымша функционалдық мүмкіндіктер БО модульдерінде болатын кодтың тесті фрагменттерімен қамтамасыз етіле алады;

е) қол жеткізуді тексеру уақыты мен пайдалану уақыты арасындағы кідірісті пайдалану қол жеткізуді тексеру орындалатын және қол жеткізу ұсынылатын сценарийді қамтиды, ал бұзушы осының салдарынан қол жеткізуді тексеруді орындаған уақытта болуы мүмкін қол жеткізуді тексеру жаңылысы кезінде жағдай жасауға жарамды. Пайдаланушы терминалына жоғары сезімтал деректерді жіберу және оқуға арналған фондық процесті тудыратын және содан соң жүйеден шығуды және жүйеге сезгіштіктің барынша төменгі деңгейінде кіруді іске асыратын пайдаланушы үлгі болып табылады. Егер фондық процесс пайдаланушы жүйеден шыққан кезде аяқталмаса, онда қол жеткізуді мандатты басқаруға сәйкес тексеру шын мәнінде аралап өтілуі мүмкін;

ж) артықшылықтарды мұрағаттауға негізделген шабуылдар негізінен артықшылықтарды немесе кейбір артықтау БЖ құраушышының мүмкіндіктерін заңсыз иелену, әдетте, одан бақыланбайтын немесе қарастырылмайтын тәсілмен шығу жолымен негізделеді. Ықтимал нұсқалар қамтиды:

1) деректерді орындау үшін тағайындалмаған немесе орындау үшін ықтимал түрлендіруді орындау;

2) кейбір құрауыш үшін қарастырылмаған бастапқы деректерді өндіру;

3) барынша төменгі деңгейдегі құрауыштар болжанатын болжамдар мен қасиеттердің бұзылуы;

и) орындау үшін тағайындалмаған деректерді орындау немесе оларды орындау үшін ықтимал түрлендіру вирустарды пайдаланып шабуылдауды қамтиды (мысалы, кейбір файлға орындалатын коды немесе файлдың иесінде болатын артықшылықтарды осылайша мұрағаттай отырып, қол жеткізуді алу немесе осы файлды редакциялау кезінде автоматты түрде орындалатын командаларды орналастыру);

к) кейбір құрауыш үшін қарастырылмаған деректерді өндіру бұзушының пайдалануы мүмкін алдын ала қарастырылмаған нәтижелерге әкелуі ықтимал. Мысалы, егер БО базалық операциялық жүйеге пайдаланушы рұқсат алатын кезде айналып кетуге болатын қауіпсіздік функцияларын жүзеге асыратын қосымша болып табылатын болса, онда пароль идентификацияланғанша түрлі басқарулар немесе *escape*-тізбектіліктерді енгізу нәтижелерін зерттей отырып, кіру жүйелілігін орындаған соң бірден осындай рұқсатты алу мүмкін болуы ықтимал;

л) барынша төменгі деңгейдегі құрауыштар болжанатын болжамдар мен қасиеттердің бұзылуы қосымшада жүзеге асырылатын қауіпсіздік функцияларын айналып өту үшін базалық операциялық жүйеге рұқсат алу үшін қосымшада шектеулер қолданылатындығынан шығуға негізделген шабуылдарды қамтиды. Мұндай жағдайда бұзылатын болжам қосымшаны пайдаланушының мұндай рұқсатты алуы мүмкін еместігін білдіреді. Осы тәріздес шабуылды, егер деректер базасын басқару жүйесінің басқаруында жұмыс істейтін қосымшамен қауіпсіздік функциясы жүзеге асырылатын болса алдын ала болжауға болады: егер бұзушы қосымша шектеулері әсерінен шыға алатын болса, тағы да қауіпсіздік функцияларын айналып өту мүмкіндігі бар;

м) жеткіліксіз қорғалған аумақта сақталған сезімтал деректерді оқуға негізделген шабуылдар (құпиялылық маңызды болғанда қолданылатын) сезімтал деректерге рұқсат алудың ықтимал тәсілдерін қарастыруға тиіс мынадай мәселелерді қамтиды:

- 1) дискіде «қоқысты» жинау;
- 2) қорғалмаған жадыға қол жеткізу;
- 3) жазбалар бойынша бірге пайдаланылатын файлдарға немесе бірге пайдаланылатын басқа ресурстарға (мысалы, басқылау файлдарына) қол жеткізуді пайдалану;
- 4) пайдаланушылардың қандай қол жеткізуді алатынын анықтау үшін қателерден кейін қалпына келтіруді жандандыру. Мысалы, істен шыққаннан кейін тақырыпсыз файлдар үшін файлдарды автоматты қалпына келтіру жүйесі дискіде таңбасыз болуы мүмкін жоғалған және табылған файлдарға арналған каталогты пайдалануы мүмкін. Егер БО қол жеткізуді мандатпен басқаруды жүзеге асыратын болса, онда осы каталог үшін қандай қауіпсіздік деңгейі сақталатынын (мысалы, жоғары жүйелік) және осы каталогқа кімнің қол жеткізе алатынын зерттеу маңызды.

Бағалаушы негізгі екі техниканы қоса отырып, «құпия кіруді» идентификациялай алатын бірнеше түрлі әдістер болады. Біріншісі, бағалаушы дұрыс пайдаланылмауы мүмкін интерфейсті тестілеу кезеңінде абайсызда идентификациялаған кезде. Екіншісі, құжатталған интерфейстерді тестілеу бөліктері болып аталмайтын кез келген модульді идентификациялауға арналған жөндеу тәсілімен ОФҚ сыртқы әрбір интерфейсін тестілеу және содан соң «құпия шығу» болып саналмайтын кодты тексеру арқылы.

Б.2.2.2 Қол сұғу

Қол сұғу бұзушының қауіпсіздік функциясын немесе механизмін орындау режиміне әсер етуге негізделген кез келген шабуылды қамтиды (яғни, бұрмалау немесе бұғаттау), мысалы мынадай жолдармен:

- а) деректерге, қауіпсіздік функциясы немесе механизмі болжанатын құпиялылық немесе бүтіндікке қол жеткізу;

б) БО әдеттегіден тыс немесе қарастырылмаған жағдайда қолдануға мәжбүрлеу;

в) қауіпсіздікті қамтамасыз етуді сөндіру немесе кідірту;

г) БО физикалық модификациясы.

Бағалаушының осалдықты тәуелсіз талдау барысында мынадай аспектілердің әрқайсысын қарастыруы керек (бұл орынды болған кезде):

а) деректерге, қауіпсіздік функциясы немесе механизмі болжанатын құпиялылық немесе бүтіндікке қол жеткізуге негізделген шабуылдар мынаны қамтиды:

1) ішкі деректер модификациясын тікелей немесе жанама оқу;

2) алдын ала байқалмаған контексте немесе алдын ала болжанбаған мақсатпен кейбір құрауышты пайдалану;

3) абстракцияның барынша жоғарғы деңгейінде көрінбейтін құрауыштардың өзара әсерін пайдалану.

б) қарастырылуы керек шабуылдардың мынадай типтерін тікелей немесе жанама қамтитын ішкі деректерді оқу, жазу немесе түрлендіру:

1) пайдаланушылардың паролі сияқты БО ішінде сақталатын «құпияларды» оқу;

2) қауіпсіздікті қамтамасыз ететін механизмдер болжанатын ішкі деректерді ауыстыру;

3) пішін үйлесімі файлдарында немесе уақытша файлдарда ауыспалы ортаны (мысалы, логикалық атаулар) немесе деректерді өзгерту;

в) әдеттегі жағдайда рұқсат алынбаған қорғалған файлды түрлендіруге арналған сенімді процесті алдауы мүмкін болуы ықтимал;

г) бағалаушының сондай-ақ мынадай «қауіпті сипаттамаларды» қарастыруы қажет:

1) БО үнемі қолда болатын құрастырушымен бірге болатын бастапқы мәтіні (мысалы, жүйеге кірумен байланысты бастапқы кодты өзгерту мүмкін болуы ықтимал);

2) интерактивті жөндеуші және өзгерістер енгізу құралдары (мысалы, орындалатын бейнені өзгерту мүмкін болуы ықтимал);

3) файлды қорғау болмайтын құрылғылар контроллері деңгейінде өзгерістер енгізу мүмкіндігі;

4) бастапқы кодта болатын және опционалды қамтылуы мүмкін диагностикалық код;

5) БО қалдырылған әзірлеушінің аспаптық құралдары;

д) алдын ала байқалмаған контексте немесе алдын ала болжанбаған мақсатпен кейбір құрауышты пайдалану (мысалы) БО операциялық жүйеге сүйенетін қосымша болып табылатын, ал пайдаланушылар өздерінің меншікті командалық файлдарын (мысалы, көп артықшылыққа ие болу үшін) өзгерту үшін мәтіндік процессор немесе басқа редактордың пакетінің білімін пайдаланатын кездегі жағдай болып табылады;

е) абстракцияның барынша жоғары деңгейінде көрінбейтін құрауыштардың өзара әсерін пайдалану ресурсты бір құрауышпен түрлендірген кезде басқа (сенім білдірілген) құрауышты орындау режиміне әсер етуі мүмкін ресурстарға бірге қол жеткізуді пайдаланатын шабуылды қамтиды, мысалы, бастапқы код деңгейінде бірге пайдаланылатын жады немесе семафорлар сияқты жанама деректер немесе жалпы деректерді пайдалану арқылы;

ж) әдеттегі немесе қарастырылмаған жағдайда БО қолдануға мәжбүрлеуге негізделген шабуылдарды әрқашан ескеру қажет. Ықтимал нұсқалар қамтиды:

1) кейбір құрауыш үшін қарастырылмаған бастапқы деректерді өндіру;

2) барынша төмен деңгейдегі құрауыштар жобаланатын болжамдар мен қасиеттердің бұзылуы;

и) құрауыш үшін қарастырылмаған бастапқы деректерді өндіру орны болатын кезде БО қолданылу режимін зерттеуді қамтиды:

1) командаларды енгізу буферінің аса толып кетуі («ағынның бұзылуы» мүмкін немесе бұзушы өз мүддесіне пайдалануға жарамды басқа сақтау саласын қайта жазу немесе парольдердің ашық мәтіні сияқты сезімтал ақпарат болуы мүмкін апаттық дампаны мәжбүрлі беру);

2) дұрыс емес командалар немесе параметрлерді енгізу (осы параметр арқылы деректер берілуін болжайтын интерфейс үшін «тек қана оқуға арналған» жағдайға параметрді орнатуды қоса алғанда);

3) файл соңына маркерді (мысалы, CTRL/Z немесе CTRL/D) немесе аудит журналына нөлдік символды қою;

к) барынша төмен деңгейдегі құрауыштар жобаланатын болжамдар мен қасиеттердің бұзылуы қауіпсіздікке қатысты деректер нақты форматта болатын немесе мәндерінің нақты ауқымдары болады деп болжанатын (анық немесе анық емес) жерде бастапқы кодта қателерді пайдаланатын шабуылдарды қамтиды. Бағалаушы мұндай жағдайларда деректерді басқа форматта қалыптастыра отырып немесе оларға басқа мәндер бере отырып, шабуылдардың осындай болжамдарға әкелетіні туралы және егер осылай болса, онда оның бұзушыға артықшылық беретіні қорытынды жасауға тиіс;

л) қауіпсіздік функцияларын дұрыс орындау режимі ресурстардың лимиті таусылатын немесе параметрлер өзінің максималды мәніне жеткен кезде ауыспалы жағдайлар кезінде бұзылатын болжамдарға байланысты болуы мүмкін. Бағалаушы осы шектерге қол жеткен кезде БО қолданылу режимін қарастыруы керек (егер бұл мақсатқа сәйкес болса), мысалы:

1) күндерін өзгерту (мысалы, БО ауыспалы шек күніне өтуі кезінде өзін қалай ұстайтынын зерттеу);

2) дискілердің өте толып кетуі;

3) пайдаланушылардың максималды санының артуы;

4) аудит журналын толтыру;

5) аспаға берілетін қауіпсіздік сигналдарының кезегінің өте толып кетуі;
6) байланыс құрауыштарына қатты байланысты болатын көп пайдаланылатын БО түрлі бөліктерінің шамадан артық жүгі;

7) желі немесе жеке түйіндерге трафик орнату;

8) буфер немесе өрістерді толтыру.

м) қауіпсіздікпен қамтамасыз етуді ажырату немесе кідіртуге негізделген шабуылдар мынадай аспектілерді қамтиды:

1) операцияның жүйелі орындалуын бұзу үшін кесте құру функцияларын немесе үзулерді пайдалану;

2) параллель орындау кезіндегі бұзулар;

3) абстракцияның барынша жоғарғы деңгейінде көрінбейтін құрауыштар арасындағы өзара әсерді пайдалану.

Операцияның жүйелі орындалуын бұзу үшін кесте құру функцияларын немесе үзулерді пайдалану мынадай кезде БО қолдану режимін зерттеуді қамтиды:

1) команданың үзілуі (CTRL/C, CTRL/ Y бойынша және т.с.с.);

2) алғашқысы танылғанға дейін екінші үзу туындағанда.

н) қауіпсіздік үшін ауыспалы процестерді аяқтау нәтижелерін зерттеу қажет (мысалы, аудит демоны). Осыған ұқсас, олардың әкімгер үшін пайдасыз болатынынан сақтандыратын сигналдарды беру/алу немесе аудит жазбаларын тіркеуді осындай кідірту болуы мүмкін (шабуыл мақсатқа ендігі қол жеткізетін сияқты).

о) параллель орындаудағы бұзулар екі немесе одан көп субъекті бір мезгілде қол жеткізуге алдын ала әрекет жасайтын кезде БО қолданылу режимін зерттеуді қамтиды. Мүмкін, БО екі субъекті бір мезгілде қол жеткізуге әрекет жасайтын кезде қажетті бұғаттауды орындап шығуы мүмкін, бірақ мұндайда оның тәртібі қосымша субъектілер болған кезде толық анықталмаған болып табылады. Мысалы, қауіпсіздігі бойынша сыни процесс егер екі басқа процесс оған қажетті ресурсқа қол жеткізуді іске асыратын болса, ресурсты алуды күту жағдайына ауыстырылуы мүмкін.

п) абстракцияның барынша жоғарғы деңгейінде көрінбейтін құрауыштар арасындағы өзара әсерді пайдалану сенім білдірілген процесс уақытында ауыспалы кідірту тәсілін қамтамасыз етуі мүмкін.

р) физикалық шабуылдар физикалық зерттеу, физикалық манипуляция, физикалық түрлендіру және орын ауыстыру болып бөлінуі ықтимал:

1) БО-ның мақсатты сапасы туындаған кездегі физикалық зерттеу, мысалы, ішкі коммуникациялық интерфейстерде, желілер немесе жадыларда оқу;

2) физикалық манипуляция БО ішкі түрлендіруіне (мысалы, өзара әрекет ету процесі ретінде оптикалық қателік индукциясын пайдаланған кезде), БО сыртқы интерфейстеріне (мысалы, сағаттардың қуаттылығы немесе дәлсіздігі кезінде) және БО ортасына (мысалы, температураны өлшеген кезде)

бағытталған БО ішкі сапалары болуы мүмкін;

3) жеткізу кезеңінде немесе БО операциясында БО басқа АТ объектісімен ауыстыруға арналған физикалық ауыстыру. БО жеткізу уақытында әзірлеу ортасынан пайдаланушыға дейін орнын ауыстыру қауіпсіз жеткізу процедураларын қолдану арқылы алды алынуға тиіс (Әзірлеу қауіпсіздігімен (ALC_DVS) қарастырылатындар сияқты). БО-ның операция уақытында орнын ауыстыру пайдаланушының олардың БО-мен өзара әрекет ететініне сенімді болуы үшін, пайдаланушы нұсқауы мен операциялық ортаның қиыстыруы кезінде қарастырылуы мүмкін.

Б.2.2.3 Тура шабуылдар

Тура шабуыл қауіпсіздік функциясының мәлімделген минимальды орнықтылығымен растау немесе теріске шығару үшін қажетті кез келген ену тестілерін идентификациялауды қамтиды.

Мысалы, сандардың жалған кездейсоқ генераторының ерекше орындауының қауіпсіздік механизмін іріктеу үшін қажетті энтропиясы болады деген болжам дұрыс болмауы мүмкін.

Ықтималдылық немесе қайта орнатылатын механизм қауіпсіздіктің атрибутты мәнін іріктеуге (мысалы, пароль өлшемін таңдау) немесе пайдаланушы-адамның күнін енгізуге (мысалы, парольді таңдау) негізделетін жерде жасалған болжамдар нашар жағдайды көрсетуге тиіс.

Ықтималдылық немесе қайта орнатылатын механизмдер қызметтің осы ішкі түрінің енгізу деректері ретінде талап етілетін бағалау куәліктерін зерттеу уақытында идентификациялануға тиіс (қауіпсіздік мақсаты, функционалдық сипаттізім, жоғары деңгейлі жоба, орындауды көрсететін ішкі топ) және басқа БО құжаттамалары (мысалы, нұсқау) қосымша ықтималдылықтарды немесе қайта орнатылатын механизмдерді идентификациялауы мүмкін.

Жоба куәлігі немесе нұсқау бекіту немесе болжауды қамтитын кезде (мысалы, минутына қанша тану әрекеттері мүмкін болатыны туралы), бағалаушы олардың дұрыс екендігін тәуелсіз растауға тиіс. Бұған тестілеу арқылы немесе тәуелсіз талдау арқылы қол жеткізілуі мүмкін.

Криптографиялық алгоритмдегі кемшіліктерге байланысты болатын тура шабуылдар олар ИСО/МК 15408 қолданылу саласы шегінде болатындықтан, Осалдықты талдауда (AVA_VAN) қарастырылмауы керек. Криптографиялық алгоритмді дұрыс орындау ADV және ATE қызметі уақытында қарастырылады.

Б.2.2.4 Мониторинг

Ақпарат объектінің қасиеттері арасындағы абстрактілі ұғым болып табылады, яғни, егер БО осы сигналға әрекет етуге жарамды болса, сигналда жүйеге арналған ақпарат болады. БО пайдаланушы деректерімен ұсынылатын ақпаратты жабдықтайды, өңдейді және сақтайды. Сондықтан:

а) ақпарат пайдаланушы деректерімен бірге БО шегінде немесе БО экспортынан берілу арқылы субъектілер арасында өтуі мүмкін;

б) ақпарат өндірілуі және пайдаланушының басқа деректерімен берілуі мүмкін;

в) ақпарат оны білдіретін деректермен бірге операция мониторингі арқылы алынуы мүмкін.

Операцияны деректермен бақылау үшін пайдаланушы деректерімен ұсынылатын ақпарат мынадай қауіпсіздік атрибуттарымен сипатталуы мүмкін, мысалы, құпия емес, құпия, жасырын, аса құпия ретіндегі мәндері болатын «құпиялылық деңгейі» болуы мүмкін. Осы ақпарат және қауіпсіздік атрибуттарын операциялар өзгертуі мүмкін, мысалы FDP_ACC.2 «тазалық сақтау» арқылы деңгейін азайтып немесе деректерді үйлестіру арқылы деңгейін арттырып сипаттай алады. Бұл бақыланатын субъектілердің бақыланатын объектілермен болатын бақыланатын операциясына бағытталатын ақпарат ағынын талдау аспектілерінің бірі.

Рұқсат етілмеген ақпарат ағынын талдау басқа аспекті болып табылады. Бұл аспекті FDP_ACC тобына жіберілетін пайдаланушы деректері болатын объектілерге тура қол жеткізуден гөрі барынша ортақ болып табылады. Ақпарат ағынымен басқару саясатының бақылауымен ақпаратты тасымалдайтын еріксіз сигналдық арна сондай-ақ осы ақпарат болатын немесе онымен байланысты кез келген объектіні (мысалы, қапталдас арналар) өңдеу мониторингі арқылы шақырылуы мүмкін. Еріксіз сигналдық арналар осындай манипуляцияны қадағалайтын субъектілер немесе пайдаланушыны манипуляциялау ресурстары арқылы идентификациялануы мүмкін. Классикалық жабық арналар ресурсты түрлендіру немесе модульдеуге сәйкес уақытша немесе жадысы болатын арналармен идентификацияланған болатын. Басқа шабуылдар мониторингіне келетін болсақ, БО пайдалану функционалдық қауіпсіздік талаптарына сәйкес іске асырылады.

Жабық арналар, әдеттегідей, БО-ның қадағалауы және көп деңгейлі бөлу саясатының талаптары болған кезде қолданылады. Жабық арналар осалдықты талдау және жобалық іс-шаралар барысында жүйелі байқалуы мүмкін және сондықтан тестілеуге түсуі керек. Дегенмен, жалпы алғанда, осындай шабуылдар мониторингі «жабық арналарды талдау» деген жалпылама атаумен аталатын мамандандырылған талдау әдістері арқылы ғана идентификацияланады. Бұл әдістер бірнеше зерттеуге түскен, сондай-ақ осы мәселе бойынша жарияланған көптеген мақалалар бар.

Жабық арналарға талдау жүргізуге арналған нұсқау бағалау органдарынан талап етілуге тиіс.

Еріксіз ақпарат ағынын шабуылдау мониторингі жетекші құжаттарға сәйкес келетін БО басқару арқылы БО сезімтал ішкі деректерін ашуға бағытталатын пассивті талдау әдістерін қамтиды.

Қапталдас арна талдауы БО физикалық кемуіне негізделген талдамалық тереңдету әдістерін қамтиды. Физикалық кему уақытша ақпарат, электр энергиясын тұтыну және ОФҚ есептеген кезде энергияның сәулеленуінен болуынан болуы мүмкін. Уақытша ақпаратты сондай-ақ қаскүнем қашықтан алуы мүмкін (БО желілік рұқсаты болатын), энергияға негізделген ақпараттық арналар қаскүнемнің БО жақын ортада болғанын талап етеді.

Тыңдау әдістері энергияның барлық түрін қамтиды, мысалы, компьютерлік дисплейлердің электр магниттік немесе оптикалық сәулеленулері, БО жақын өрісінде болуы міндетті емес.

Мониторинг сондай-ақ хаттамалар ағынының пайдаланылуын қамтиды, мысалы, қорғалған сокеттер хаттамасын жүзеге асыруға арналған шабуыл.

Б.2.2.5 Дұрыс қолданбау

Дұрыс қолданбау мыналардан пайда болуы мүмкін:

- а) жетекші құжаттаманың толық болмауы;
- б) негізделмеген нұсқау;
- в) БО пішін үйлесіндегі абайсыз қателер;
- г) БО қолдану режимін еріксіз болдырмау.

Егер жетекші құжаттама толық болып табылмаса, пайдаланушының БО функционалдық қауіпсіздік талаптарына сәйкес қалай басқарылатынын білмеуі мүмкін. Бағалаушы нұсқаудың толық екендігін анықтауға арналған бағалау бойынша басқа іс-шаралар өткізген кезде алынатын БО білімін қолдануға тиіс. Атап айтқанда, бағалаушы функционалдық сипаттізімді ескеруі керек. Осы құжатта сипатталатын ОФҚ талап етілетіндей, қауіпсіз басқаруға рұқсат беру үшін және пайдаланушылар үшін қолжетімді ОФҚИ арқылы пайдалану үшін нұсқауда сипатталған. Одан басқа, әр түрлі жұмыс әдістері барлық жұмыс әдістері бойынша нұсқау ұсынылуын қамтамасыз ету үшін ескерілуге тиіс.

Бағалаушы көмек ретінде нұсқау және осы құжаттар арасындағы бейресми құрылымды дайындауы мүмкін. Осы құрылымдағы кез келген жетіспеушілік толық болмайтыны туралы куәландыра алады.

Нұсқау егер ол ҚТ-мен үйлеспейтін немесе қауіпсіздікті сақтау үшін шектен тыс қиындық келтіретін болып табылатын БО пайдалануды немесе операциялық ортаны талап ететін болса, негізделмеген болып саналады.

БО тұтынушыға осы БО функционалдық қауіпсіздік талаптарына сәйкес тиімді пайдалануға және пішін үйлесімінде абайсыздықтан болатын қателерді болдырмауға көмек көрсету үшін түрлі жолдарды пайдалануы мүмкін. БО тұтынушыны басқа БО барынша тиімді қауіпсіздік функциялары болатын пайдалануға қатысты ұсынымдар, еске түсірулер, процедуралар және т.с.с. болатын кеңейтілген нұсқаумен жеткізілуі мүмкін уақытта БО функционалдық қауіпсіздік талаптарымен үйлеспейтін жағдайда болатын кезін ескертуі үшін функцияны (функцияларды) пайдалана алады, мысалы, функционалдық қауіпсіздік талаптарының мәні болмайтын, яғни қауіпсіз

болмайтын кезін байқауға арналған қосалқы құрал ретінде айдит функциясын пайдалану жөніндегі нұсқау.

Бағалаушы нұсқауды пайдаланудың қорғалмаған күйге өтуін уақытылы байқауға мүмкіндік беруін күтудің дұрыс негізі болатыны туралы операциялық орта тұжырым жасауы үшін БО іс-қимылын, оның тағайындалымы мен қауіпсіздік мақсаттарын ескеруге тиіс.

БО қорғалмаған күйге ену әлеуеті жиынтықтаушы бағалау торабы арқылы анықталуы мүмкін, мысалы, БО арналған кепілдік ретінде пакетке қосылатын құрауыштарға арналған дәлелдер ретінде кез келген басқа жобаны, ҚТ және функционалдық сипаттізімді ұсыну (мысалы, егер БО (ADV_TDS) жобасының бір құрауышы қамтылса, БО/ОФҚ жобасының сипаттізімі).

ОФҚ қолдану режимін еріксіз болдырмау жағдайы қамтуы мүмкін, бірақ мыналармен шектелмейді:

а) іске қосу, жабу немесе қалпына келтіру қатесін жандандыру кезінде БО қолдану режимі;

б) Төтенше жағдайлардағы БО қолдану режимі (кейде асқын жүктеу немесе асимптомды қолдану режимі деп аталады), әсіресе, бұл ОФҚ бөліктерінің белсендірмейтін немесе сөндіретін жерде;

в) пішін үйлесіміндегі абайсыздықтан болатын қатенің кез келген әлеуеті немесе жоғарыдағы тармақшада әсер туралы белгіленген шабуылдармен байланысты қауіпсіз емес пайдалану.

Б.2.3 Әлеуетті осалдықтарды идентификациялау

Бағалаушы әлеуетті осалдықты түрлі іс-шаралар барысында идентификациялауы мүмкін. Олар бағалау барысында анық болуы мүмкін, не олар осалдықты іздеуге арналған деректерді талдау нәтижесінде идентификациялануы мүмкін.

Б.2.3.1 Осалдықтарды қарсы идентификациялау

Осалдықтардың қарсы идентификациясын бағалаушы әлеуетті осалдықтар болатын жерде бағалау жүргізген кезде анықтайды, яғни дәлелдеулер әлеуетті осалдықтарды анықтаудың белгілі бір мақсатымен талданбайды.

Қарсы идентификациялау әдісі бағалаушының бағалау органы бақылайтын тәжірибесі мен біліміне байланысты болады. Бұл тәсілде жасалмайды, бірақ әлеуетті осалдықтар есебінен жасалатын тұжырымдардың қайталануын қамтамасыз ету үшін құжатталатын болады.

Осы әдіс үшін ресми талдау критерийі болмайды. Әлеуетті осалдықтар куәліктен білімі мен тәжірибесінің нәтижесі ретінде идентификацияланады. Алайда, осы идентификациялау тәсілі куәліктердің қандай да нақты ішжиынымен шектелмейді.

Бағалаушының, болжанғандай, жалпы қолжетімді көздерде құжатталған сияқты БО типтерінің әдістері мен қауіпсіздігіндегі белгілі кемшіліктер

жиынтығын білуі керек. Білім деңгейі БО типіне қатысы болатын электронды пошта қауіпсіздігі тізімінен алынуы мүмкін, кеңінен пайдаланылатын өнімдер мен технологияларда қауіпсіздік проблемаларын зерттейтін ұйымдар жариялайтын жүйелі бюллетеньдерден (бұзылғандық, осалдықтар тізімі және қауіпсіздік кемшіліктері) тұрады.

Бұл ақпарат AVA_VAN.1 немесе AVA_VAN.2 үшін университеттік зерттеулер арқылы алынған нақты конференция немесе нақтылы тезистерге дейін кеңейтілмейді. Сонымен бірге, білімді қолдану қазіргі заманға сай екенін қамтамасыз ету үшін бағалаушыға жалпы қолжетімді көздер материалдарын іздеуді орындауға тура келеді.

AVA_VAN.3 үшін AVA_VAN.5 арналған қоғамдық қолжетімді ақпаратты іздеу университеттер мен басқа тиісті ұйымдардың зерттеу қызметі кезеңінде алынатын конференциялар мен тезистерді қамтитын болады.

Қалай болатын үлгілері (бағалаушы әлеуетті осалдықтармен қалай соқтығысады):

а) Бағалаушы кейбір куәліктерді қарастырғанша, бағалаушы БО бағалау кезінде қатысуы мүмкін деп санайтын өнімнің ұқсас типінде табылатын әлеуетті осалдықтар туралы жады пайда болады;

б) бағалаушы кейбір куәліктерді қараған кезде әлеуетті осалдықты бейнелейтін интерфейс сипаттізіміндегі кемшіліктерді байқайды.

Бұның АТ жариялағанда өнімнің ерекше типіндегі жалпы осалдықтар туралы оқу арқылы БО-дағы әлеуетті осалдықты мойындауды қамтуы мүмкін – қауіпсіздік немесе бағалаушы жазылған электронды пошта қауіпсіздігі тізімінде.

Шабуылдау әдістері осы әлеуетті осалдықтарға тікелей әзірленуі мүмкін. Осылайша, қарсы әлеуетті осалдықтар бағалаушының осалдық талдауына негізделген ену тестілерін өткізу кезінде бірігеді. Бағалаушының қарсы әлеуетті осалдықтарға арналған ширақ әрекеттері болмайды.

Осылайша, бағалаушы AVA_VAN.1.2E және AVA_VAN .*. 4E көрсетілген айқын емес әрекеттер негізінде бағдар ұстайды.

Жалпы қолжетімді көздер осалдықтары мен шабуылдарына қатысты осы ақпарат бағалаушыға ұсынылуы мүмкін, мысалы, бағалау органы. Бұл ақпаратқа бағалаушы ену тестілерін әзірлеу кезінде қарсы осалдықтар мен шабуылдау әдістерін біріктіргенде назар аударуы қажет.

Б.2.3.2 Талдау

Бағалаушының әрекеті шеңберінде ұсынылатын мынадай талдау типтері бөлінеді.

Б.2.3.2.1 Құрылымдалмаған талдау

Бағалаушы орындайтын құрылымдалмаған талдау ((AVA_VAN.2) қызметімен бағалауға арналған) бағалаушыға жалпы осалдықтарды қарастыруға мүмкіндік береді (B.2.1 айтылғандай). Бағалаушы сондай-ақ

ұқсас технология типтеріндегі кемшіліктер туралы олардың тәжірибесі мен білімін қолданатын болады.

Б.2.3.2.2 Мақсатқа сәйкес талдау

Бағалаушы сондай-ақ бағалау жөніндегі іс-шаралар өткізу барысында проблемалық аймақтарды идентификациялай алады. Олар куәліктер топтасатын қызметтің осы түріне арналған талаптарды қанағаттандырғанымен, бағалаушының кейбір резервте ұстаулары болады. Мысалы, интерфейстің қандай да бір нақты сипаттізімі ерекше маңызды болып көрінеді және сондықтан БО әзірлеуде не БО операциясында қателерге ұшырауы мүмкін.

Әлеуетті осалдық осы сатыда байқалмайды, одан әрі зерттеу талап етіледі. Бұл одан әрі зерттеу талап етілетіндіктен, қарсы осалдық шеңберінен шығады.

Әлеуетті осалдық пен қолданылатын сала арасындағы айырмашылық:

а) әлеуетті осалдық – Бағалаушы осал жерлерді қолдану үшін пайдаланылатын шабуыл әдісін біледі немесе бағалаушы БО қатысы болатын осалдық ақпаратын біледі;

б) проблемалық сала – Бағалаушы басқа жерлерде ұсынылатын ақпарат негізінде әлеуетті осалдық ретінде санай алады. Бағалаушы интерфейс сипаттізімін оқыған кезде, интерфейстің төтенше күрделілігінен (қажет емес) әлеуетті осалдықтың осы бастапқы зерттеу негізінде анық болып табылмаса да, осы салаға кіруі мүмкін екенін анықтайды.

Осалдықты табудың мақсатқа сәйкес тәсілі қолдағы бар ақпарат арқылы кез келген анық әлеуетті осалдықтарды табу мақсатында куәліктерді талдау болып табылады. Ол осындай тәсіл алдын ала анықталмағандықтан, құрылымдалмаған талдауды білдіреді. Ықтимал осалдықтарды анықтауға арналған осындай тәсіл (AVA_VAN.3) қызметімен талап етілетін бағалаумен осалдықты тәуелсіз талдау барысында пайдаланылуы мүмкін.

Бұл талдауға өлшемдес сенім деңгейіне әкелетін түрлі тәсілдер арқылы қол жеткізілуі мүмкін. Тәсілдердің ешқайсысының орындалатын куәліктерді зерттеуге арналған қатты пішіні болмайды.

Қабылданған тәсіл куәлікті бағалау нәтижелерімен оның AVA / AGD талаптарына сәйкестігін анықтау үшін жөнелтіледі. Осылайша, әлеуетті осалдықтардың болатыны туралы куәліктер зерттеуі мынадай сипаттамалардың кез келгенінен бағыттала алады:

а) бағалау жүргізген уақытта куәліктерді қарау барысында табылған проблемалық салалар;

б) одан өтіп кетуге болмайтынын анықтау үшін қосымша талдау талап етілетін архитектура дизайнын ((ADV_ARC.1) қызметімен бағалаудағы сияқты) талдау барысында анықталған бөлуді қамтамасыз етуге арналған нақты функционалдық мүмкіндіктерді қолдау;

в) БО әлеуетті осалдықтарын қалыптастыруға арналған куәліктерді типтік зерделеу.

Бағалаушы куәліктердегі әлеуетті осалдықтарды табу үшін қандай шаралар қолданылғанын хабарлайды. Алайда, бағалаушының зерттеуді бастағанша әлеуетті осалдықтарды табуда операцияларды сипаттай алмауы мүмкін. Бұл тәсіл бағалау нәтижелері бойынша дамытылатын болады.

Проблемалық салалар БО бағалау талаптарын қанағаттандыру үшін ұсынылатын қандай да бір куәлікті тексеру нәтижесінде туындауы мүмкін. Сондай-ақ жалпы қолжетімді ақпарат ескерілетін болады.

Бағалаушы өткізетін іс-шаралар қайталануы мүмкін және сол тұжырымдарға қол жеткізу үшін қолданылған шаралар ерекшеленетін болса да, ол тұжырымдарға БО сенімділік деңгейіне байланысты қол жеткізілуі ықтимал. Бағалау әдісі өткізілген талдау формаларын құжаттау болып табылатындықтан, осы тұжырымдарға қол жеткізу үшін қолданылатын шаралар сондай-ақ қайталанғыш болып табылады.

Б.2.3.2.3 Жүйеге келтірілген

Талдауға арналған жүйелеген талдау куәлікті құрылымдық тексеру формасын қабылдайды. Бұл әдіс бағалаушыдан талдау құрылымы мен формасын анықтауды талап етеді (мысалы, талдаудың мақсатқа сәйкес идентификациялау әдісінен ерекше алдын ала талдаумен қалай өткізілетіні). Ақпаратқа сәйкес көрсетілген қарастырылатын осы әдіс және ол қалай/неліктен қарастырылатын болады. Ықтимал осалдықтарды анықтауға арналған мұндай тәсіл (AVA_VAN.4) және (AVA_VAN.5) қызметінің бағалауымен талап етілетін тәуелсіз талдау барысында пайдаланылуы мүмкін.

Куәліктердің осы талдауы талдауды енгізу ретінде идентификацияланған барлық куәліктер ескеріліп, тәсілде әдейі және бұрын жоспарланған болып табылады.

Барлық куәліктер кепілдік пакетінде көрсетілген сенімділік талаптарын (ADV) қанағаттандыру үшін ұсынылды, әлеуетті осалдықты идентификациялау қызметіндегі енгізу ретінде пайдаланылады.

Осы талдау үшін «жүйеленген» дескриптор әлеуетті осалдықты осы анықтаудың тапсырыс берілген және жоспарланған тәсілді қолдануды білдіретін сипаттамасын қамту әрекетінде пайдаланылған болатын. «Әдіс» немесе «жүйе» тексеріс кезінде қолданылатын болады.

Бағалаушы жоспарда қарастырылатын куәліктер әдісін сипаттайды, куәліктердегі ақпарат осы ақпараттың қалай қарастырылатынын және қалыптасатын жорамалды тексеретін болады.

Мыналарда жорамалды қабылдауы мүмкін бірнеше үлгілер болады:

а) сыртқы интерфейстерде қаскүнем үшін қолжетімді интерфейстердің дұрыс енбеуін қарастыру;

б) бөлуде деградацияға әкелетін домендерді бөлу, ішкі буферді қалыптастыру сияқты қауіпсіздік механизмдерін тексеру;

в) кейін ОФҚ толық бақыламайтын және функционалдық қауіпсіздік талаптарын ұзу үшін қаскүнем пайдалануы мүмкін БО жүзеге асыруда жасалатын қандай да бір объектілерді табу үшін талдау.

Мысалы, бағалаушы БО-да әлеуетті осал жерлер болып табылатын интерфейстерді анықтай және БО функционалдық сипаттізімі мен жобасында ұсынылатын барлық интерфейс сипаттізімдерінің әлеуетті осалдықтарды қалыптастыру үшін талданатынын анықтай және жорамалда пайдаланылатын әдістерді түсіндіруге көше алады.

Осы идентификациялау әдісі бағалаушы БО-да әлеуетті осалдықтардың ену тестілеуін аяқтаған кезде орындайтын БО шабуыл жоспарын ұсынады. Идентификациялау әдісінің негіздемесі БО үшін орындалатын пайдалануды анықтау мәні мен қамту жөніндегі куәліктерді ұсынған болар еді.

Б.3. Шабуыл әлеуеті қашан пайдаланылады?

Б.3.1 Әзірлеуші

Шабуыл әлеуетін ҚП / ҚТ авторы орта қатерін және сенімділік құрауыштарын іріктеуді назарға ала отырып, ҚП / ҚТ әзірлеу барысында пайдаланады. Бұл БО болжанатын қаскүнем ие болуы мүмкін шабуыл әлеуетінің жай тәуелсіз қорытындысы болуы мүмкін, негізгі, орташа немесе жоғары сияқты болып сипатталады. Басқа жағынан, ҚП / ҚТ, қаскүнем ие болатын болжанатын жекелеген факторлар деңгейінің ерекшеліктерін нақтылауды қажет етуі мүмкін (мысалы, қаскүнемдер, болжанатындай, мамандандырылған жабдыққа рұқсаты болатын БО технологиясы типіндегі сарапшылар болып табылады).

ҚП / ҚТ авторы қатер пішіні тәуекелді бағалау барысында әзірленді деп санайды (ҚР СТ ИСО / МЭК 15408 қолданылу саласынан тыс, бірақ қауіпсіздік проблемаларын анықтау тұрғысынан немесе ҚТ сенімділігі төмен жағдайында ҚП / ҚТ әзірлеуге енгізу ретінде пайдаланылады). Осы қатер пішінін келесі тармақшаларда қарастырылатын тәсілдердің бірінің тұрғысынан қарастыру БО шабуыл әлеуетіне сипаттізімнің қарсы тұруына мүмкіндік береді.

Б.3.2 Бағалаушы

Бағалаушы шабуыл әлеуетін әсіресе ҚТ және осалдықтарды бағалау барысында екі түрлі бағытта қарастырады.

Бағалаушы шабуыл әлеуетін БО қаскүнемнің болжанатын нақты шабуыл әлеуетіне орнықты болып табыла ма, жоқ па, соны анықтау үшін қызметтің осалдықтарына талдау жүргізген кезде пайдаланады. Егер бағалаушылар әлеуетті осалдық БО-да пайдаланылады деп санаса, онда олар оның болжанатын ортаның барлық аспектісі ескеріліп, оның ішінде қаскүнемнің болжанатын шабуыл әлеуетінде пайдаланылатынын растауға тиіс.

Осылайша, бағалаушы ҚТ қауіпсіздік қатерін қалыптастыруда баяндалатын ақпаратты пайдалана отырып, қаскүнемнің шабуыл жасау үшін қажет ететін минимальды шабуыл әлеуетін анықтайды және БО шабуылдарға қарсылығы туралы кейбір тұжырымдар жасайды. Б.1 кестесінде осы талдау және шабуыл әлеуеті арасындағы өзара байланыс көрсетіледі.

Б.1 кестесі Осалдықты және шабуыл әлеуетін тестілеу

Осалдық құрауышы	Шабуыл әлеуеті болатын қаскүнемге БО орнықтылығы:	Шабуыл әлеуеті болатын қаскүнем ғана пайдаланатын қалдық осалдықтар:
VAN.5	Жоғары	Аса жоғары
VAN .4	Орташа	Жоғары
VAN.3	Негізгі повышенный	Орташа
VAN .2	Негізгі	Негізгі жоғары
VAN.1	Негізгі	Негізгі жоғары

Жоғарыдағы кестедегі келтірілген қалдық осалдықтар бағанындағы «аса жоғары» шабуыл әлеуеті қаскүнемнен талап етілетін әлеуетті осалдықтарды тиісті түрде пайдалану үшін жай «жоғарыдан» гөрі барынша жоғары шабуыл әлеуеті болатын әлеуетті осалдықтарды білдіреді. Осы жағдайда қалдық ретінде жіктелетін осалдық БО осал орындар болатыны туралы факті болатынын бейнелейді, бірақ болжанатын шабуыл әлеуеті болатын сыртқы операциялық ортада осал орындар пайдаланылмауы мүмкін.

Шабуыл әлеуетінің кез келген деңгейінде әлеуетті осалдық пайдалануға байланысты осалдықты болдырмайтын операциялық ортада контрмерге байланысты «мүмкін емес» болып саналады.

Осалдық талдауы қолжетімді ықтималдылық немесе пермутациялық механизмдерді қоса алғанда, барлық ОФҚИ-ға қолданылады. ОФҚИ әзірлеу және жүзеге асыру дұрыстығына қатысты болжамдар қаскүнемнің БО-ға шабуылдау әдісіне немесе өзара әрекетіне шектеулер сияқты жасалған жоқ – егер шабуыл мүмкін болған жағдайда, ол осалдықты талдау барысында қарастырылуға тиіс. В.1 кестесінде көрсетілгендей, сенімділік құрауыштарының осалдығына қарсы сәтті бағалау ОФҚ қажетті қатер деңгейінен қорғау үшін әзірленгенін және жүзеге асырылғанын көрсетеді.

Бағалаушы үшін әрбір әлеуетті осалдық үшін шабуыл әлеуетін есептеуді орындау міндетті емес. Кейбір жағдайларда, шабуылдау әдісін әзірлеген кезде шабуыл әлеуетіне қажет болатыны немесе болмайтыны операциялық ортада қаскүнемнің болжамымен өлшемдес болатыны анық. Пайдаланылуы анықталған кез келген осалдықтар үшін, бағалаушы пайдаланудың қаскүнемнің болжайтын шабуыл әлеуетінің деңгейіне сәйкес келетінін анықтау үшін шабуыл әлеуетін есептеуді іске асырады.

Төменде сипатталатын тәсіл егер бағалау органы балама тәсілді қолдану туралы міндетті нұсқауды ұсынатынын есептемегенде, шабуыл әлеуетін есептеу үшін қажет кезде қолданылуға тиіс. Төменде Б.2 және Б.3 келтірілген мәндер математикалық расталмаған. Осылайша, осы кестелер үлгісінде көрсетілген мәндерді технология типіне және нақты ортаға байланысты түзету қажет болуы мүмкін. Бағалаушы бағалау органдарында нұсқау туралы сұрастыруы қажет.

Б.4 Шабуыл әлеуетін есептеу

Б.4.1 Шабуыл әлеуетін қолдану

Шабуыл әлеуеті тәжірибе, ресурстар және мотивация функциясы болып табылады. Осы факторларды білдіретін және есептейтін көптеген әдістер болады. Одан басқа, БО белгілі бір типтері үшін қолданылуы мүмкін басқа факторлар да болуы мүмкін.

Б.4.1.1 Мотивацияны түсіндіру

Мотивация қаскүнем және оның тілегімен байланысты бірқатар аспектілерді сипаттау үшін пайдаланылуы мүмкін шабуыл әлеуетінің факторы болып табылады. Біріншіден, мотивация шабуыл ықтималдылығын білдіре алады – жоғары дәлелденген сияқты сипатталған қатерден шабуылдың болмай қалмайтынын немесе дәлелденбеген қатерден ешқандай да шабуыл күтілмейтіні туралы тұжырым жасауға болады. Алайда, дәлелдеудің соңғы екі деңгейін қоспағанда, дәлелдеуден болатын шабуыл ықтималдығын сезіну қиын.

Екіншіден, мотивация не қаскүнем, не ресурс иесінің ресурсының, ақшалай немесе басқа мәнін болжауы мүмкін. Барынша жоғары мәні болатын ресурс, дұрысы, жоғары мәнділігі аз ресурстармен салыстырғанда шабуылды барынша дәлелдейтін болады. Дегенмен, жалпы түрінде емес басқаша, ресурс мәні субъективті болып табылатындықтан, дәлелдеуге арналған ресурс мәнін жатқызу қиын – ол елеулі шамада ресурс иесіне арналған мәнге байланысты болады.

Үшіншіден, мотивация қаскүнем шабуыл жасауға дайын болатын тәжірибе мен ресурстарды білдіруі мүмкін.

Жоғары дәлелденген қаскүнемнің ресурстарды қорғау шараларын бүлдіру үшін жеткілікті тәжірибе және ресурстарға ие болуы мүмкін деген тұжырым жасауға болады. Және керісінше, елеулі тәжірибесі мен ресурстары болатын қаскүнемнің егер қаскүнемді дәлелдеу төменгі деңгейде болатын болса, оларды пайдалана отырып шабуылды іске асырғысы келмейтіні туралы да тұжырым жасауға болады.

Бағалауды дайындау және өткізу барысында дәлелдеудің барлық үш аспектісі қандай да бір шамада ескеріледі. Шабуыл ықтималдылығының бірінші аспектісі әзірлеушіні бағалау өткізуге итермелеген нәрсе болып табылады. Егер әзірлеуші қаскүнемдерді шабуылға жеткілікті түрде

дәлелденген деп санаса, онда бағалау БО қаскүнем күштеріне кедергі жасауға жарамдылығына сенімділікті қамтамасыз ете алады. Операциялық орта толығымен анықталған жағдайда, мысалы, бағалау жүйесінде шабуылды дәлелдеу деңгейі белгілі болуы мүмкін және контрмерді таңдауға әсер етуі ықтимал.

Ресурс иесі екінші аспектіні ескере отырып, ресурстар мәнінің (алайда өлшенген) оларға жасалатын шабуылға жеткілікті болатынын болжауы мүмкін. Егер бағалау қажетті болып саналса, қаскүнем дәлелдеуі осы шабуылдарда пайдаланылатын тәжірибе мен ресурстар сияқты алдын ала қабылдануы мүмкін шабуыл әдістерін анықтау үшін ескеріледі. Әзірлеушінің тексеруден кейін тиісті сенімділік деңгейін, атап айтқанда, қатерге арналған шабуыл әлеуетімен өлшенетін құрауыштардың AVA талабын таңдау мүмкіндігі бар. Бағалау барысында бағалаушы осалдықты бағалауды аяқтау нәтижесі ретінде анықталған тәжірибесі мен ресурстары болатын қаскүнемдерге кедергі жасау үшін өзінің операциялық ортасында БО әрекеті жеткілікті болып табылатынын анықтайды.

ҚТ авторы үшін ҚТ авторы БО орналасқан операциялық орта ауқымында үлкен мәндерге ие болатындықтан қаскүнемнің дәлелдеуін мүмкін деп санауы мүмкін (ҚТ талаптарына сәйкес). Осылайша, мотивация ҚТ-ға жасалатын шабуыл әлеуетін өрнектейтін дәл бөліктерді, сондай-ақ дәлелдеуді сандық бағалауға бағытталған қажетті әдістер мен шараларды қалыптастыруы мүмкін.

Б.4.2 Шабуыл әлеуетін анықтау

Осы тармақшада шабуыл әлеуетін анықтайтын факторлар қарастырылады және бағалау процесінің осы аспектісінен кейбір өзіндікті жоюға көмек беру үшін кейбір нұсқаулар болады.

Б.4.2.1 Шабуыл әлеуетін анықтау

Шабуылға арналған шабуыл әлеуетін анықтау шабуыл жасау үшін, сондай-ақ оның БО үшін сәтті қолданылатынын көрсету үшін қажетті күштерді идентификациялауға сәйкес келеді (оның ішінде кез келген қажетті сынақ жабдығын жасау немесе құру туралы), сонысымен осалдықты БО-да пайдаланады. Шабуылдың сәтті қолданылатынын көрсету үшін пайдалы шабуыл жасау үшін зертханалық жағдайларда көрсетілген нәтижелерді кеңейтуде қандай бір қиындықтарды ескеру талап етіледі. Мысалы, егер тәжірибе заттың құпия деректерінің кейбір биттерін немесе байттарын көрсететін болса (мысалы, кілт), онда осы заттың қалған бөлігін қалай алу туралы ойластыру қажет (осы үлгіде кейбір биттер басқалары жан-жақты іздеу сияқты түрлі тәсілдер арқылы табылатын уақытта одан кейінгі тәжірибелермен тікелей өлшенуі мүмкін). Егер шабуыл БО ресурстарына қол жеткізу алынғанын және толық шабуыл AVA_VAN шабуыл құрауышына сәйкес пайдалануда шынайы іске асырылуы мүмкін екенін дәлелдейтіні айқын болса, барлық шабуылды анықтауға арналған барлық тәжірибені

жүргізіп қажеті жоқ. Кейбір жағдайларда AVA_VAN шабуыл құрауышына сәйкес пайдалануда шабуылдың шынайы іске асырылатынын дәлелдеудің бірден-бір тәсілі шабуылды толық орындау үшін, ал содан соң талап етілетін ресурстарға байланысты бағалаудан тұрады. Әлеуетті осалдықтарды идентификациялаудан шығулардың бірі БО басқа үлгісінің осалдығын пайдаланған кезде пайдаланылуы мүмкін шабуылды қалай өткізуді қадамдық сипаттауды беретін скрипт болып саналады.

Көптеген жағдайларда бағалаушы толық пайдалануды орындауды емес, пайдалану параметрлерін бағалайды. Бағалау және олардың негіздемесі техникалық бағалау есебінде құжатталады.

Б.4.2.2 Ескерілетін факторлар

Келесі факторлар осалдықтарды пайдалану үшін қажетті шабуыл әлеуетін талдау барысында ескерілуге тиіс:

- а) анықтау және пайдалану үшін жұмсалған уақыт (өткен уақыт);
- б) маманның талап етілетін техникалық тәжірибесі (маманның тәжірибесі);
- в) БО жобасын және пайдалануды білуі (БО білімі);
- г) мүмкіндіктер терезесі;
- д) АТ – жабдық және (немесе) программалық қамтамасыз ету немесе пайдалану үшін қажетті өзге жабдық.

Көп жағдайларда осы факторлар тәуелді болып табылады, бірақ түрлі деңгейде бір-бірімен ауыстырылуы мүмкін.

Мысалы, тәжірибе немесе аппараттық-программалық қамтамасыз ету уақытпен ауыстырылуы мүмкін. Осы факторлардың толық сипаттауы болады.

Егер бұл болатын болса, онда шамалы «қымбат» қиыстыру пайдалану сатысында ескеріледі.

Өткен уақыт – бұл қаскүнемнің БО жасалатын шабуылды құрастыру үшін қажетті күшті сақтау және шабуыл әдісін әзірлеу үшін, БО-да болуы мүмкін нақты әлеуетті осалдықты анықтау үшін жұмсайтын жалпы уақыт мөлшері. Осы факторды қарастыру, ең нашар жағдайда жұмсалған уақытты бағалау үшін пайдаланылады. Анықталған уақыт мөлшері былай болады:

- а) бір күннен кем;
- б) бір күннен бастап бір аптаға дейін;
- в) бір күннен бастап екі аптаға дейін;
- г) екі аптадан бастап бір айға дейін;
- д) 6 айға дейінгі әрбір қосымша ай мәннің артуына әкеледі;
- е) 6 айдан артық.

Маманның тәжірибесі өнім немесе шабуыл әдісі типтерінің негізін құрайтын принциптер туралы жалпы білім деңгейін көрсетеді (мысалы, Unix операциялық жүйелерінің интернет-хаттамалары, буфердің аса толып кетуі). Анықталған деңгей болып табылады:

а) сарапшылар немесе ерекше тәжірибесі болмайтын тұлғалармен салыстырғанда білімі болмайтындар маман болып табылмайды;

б) мамандардың өнім немесе жүйе типінің қауіпсіздігін қолдану саласымен таныстырылғаны туралы хабарланған;

в) сарапшылар негізгі алгоритмдер, хаттамалар, жабдықтар, құрылым, қауіпсіздіктің қолданылу саласы, жұмыс істейтін қауіпсіздік принциптері мен тұжырымдамалары, жаңа шабуылдарды анықтауға арналған әдістер мен аспаптар, криптография, өнім типтеріне арналған классикалық шабуылдар, шабуыл әдістерімен және өнімде немесе жүйенің типінде жүзеге асырылған т.б. таныстырылған;

г) «Қайта сараптаушы» деңгейі сарапшылардың түрлі шабуыл сатыларына арналған деңгейдегі түрлі салаларды білуі үшін қажетті жердегі жағдайды қамтамасыз ету үшін енгізілген.

Білімнің бірнеше саладан талап етілуі мүмкін. Келісім бойынша, әр түрлі тәжірибе факторларының ең жоғарғысы таңдалды. Нақты жағдайларда «қайта сараптаушы» деңгейі пайдаланылуы мүмкін, бірақ білімнің өте әр түрлі болып табылатын салаларды ғана сөз етуі керек екенін айтып кету керек, мысалы, бір жарты кезеңдік манипуляция және криптография.

БО білімі БО қатысты нақты тәжірибеге қатысты болады. Бұл жалпы, бірақ онымен байланысты емес тәжірибеден ерекшеленеді. Мынадай деңгейлер анықталған болып табылады:

а) БО қатысты қоғамдық ақпарат (мысалы, интернеттен алынған сияқты);

б) БО туралы шектелген ақпарат (мысалы, әзірлеуші ұйымының немесе басқа ұйымдармен бірге жарияламау туралы келісім шеңберінде бақылауда болатын ақпарат);

в) БО сезімтал ақпараты (мысалы, әзірлеуші ұйымдар ішіндегі дискретті топ арасында бөлінетін білімдер, аталған топ мүшелері үшін ғана шектелген қол жеткізу);

г) БО сыни ақпараты (мысалы, қол жеткізу білуге қатаң тыйым салынған және жеке міндеттер негізінде өте қатаң бақыланатын, небәрі бірнеше тұлғаларға ғана белгілі ақпарат).

БО ақпараты жоба абстракциясына сәйкес шығарылуы мүмкін, дегенмен бұл БО негізіндегі БО-ға ғана жасалуы мүмкін. БО кейбір объектілері жалпы қолжетімді болуы мүмкін (немесе шамалы деңгейде қоғамдық қол жеткізуге негізделген) және сол себепті тіпті объектіні ұсыну басқа БО үшін жүзеге асыруды көрсету уақытында бұл қаскүнемге шабуыл жасауға ықпал ететін ақпаратты беретіндіктен өте мұқият бақыланатындықтан, қоғамдық немесе барынша шектелген болып жіктелген болар еді және сондықтан сезімтал немесе тіпті сыни болып саналады.

Бірнеше салалар білімі талап етілетін жағдай болуы мүмкін. Келісім бойынша әр түрлі тәжірибе факторларының ең жоғарғысы таңдалды.

Мүмкіндіктер (мүмкіндік) терезесі сондай-ақ маңызды фактор болып табылады және өткен уақыт факторына қатысы болады. Осалдықты анықтау немесе пайдалану байқау ықтималдығын арттыруы мүмкін БО-ға қол жеткізудің елеулі санын талап етуі ықтимал. Кейбір шабуыл әдістері автономды режимде елеулі күшті және пайдалану үшін БО-ға тез қол жеткізуді ғана талап етуі мүмкін. Қол жеткізудің үздіксіз болуы немесе бірнеше сессия бойында қалуы талап етілуі ықтимал.

Кейбір БО үшін мүмкіндіктер терезесі хакер қол жеткізуі мүмкін БО үлгілерінің санына теңестірілуі мүмкін. Бұл БО ену және БО және оны әрі қарай сынайтын үлгілерді пайдалануды болдырмауды қадағалайтын қауіпсіздік талаптары функциясын бұзу әрекеті болатын жердегі өте маңызды сәт, мысалы, аппараттық құрылғылар. Мұндай жағдайларда БО жиі бөлу бақыланады және хакер БО одан арғы үлгілерін алу үшін күш қолдануға тиіс.

Осы талқылау мақсаты болып табылады:

а) артық/шектелген қол жеткізу шабуылдың мүмкіндігінше жүзеге асырылуын қажет етпейтінін негізге алады, себебі БО-ға қол жеткізу кезеңінде байқалу үшін ешқандай қатер жоқ және БО-ның үлгілер санын шабуылға рұқсат беру үшін проблема болмайды;

б) жеңілдік қол жеткізудің оннан аз болмайтын шабуылды орындау үшін талап етілетін БО үлгілерінің саны сияқты бір күннен артық қол жеткізу талап ететінін білдіреді;

в) өзгерту жүзден аз болмайтын шабуылды орындау үшін талап етілетін БО үлгілерінің саны сияқты бір айдан көп болмайтын қол жеткізуді білдіреді;

г) қиыншылық жүз шабуылды орындау талап етілетін БО үлгілер саны немесе ең аз дегенде бір айға қол жеткізу талап етілетінін білдіреді;

д) «бір де бір» термині мүмкіндіктер терезесінің шабуылды орындау үшін жеткілікті болып табылатынын білдіреді (активтер қолжетімді немесе сенімді болатын ұзындық шабуылды орындау үшін қажетті мүмкіндіктер өлшеміне қарағанда аз - мысалы, егер активтер кілті әр аптада өзгертін болса, ал шабуыл екі апта көлемінде жүргізілсе); екінші жағдай – бұл шабуылды орындауға қажетті БО үлгілерінің саны қолжетімді болған кезде, бірақ бұған хакердің қолы жетпейді - мысалы, егер БО аппарат болып табылса және шабуыл кезінде БО қирату мүмкіндігі сәтті болудың орнына өте жоғары болса, онда хакер БО бір үлгісіне ғана қол жеткізеді.

Осы факторды талқылау мүмкіндік уақытына қарағанда қол жеткізу уақытына арналған талаптарға жататын пайдалануды аяқтауды анықтау салдары болуы мүмкін.

АТ аппараттық және (немесе) программалық қамтамасыз ету немесе өзге жабдықтар осалдықты анықтау немесе пайдалану үшін тексеруге жіберіледі:

а) стандарттық жабдық хакер үшін не осалдықты анықтау үшін, не шабуыл үшін оңайлықпен қол жеткізу болып табылады. Бұл жабдық БО

бөлігі болуы мүмкін (мысалы, операциялық жүйедегі жөндеу программасы) немесе тез сатып алынуы мүмкін.

ҮЛГІ: Интернеттен жүктеулер, хаттама талдаушы немесе шабуыл сценарии.

б) мамандандырылған жабдыққа хакердің қолы оңай жетпейді, бірақ ерекше қиындықсыз сатып алынуы мүмкін. Онда жабдықтардың орташа саны (мысалы, тұтылатын қуатты талдауға арналған құрал-сайман, Интернетпен о шетінен бұ шетіне дейін байланысты жүздеген ДК пайдалану осы санатқа жатады) немесе шабуылдар мен программалардың барынша маңызды сценарийлерінсіз дамыту болуы мүмкін. Егер мамандандырылған жабдықтан тұратын түрлі сынақ стенділері ерекше шабуыл операциялары үшін талап етілетін болса, бұл тапсырыс ретінде бағаланатын болады;

в) тапсырысты жабдық ол арнайы тапсырыс бойынша дайындалатындықтан (мысалы, аса нақтыланған программалық қамтамасыз ету) немесе жабдықтың мамандандырылғаны соншалық, оны тарату бақыланатын, тіпті мүмкін шектелген болған себепті қоғам үшін қолжетімді емес. Немесе ол өте қымбат болуы мүмкін.

г) «Құрамдас тапсырысты» деңгейі тапсырыспен жасалған жабдықтың түрлі типтері ерекше шабуыл операциялары үшін талап етілетін кездегі жағдайға мүмкіндік беру үшін енгізілді. БО шабуылда қол жеткізу үшін тұлғаларға қажет болатын ақпарат мамандарға және олардың БО білуіне сараптама жасау үшін қажет. Хакер сипаттамасы (қосымша сфералық білімі бар бір немесе бірнеше адам хакер болуы мүмкін) мен шабуылда жабдықты тиімді пайдалану қабілеті арасында жабық өзара байланыс болады. Хакердің сараптама қаншалықты әлсіз болса, жабдықтың пайдалану әлеуеті сонша төмен болады (АТ аппараттық/программалық қамтамасыз етуі немесе өзге жабдықтар). Осыған ұқсас, сараптама қанша көп болса, шабуылда жабдыққа арналған әлеует жақсы пайдаланылады. Сондай-ақ осы сараптама мен жабдықты пайдалану арасындағы өзара жабық байланыс әрқашан қолданылмайды, мысалы, қоршаған ортаны қорғау бойынша шаралар хакердің жабдықты пайдалануын болдырмайтын кезде немесе тиімді пайдалану үшін шағын сараптама қажет болатын шабуылдың басқа күштері, құралдары арқылы жүргізіледі және еркін таратылады (Интернет арқылы).

Б.4.2.3 Шабуыл әлеуетін есептеу

Б.2 кестесі алдыңғы тармақшаларда талқыланған факторларды және әрбір фактордың жиынтық шамасы болатын сандық шамалар тобын анықтайды.

Бағалаушы фактор ауқым шегіне өте жақын болатын жерлерде кестедегілерге аралық шамаларды пайдалануды ойластырады. Мысалы, егер шабуылды орындау үшін жиырма үлгі талап етілетін болса, онда бірінші және төртінші арасындағы шама осы фактор үшін таңдалуы мүмкін немесе егер сызбанұсқа жалпы қолжетімді жоспарда негізделген болса, бірақ

әзірлеуші кейбір өзгерістер енгізсе, онда нөл және үштік арасындағы шаманы бағалаушы олардың жоспарлық өзгерістерінің өзара әрекеттерін қарауға сәйкес таңдауға тиіс. Кесте нұсқау ретінде тағайындалған.

Б.2 кестесіндегі «мүмкіндіктер терезесі» назарға алынып қабылданған белгілеулер осы фактормен байланысты алдыңғы ауқымдарда көрсетілген уақытша шеңберден болатын табиғи прогрессия болып табылмайды. Осы сипаттізім осалдықтың ерекше жағдайда БО-да оның тағайындалған операциялық жабдығымен бірге әзірлене алмайтынын көрсетеді. Мысалы, БО-ға қол жеткізу жүйелі тексеру жүргізілетін жерде және бұзушы талап етілетін ашылмаған екі аптада БО-ға қол жеткізе алмайтын БО-да аталған жабдықпен өткізілген белгілі бір уақыт мөлшерінен кейін байқалуы мүмкін (яғни, жүйе корпусында). Алайда, бұл қашықтан қол жеткізу мүмкін болатын жерде және БО арналған физикалық орта белгісіз болатын жерде БО үшін қолданылмайтын болады.

Б.2 кестесі Шабуыл әлеуетін есептеу

Фактор	Бағалау
Жұмыс уақыты	
<= бір күн	0
<= бір апта	1
<= екі апта	2
<= бір ай	4
<= екі ай	7
<= үш ай	10
<= төрт ай	13
<= бес ай	15
<= алты ай	17
> алты ай	19
Тәжірибе	
Кәсіби емес	0
Маман	3* ¹⁾
Сарапшы	6
Біліктілігі жоғары маман	8
БО білу	

Жалпы рұқсат етілген	0
Шектелген	3
Сезгіш	7
Сыни	11
Мүмкіндіктер терезесі	
Артық/ шектелген қол жеткізу	0
Оңай	1
Біркелкі	4
Қиын	10
Ешбірі	** ²⁾
Жабдық	
Стандарттық	0
Мамандандырылған	4 ³⁾
Тапсырысты	7
Құрауыш тапсырысты	9
⁽¹⁾ – шабуылдау барысын орындау үшін бірнеше маман қажет болатын кезде, қорытындылаушы сараптама деңгейі сонда да «тәжірибелік» болып қалады (3-көрсеткішке әкелетін); ⁽²⁾ – шабуыл барысының БО тағайындалған операциялық ортасында қалған бірліктермен салыстыру бойынша тиісінше пайдаланылмайтынын көрсетеді; ⁽³⁾ – егер мамандандырылған жабдыктан тұратын түрлі сынақ стендтері ерекше операциялар үшін талап етілсе, бұл тапсырыс сияқты бағалануға тиіс.	

БО-ның идентификацияланған әлеуетті осалдыққа қатысы бойынша қарсылығын анықтау үшін мынадай операциялар қолданылуға тиіс:

- а) операциялық ортада БО арналған ықтимал шабуыл сценарийлерін {AS1, AS2, ..., ASn} анықтау;
- б) әрбір шабуыл сценарийі үшін теориялық талдауды орындау және В.2 кестесін пайдалана отырып, маңызды әлеуетті шабуылдарды есептеу;
- в) әрбір шабуыл сценарийі үшін егер қажет болса, теориялық талдауды растау немесе теріске шығару үшін енуге арналған сынақты орындау;
- г) барлық шабуыл сценарийін {AS1, AS2, ..., ASn} екі топқа бөлу:
 - 1) сәтті шабуыл сценарийлері (яғни, Функционалдық Қауіпсіздік

Талаптарын бұзу үшін сәтті пайдаланылған) және

2) жеңіліске ұшыраған шабуыл сценарийлері.

д) әрбір шабуыл сценарийі үшін В.3 кестесін қолдану керек және БО қарсылығы мен AVA_VAN таңдалған сенімділік құрауыштары арасында қарама-қайшылық болатынын анықтау, В.3 кестесінің соңғы қатарын қараңыз;

е) бір қарама-қайшылықты табу керек, осалдықты бағалау түседі, мысалы, ҚТ авторы AVA_VAN.5 құрауышын таңдауда, онда шабуыл әлеуеті болатын шабуыл сценарийі БО қауіпсіздігін 21 баллға (жоғары) бұзды. Мұндай жағдайда БО шабуылдаушыға «Орташа» шабуыл әлеуеті арқылы қарсыласады, бұл AVA_VAN.5 қайшы келеді, осыдан осалдық сенімділігі төмендейді.

В.3 кестесі қатарының «құндылықтары» Функционалдық Қауіпсіздік Талаптарының бұзылуына әкелген сценарийге жасалған шабуыл әлеуетін (В.2 кестесі арқылы есептелген) бағалау ауқымын көрсетеді.

В.3 кестесі – БО осалдығы мен қарсылығын бағалау

Бағала р	Сценарий үшін талап етілетін шабуыл әлеуеті:	Шабуыл әлеуетімен шабуыл жасайтын БО қарсылығы:	Сенім құрауыштарын кездестіреді:	Құрауыштардың білініп қалуы:
0-9	Негізгі	Бағаланбаған	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Үдемелі – Негізгі	Негізгі	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Өзгертілген	Үдемелі –Негізгі	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	Жоғары	Өзгертілген	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Аса жоғары	Жоғары	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Осы сияқты тәсіл әрбір жағдай немесе факторды ескере алмайды, бірақ стандарттық бағалауға қол жеткізу үшін шабуыл қарсылығы деңгейіне жақсы нұсқау беруге тиіс. Ықтималдығы аз кездейсоқ оқиғаларға сенімділік сияқты қалған факторлар негізгі модельде қамтылмайды, бірақ негізгі модельді көрсететіндермен салыстырғанда басқаларының құнын анықтаудағы растау ретінде пайдалануы мүмкін.

Жеке бағаланған осалдықтар саны шабуылға жоғары қарсылықты анықтай алатын кезде бірге бағаланған осалдықтар қиыстыруының төмен бағалаулардың толық қолданылатынын анықтай алатынын айтып кету қажет. Бір осалдықтың болуы екіншісін оңай пайдаланылатын етіп жасай алады.

Егер ҚП/ҚТ авторы шабуыл деңгейін анықтау үшін шабуыл әлеуеті кестесін пайдаланғысы келсе, онда ол БО осалдық талдауы құрауышына шыдауға тиіс ((AVA_VAN) осалдық талдауы құрауышын таңдау), ол мынадан шығуға тиіс:

ФҚТ бұзуға тиіс емес барлық әр түрлі шабуыл сценарийлері үшін (яғни, автор ойлайтын барлық әр түрлі шабуылдаушы типтері және (немесе) әр түрлі шабуыл типтері) В.2 кестесі арқылы бірнеше аралық әрбір сәтсіз шабуыл сценарийі үшін ойластырылған шабуыл әлеуетін түрлі бағалауды анықтауға тиіс. ҚП/ҚТ авторы содан соң В.3 кестесінен БО қарсылық деңгейін анықтау үшін жоғары бағаны таңдайды: БО қарсылығы кем дегенде осы анықталған жоғарғы бағалаумен тең болуы керек. Мысалы, орташа тәсіл бойынша белгіленген БО қауіпсіздік саясатын бұзбауға тиіс барлық шабуыл сценарийлерінің шабуыл әлеуетін жоғары бағалау; осыдан БО қарсылығы, кем дегенде, орташа (яғни, орташа немесе жоғары); сондықтан ҚП/ҚТ авторы қолайлы сенімділік құрауышы ретінде не AVA_VAN.4 (орташа үшін), не AVA_VAN.5 (жоғарғы үшін) үшін таңдай алады.

Б.5 Тікелей шабуылды есептеу үлгісі

Тура шабуылға арналған механизм объектілері осы механизмдерді жиі күшейтетін әзірлеушілер және жүйе қауіпсіздігі үшін жиі өмірлік маңызды элементтер болып табылады. Мысалы, БО оны пайдаланушы санының басқа жиынтығын тез шешу мүмкіндігі күшіне жасалатын шабуылды жеңе алатын түпнұсқаландыру механизмінің санын қарапайым кезекпен пайдалана алады. Жүйе сандар жиынтығын және оларды түрлі тәсілдермен пайдалануды шектеу арқылы осы механизмді күшейтуі мүмкін. Бағалау курсы көлемінде осы тура шабуылды талдау былайша өтуі мүмкін:

ҚТ және деректер сызбанұсқасын ашу кезінде жиналған ақпарат кең таралған терминал желісінің ресурстарына қол жеткізуді басқаратын негіздерді қамтамасыз етуді анықтайды және түпнұсқаландырады. Терминалға физикалық қол жеткізу ешқандай тиімді құралдармен бақыланбайды. Сондай-ақ терминалға қол жеткізу ұзақтығы ешқандай тиімді құралдармен бақыланбайды. Авторластырылған жүйе пайдаланушылары

олардың жүйені пайдалану үшін тіркелетін және содан соң пайдаланушы атымен кіретін өзіндік парольдерін таңдайды. Жүйе пайдаланушылар таңдаған парольдер үшін мынадай шектеулер қояды:

- а) пароль төртеуден кем болмауы және өлшемі алты цифрдан артық болмауы керек;
- б) сандар кезектілігінің бірізділігіне тыйым салынады (7,6,5,4,3 сияқты);
- в) цифрлардың қайталануына тыйым салынады (әрбір цифр жеке болуға тиіс).

Пайдаланушылар үшін пароль таңдауда қамтамасыз етілетін нұсқау бұл қаншалықты мүмкін болса, пароль соншалықты кездейсоқ болуын білдіреді және кейбір жағдайларда пайдаланушымен қалай да байланысты болуға тиіс емес – мысалы, туған күні.

Пароль ауқымы былай түсіндіріледі:

- а) адамның әдет үлгілері – парольді ашуға арналған тәсілге әсері болатын маңызды ойлау бөлігі. Жаман жағдайда, сценарий және пайдаланушы төрт цифрды ғана қамтитын санды таңдайды, әрбір цифр жеке болуға тиіс жағдайда парольді қайта орнату саны болып табылады:

$$7 (8) (9) (10) = 5040$$

- б) тізбектіліктің кемуіндегі сияқты жеті цифры тізбектіліктің ықтимал өсу саны болып табылады. Тізбектілікке тыйым салудан кейінгі пароль болады:

$$5040 - 14 = 5026$$

Парольдің деректер сызбанұсқасынан жинақталған одан арғы ақпаратына негізделген механизмі ерекшеліктерді байланыстыратын терминалмен жоспарланған. Сәтсіздікке ұшыраған алты әрекеттен кейін бір сағатқа жабылады. Сәтсіздікке ұшыраған түпнұсқаландыру есептеулері бес минуттан кейін қалпына келтіріледі және хакер жақсы әрекет еткенде бес минут сайын бес пароль немесе сағатына 60 парольді енгізе алады.

Орташа алғанда, хакер дұрыс пароль енгізілгенше, 2513 минутта 2513 пароль енгізе алады. Орташа сәтті шабуыл (Б.1) формула бойынша аз есептеледі:

$$\frac{2513}{60 \frac{\text{min}}{\text{hour}}} \approx 42 \text{ hours} \quad (\text{Б.1})$$

Алдыңғы тармақшада сипатталған шабуыл әлеуетін есептеу тәсілін пайдалана отырып, кәсіби еместің мұндайда стандарттық жабдықты пайдалана отырып және БО ерекше білмей-ақ 1-бағалауға сәйкес бір күн

ішінде механизмді аша алатыны белгіленді (бағалау объектісіне рұқсат алып). Алынған осы бағалау, 1, сәтті шабуыл жасау үшін талап етілетін шабуыл әлеуеті ол негіз ретінде қарастырылып төмен түсетіндіктен бағаланбайды.

ӘОЖ 681.324

МСЖ 35.040

Түйінді сөздер: Альбрехт 1984, функционалдық нүктелерді талдау (АФТ), шекаралар, өзгеріс, функционалдық өлшемін өлшеу (ФӨӨ), түзетілген өлшем, техникалық күрделілікті түзету, логикалық транзакция, объекті, базалық деңгейдің функционалдық нүктелерін есептеу, қосымшаның функционалдық нүктелерін есептеу, жоба әзірлемесінің функционалдық нүктелерін есептеу, жоба бойынша өзгерістердің функционалдық нүктелерін есептеу, объектінің тармағына орнатылған функционалдық нүктелерін есептеу, объекті тармағы, пайдаланушы, қосымша, жүйе, деректер элементтерінің типі (ДЭТ), МГПФТ, ӨЖЖ

Басуға _____ ж. қол қойылды Пішімі 60x84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы _____ дана. Тапсырыс _____

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