ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
7-бөлім
Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу негіздері

Информационная технология
ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ
Основы безопасности для открытых систем
Часть 7
Основы учета событий безопасности и оперативного оповещения

ҚР СТ ИСО/МЭК 10181-7-2008

(ИСО/МЭК 10181-7:1996 «Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу негіздері», IDT)

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТІК СТАНДАРТЫ

Ақпараттық технология

АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ

Ашық жүйелерге арналған қауіпсіздік негіздері
7-бөлім
Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу негіздері

ҚР СТ ИСО/МЭК 10181-7-2008
(ИСО/МЭК 10181-7:1996 «Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу негіздері», IDT)

Ресми басылым

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

Астана

Алғысөз

1. «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасының Ақпараттандыру және байланыс жөніндегі агенттігі **ЕНГІЗДІ**

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

3. Осы стандартта Қазақстан Республикасы экономикасының қажеттіліктерін білдіретін қосымша талаптар көлбеу қаріппен белгіленді. «Ақпараттық технология. Ашық жүйелердің өзара іс-әрекеті. Ашық жүйелерге арналған қауіпсіздік негіздері. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу негіздері» («Information technology. Open Systems Interconnection. Security frameworks for open systems. Security audit and alarms framework») ИСО/МЭК 10181-7:1996 халықаралық стандартына, IDT балама болып табылады.

4. БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5. АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

Осы стандарт *ҚР СТ ИСО/МЭК 10181 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ашық жүйелердің өзара іс-әрекеті. Ашық жүйелердің қауіпсіздік негіздері»* жалпы атауымен мынадай бөліктерден тұрады:

– 1-бөлім. Шолу.

– 2-бөлім. Сәйкестендіру негіздері.

– 3-бөлім. Қол жеткізімділікті басқару негіздері.

– 4-бөлім. Бас тартпаушылық негіздері.

– 5-бөлім. Құпиялылық негіздері.

– 6-бөлім. Біртұтастылық негіздері.

– 7-бөлім. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу негіздері.

Осы стандарт *ҚР СТ ИСО/МЭК 10181-1* стандартында суреттелген қауіпсіздік оқиғаларын есепке алу тұжырымдамасын анықтайды. Тұжырымдама жүйедегі қауіпсіздік оқиғаларын табудан, сол сияқты оған керісінше жедел жауап қайтарудан тұрады. Сондықтан ашық жүйелер қауіпсіздігінің негіздері қауіпсіздік оқиғаларын, сол сияқты олар туралы жедел хабарлау сызбанұсқасын есепке алуға қатысты болып табылады.

Қауіпсіздік оқиғаларын есепке алу жүйедегі оқиғаларды тәуелсіз талқылау және сараптау болып табылады. Қауіпсіздік оқиғаларын есепке алу мақсаттары:

– рұқсат етілмеген іс-әрекеттерді немесе шабуылдарды бірдейлендіру және талдау кезінде көмек;

– белгілі бір әрекеттер мұндай әрекеттер үшін жауапты объектіге есептелуі мүмкін екендігінің кепілдігін талдау;

– залалдарды бақылаудың жетілдірілген тәртібін әзірлеуге үлес;

– қолданыстағы қауіпсіздік саясатына сәйкестігін растау;

– жүйелік бақылаудың талаптарға сәйкес келмеуін көрсетуі мүмкін есептік мәліметтер;

– басқарудың, саясаттың және қорғаныс тәртіптерінің мүмкін болатын қажетті сәйкестендіру.

Қарастырылып отырған қауіпсіздік негіздері шеңберінде қауіпсіздік оқиғаларын есепке алуға қорғаумен әр түрлі байланысты оқиғаларды есепке алу журналдарынан, сол сияқты осы журналдарды талдау нәтижелері бойынша табу, жинау және тіркеу кіреді.

Қауіпсіздік оқиғаларын есепке алу және есептілік талаптары белгілі бір ақпаратты тіркеу қажеттігінде болып табылады. Қауіпсіздік оқиғаларын есепке алу жұмыстың белгіленген тәртібі мен ерекше жағдайлар туралы жазылған ақпараттың жеткіліктігіне кепілдік береді. Сонымен, анағұрлым

кеш тексеру қорғаныс бұзылуының болған-болмағандығын, және нақты қандай ақпарат немесе өзге қор көздеріне қауіптілік төнгендігін анықтай алады. Есепке алуды сақтау қолданушылардың іс-әрекеттері немесе олардың атынан болып жатқан процестер туралы іске қатысты ақпаратты тіркеуге кепілдік береді. Осылайша, белгілі бір қолданушылардың іс-әрекеттері туралы бұдан арғы қорытындылар олармен тікелей байланысты болуы мүмкін, және бұл қолданушылар өз әрекеттері үшін жауапкершілікке тартылуы мүмкін. Қауіпсіздік оқиғаларын есепке алуды жүргізу есептілік деңгейін жоғарылатуға ықпал жасайды.

Жедел хабарлау – бұл тез арада араласуды қажет ететін жағдайдың пайда болғанын көрсету үшін белгілі бір тұлғаға немесе процесске арналған ескертпелерді (дабыл белгілерін) беру. Жедел хабарлау сервисінің жұмыс істеу мақсаттары:

– қорғанысты бұзудың іс жүзіндегі және ықтимал әрекеттері туралы хабарлау;

– «қалыпты» оқиғаларды қоса алғанда, қауіпсіздік оқиғалары туралы хабарлау;

- бастама мәндер жетістіктерінің жағдайлары туралы хабарлау.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
7-бөлім
Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу негіздері

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт ашық жүйелер ортасында қауіпсіздік сервистерін қолдану міндеттерін шешуге арналған негізгі қауіпсіздік ережелерін белгілейді. «Ашық жүйелер» термині дерекқорлар, бөлінген қосымшалар, ашық бөлінген өңдеу және ашық жүйелердің байланысы (АЖБ) сияқты аумақтар түсініледі. Қауіпсіздіктің негізгі ережелері жүйелерді құру әдіснамасына және олардың механизміне қатысы жоқ.

Қауіпсіздіктің негізгі ережелері мәліметтер элементімен, сол сияқты қауіпсіздіктің ерекше сервистерін алу үшін қолданылатын әрекеттердің бірізділігін (бірақ хаттама элементтерін емес) пайдаланады. Бұл қауіпсіздік сервистері жүйелердің өзара іс-әрекет етуші маңыздарына, сол сияқты жүйелер арасында мәліметтермен алмасуға, сондай-ақ жүйелер басқаратын деректерге қолданылуы мүмкін.

Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу мақсаты осы стандартта сипатталғандай ашық жүйелердегі оқиғалар осы жүйеде әрекет етуші қауіпсіздік саясатына сәйкес ықпал жасайтынына кепілдік беруі тиіс.

Көбінесе, бұл негіздер:

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алудың негізгі тұжырымдамасын анықтайды;

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алудың қорытылған үлгісін сипаттайды;

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алудың басқа қорғаныс сервистерімен өзара байланысын анықтайды.

Қорғаныстың басқа сервистеріне қатысы сияқты қауіпсіздік оқиғаларын есепке алу іске асырылушы қауіпсіздік саясатымен түпнұсқада ғана жүргізіледі.

4-бөлімде келтірілген қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу үлгісі көптеген мақсаттарды көздейді. Олардың барлығы да нақты бір ортада қажет және қалаулы бола бермейді. Қауіпсіздік оқиғаларын есепке алу сервисіне қауіпсіздік оқиғаларын есепке алу журналына кіргізілуі тиіс оқиғаларға жөн сілтеуге мүмкіндік беретін тіркеу

органы кіреді. Аталған негіздер әртүрлі стандарттарда қолданылуы мүмкін. Соның ішінде мыналарды қоса алғанда:

1) Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу тұжырымдамасы кіретін стандарттар.

2) Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алуды қоса алғанда, абстрактілік сервистерді анықтайтын стандарттар.

3) Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алуды қолдануды сипаттайтын стандарттар.

4) Ашық жүйелер архитектурасы шегінде қауіпсіздік оқиғаларын және жедел хабарлауды есепке алуды қамтамасыз ету құралдарын анықтайтын стандарттар.

5) Қауіпсіздік оқиғаларын және жедел хабарлау механизмдерін есепке алуды сипаттайтын стандарттар.

Осы стандарттар осы стандартты былай қолдана алады:

– 1), 2), 3), 4) және 5) түрлеріндегі стандарттар осы стандарт терминологиясын қолдануы мүмкін;

– 2), 3), 4) және 5) түрлеріндегі стандарттар 6-бөлімде сипатталған құралдарды қолдануы мүмкін;

– 5) түріндегі стандарттар 7-бөлімде берілген жедел хабарлау механизмдері сипаттамасына негізделуі мүмкін.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ 1.9-2003 Қазақстан Республикасының мемлекеттік стандарттау жүйесі. Халықаралық, өңірлік және ұлттық стандарттар мен стандарттау, метрология, сертификаттау және аккредиттеу жөніндегі нормативтік құжаттарды қолдану тәртібі.

ҚР СТ ГОСТ Р ИСО/МЭК 7498-1-2008 Ақпараттық технология. Ашық жүйелердің байланысы. Базалық эталондық үлгі. 1-бөлім. Базалық үлгі.

ҚР СТ ИСО/МЭК 10181-1:1996 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ашық жүйелердің байланысы. Ашық жүйелер қауіпсіздігінің негіздері. 1-бөлім. Шолу.

ГОСТ ИСО 7498-2-2002 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Базалық эталондық үлгі. 2-бөлім. Ақпаратты қорғау архитектурасы.

3 Анықтамалар

Осы стандартта ҚР *СТ ГОСТ Р ИСО/МЭК 7498-1, ҚР СТ ИСО/МЭК 10181-1-2008,* ГОСТ ИСО 7498-2, [7] бойынша терминдер, сондай-ақ сәйкес анықтамаларымен мынадай терминдер қолданылады:

3.1. Дабыл белгілерін өңдеу процессоры (alarm processor): Дабыл белгісіне жауап ретінде тиісті әрекетті шақыратын және қауіпсіздік оқиғасы туралы хабарламаны қалыптастыратын қызмет.

3.2. Бақылаудың уәкілетті тұлғасы (audit authority): Қауіпсіздік оқиғасын есепке алуды жүргізуге қолданатын қауіпсіздік саясатының аспектілері үшін жауапты әкімгер.

3.3. Есепке алу журналын талдаушы (audit analyzer): Дабыл белгісін беруді немесе қауіпсіздік оқиғасы туралы хабарламаны талап ететін жағдайды табу мақсатында қауіпсіздік оқиғаларын есепке алу журналын талдауды іске асыратын қызмет.

3.4. Есепке алу журналының мұрағатшысы (audit archiver): Қауіпсіздік оқиғасын есепке алу журналының кейбір бөлігін мұрағаттау қызметі.

3.5. Есепке алу журналының диспетчері (audit dispatcher): Қауіпсіздік оқиғаларын есепке алу журналының бөлінген мәліметтерін есепке алу журналын жинаушыға қайта бағыттауды толық немесе ішінара қамтамасыз етуші қызмет.

3.6. Есепке алу журналының инспекторы (audit trail examiner): Бір немесе бірнеше есепке алу журналдары материалдарынан жүйедегі қауіпсіздік оқиғалары туралы есепті қалыптастыратын қызмет.

3.7. Қауіпсіздік оқиғаларын тіркеуші (audit recorder): Қауіпсіздік оқиғалары туралы жазбаны қалыптастыратын және оларды қауіпсіздік оқиғаларын есепке алу журналына енгізетін қызмет.

3.8. Жазбалар провайдері (audit provider): Тапсырылған критерийді қанағаттандыратын есепке алу журналынан жазба беруді қамтамасыз ететін қызмет.

3.9. Есепке алу журналдарын жинаушы (audit trail collector): Бөлінген есепке алу журналдарынан алынған жазбаны қауіпсіздік оқиғаларын есепке алу журналына жинайтын қызмет.

3.10. Оқиғаларды кемітуші (event discriminator): Қауіпсіздік оқиғасын бастапқы талдауды қамтамасыз ететін, және қажет болған кезде – аталған оқиғаны және/немесе ол туралы жедел хабарлауды есепке алуға бастама жасауды қамтамасыз ететін қызмет.

3.11. Дабыл белгісі (security alarm): Қауіпсіздік саясатына сәйкес тез арада жауап қайтаруды талап ететін жүйедегі қауіпсіздік оқиғасы табылған жағдайда қалыптасатын жедел хабарлау жүйесінің хабарламасы. Дабыл белгілерін беру тиісті мәндегі назарды нақты жағдайға тез арада аудару үшін қажет.

3.12. Жедел хабарлау жүйесінің әкімшісі (security alarm administrator): Оперативтік хабарлау бойынша мәселелерді шешу үшін жауапты нақты тұлға немесе процесс.

3.13. Қауіпсіздік оқиғасы (security-related event): Қауіпсіздік саясатымен қауіпсіздіктің ықтимал бұзылуы ретіндегі немесе жүйе қорғанысына қатысы бар болуы мүмкін оқиға ретіндегі кез келген оқиға. Мұндай оқиға мысалы – алдын ала анықталған алдыңғы мән жетістігі.

3.14. Қауіпсіздік оқиғасы туралы хабарлама (security audit message): Қауіпсіздіктің белгілі бір оқиғасы үшін есепке алу нәтижесі ретінде пайда болған хабарлама.

3.15. Қауіпсіздік оқиғасы туралы жазба (security audit record): Қауіпсіздік оқиғаларын есепке алу журналына бір реттік жазба.

3.16. Қорғаныс аудиторы (security auditor): Қауіпсіздік оқиғаларын есепке алу журналына қол жетімділік пен қауіпсіздік оқиғалары туралы есепті қалыптастыру рұқсат етілетін нақты тұлға немесе процесс.

3.17. Қорғаныс есебі (security report): Қауіпсіздік оқиғаларын есепке алу журналы мәліметтерін талдау нәтижесі болып табылатын және қорғаныстың бұзылу фактісін анықтау үшін қолданылуы мүмкін есеп.

4 Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу

Бұл бөлім ашық жүйелер үшін қауіпсіздік оқиғаларын есепке алу және олар туралы жедел хабарлау үлгісін сипаттайды.

Қауіпсіздік оқиғаларын есепке алу қарастырылып отырған қауіпсіздік саясатының баламалығын, қорғаныс бұзылушылықтарын табу құралдарын бағалауға мүмкіндік береді, лауазымды тұлғалардың өз әрекеттері үшін (немесе олардың атынан әрекет етуші объектілер әрекеті үшін) жауап беру сезімінің артуына ықпал жасайды, қор көздерін дұрыс емес қолдануды табуға көмектеседі, жүйеге залал келтіруге әрекет жасауға қабілетті тұлғаларға қатысты қорқытушы құрал ретінде әрекет болады. Қауіпсіздік оқиғаларын есепке алу механизмдері қорғаныстың бұзылуын болдырмауда тікелей қатыспайды, олар мұндай оқиғаларды тіркеуді және талдауды жүзеге асыра отырып, оларды табумен байланысты. Бұл штаттық емес оқиғаларға, мысалы, қауіпсіздіктің бұзылуына жауапты жүзеге асыратын тәртіптерге өзгертулерді жедел енгізуге мүмкіндік береді.

Дабыл белгісі тез арада жауап қатуды талап етуші ретінде қорғаныс саясатымен анықталатын қауіпсіздіктің кез келген оқиғасын тапқаннан кейін қалыптасады. Бұл алдын ала белгіленген алғашқы мән деңгейі жетістіктері жағдайы болуы мүмкін. Бұл оқиғалардың кейбіреулері тез арада қалпына келтіру әрекеттерін талап етуі мүмкін, ал ол уақытта басқалары қандай да бір әрекеттер талап етіле ме, және қандай әрекеттер екенін анықтау үшін одан әрі тергеуді талап етуі мүмкін.

Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу үлгілерін іске асыру кезінде қауіпсіздік оқиғаларын және жедел

хабарлауды есепке алу құралдарының жұмыс істеуін, сондай-ақ олардың нақты және тиімді жұмыс істеуін қамтамасыз ету үшін басқа қорғаныс сервистерін тарту талап етілуі мүмкін. Бұл тақырып осы стандарттың 8-бөлімінде толығырақ қарастырылады.

Қауіпсіздік оқиғаларын есепке алу журналдары мен тәртіптері ерекше сипаттамада болғандығына қарамастан, есепке алудың басқа журналдары (қауіпсіздік оқиғаларын есепке алуға жатпайтын) аталған негіздерде сипатталған құралдар мен механизмдерді қолдануы мүмкін.

Қорғаныстың басқа аспектілеріне қатысы сияқты, ең жоғарғы тиімділік қауіпсіздік оқиғаларын белгілі бір есепке алу талаптары ішкі жүйелік мақсатта болуына кепілдік берілген кезде ғана қол жеткізілуі мүмкін. Сәйкесінше, жүйелік әзірлеушілер әзірлеу кезінде жобалау процесінің және жүйенің өзінің тексерілу (яғни, сараптамаға және талдауға дайындығын) қажеттілігін назарда ұстаулары тиіс.

Ескертпе − Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу үлгісі басқа жүйені басқаруға және осы сипатталып отырған үлгімен тиісті қызметтік мүмкіндіктермен өзара қатынасты білдіре алмайды.

4.1. Үлгі және қызметтер

Төменде көрсетілген үлгі, қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алуды қамтамасыз ету үшін қолданылатын қызметтерді бейнелейді.

4.1.1 Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу қызметтері

Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алуды қамтамасыз ету үшін мынадай қызметтер жиынтығы қажет:

– **оқиғалар дискриминаторы**, оқиғаның бастапқы талдауын қамтамасыз етеді және оны журналға жазу үшін қауіпсіздік оқиғаларын тіркеушіге және/немесе дабыл белгілерін өңдеу процессорына жіберу туралы анықтайды:

– **қауіпсіздік оқиғаларын тіркеуші**, қауіпсіздік оқиғаларын есепке алу журналынан алынған және сақталған хабарламалардан қауіпсіздік оқиғалары туралы жазбаларды қалыптастырады;

– **дабыл белгілерін өңдеу процессоры**, қауіпсіздік оқиғасы туралы хабарламаны және дабыл белгісіне жауап ретінде тиісті іс-әрекетті қалыптастырады;

– **есепке алу журналының талдаушысы**, қауіпсіздік оқиғаларын есепке алу журналын тексереді, және қажет болған кезде дабыл белгісін және қауіпсіздік оқиғасы туралы хабарламаны қалыптастырады;

– **есепке алу журналының инспекторы**, бір немесе бірнеше қауіпсіздік оқиғаларын есепке алу журналдарынан қауіпсіздік оқиғалары туралы есептер қалыптастырады;

– **жазбалар провайдері**, белгілі бір өлшемдерге сәйкес қауіпсіздік оқиғалары туралы жазбаны қамтамасыз етеді;

– **есепке алу журналының мұрағатшысы**, қауіпсіздік оқиғаларын есепке алу журналының бір бөлігін мұрағаттайды.

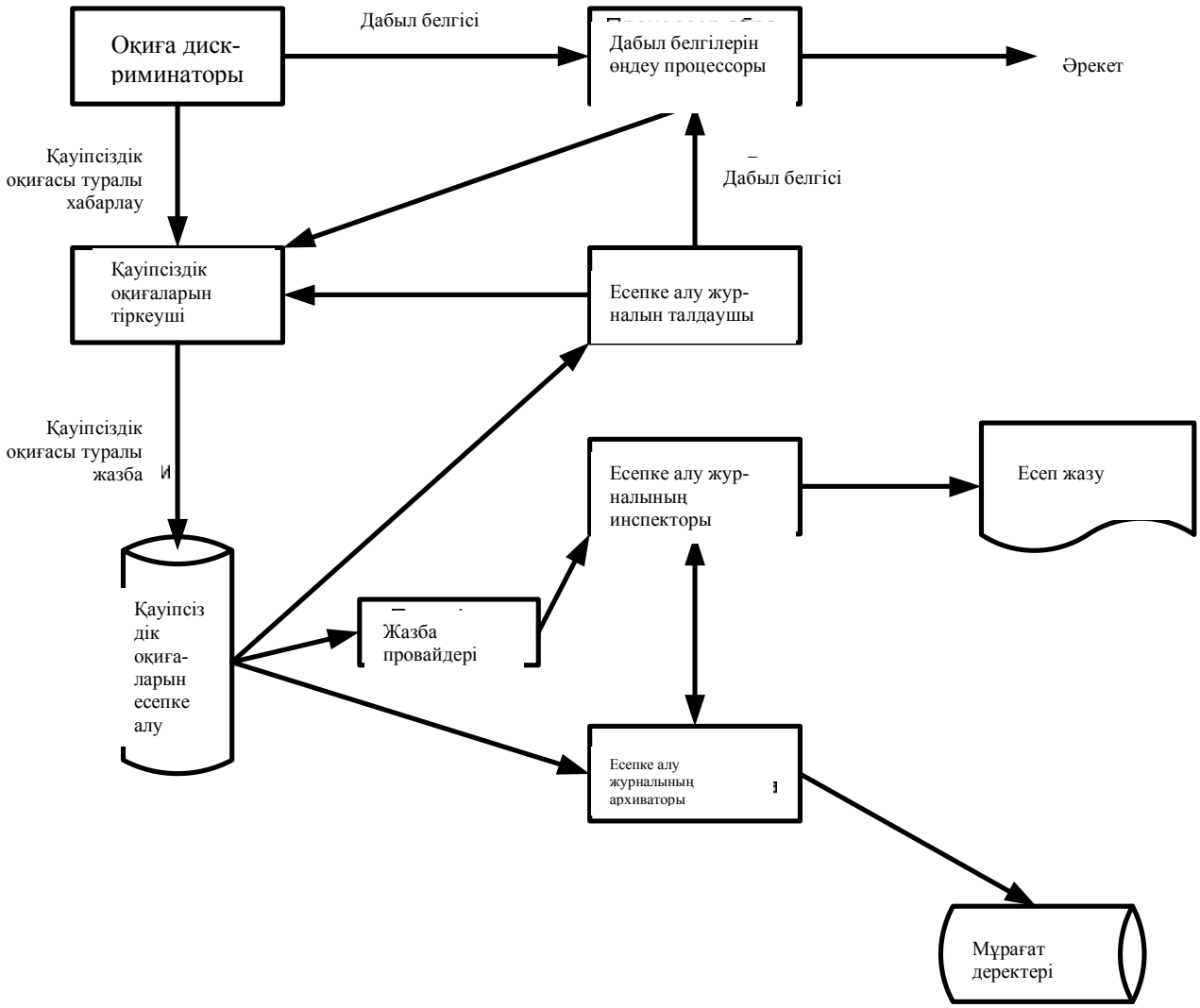
Үлестірілген қауіпсіздік оқиғаларын есепке алу журналы деректерін және жедел хабарлау деректерін қолдау үшін мынадай қосымша қызметтер қажет болуы мүмкін:

– **есепке алу журналының жинаушысы**, үлестірілген есепке алу журналдарын қауіпсіздік оқиғаларын есепке алу журналдарына жинауды жүзеге асырады;

– **есепке алу журналының диспетчері**, есепке алу журналын жинаушыға қауіпсіздік оқиғаларының есепке алынған үлестірілген деректерін ішінара немесе толық беруші.

4.1.2. Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу үлгісі

Төменде сипатталған қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу үлгісі бірнеше кезеңдерді көздейді. Оқиғаны табу және оны жүйені қорғау қатынасы пәніне сәйкестендіру орындалуы тиіс. **Оқиғалар дискриминаторы** қауіпсіздік оқиғалары туралы хабарламаны және/немесе дабыл белгісін қалыптастыру қажеттілігін анықтау үшін оқиғаны бағалайды. Қауіпсіздік оқиғалары туралы хабарламалар **қауіпсіздік оқиғасын тіркеушіге**, дабыл белгілері **дабыл белгілерін өңдеу процессорына** бұдан әрі іс-әрекетті бағалау және анықтау үшін жібереді. Қауіпсіздік оқиғалары туралы хабарламалар одан кейін пішінделіп, қауіпсіздік оқиғалары туралы жазбаларға айналады, ал олар әрі қарай қауіпсіздік оқиғаларын есепке алу журналына жазылады. Есепке алу журналындағы бұрынғы жазбалар мұрағаттануы мүмкін, ал есепке алу журналының өзі мен оның мұрағаты тапсырылған өлшемдерге сәйкес қауіпсіздік оқиғаларын есепке алу журналының нақты жазбаларын таңдау жолымен қауіпсіздік оқиғалары туралы хабарламаны жасау үшін пайдаланылуы мүмкін. Басқа сөзбен айтқанда, қауіпсіздік оқиғаларын есепке алу нәтижесі талдануы мүмкін, және қауіпсіздік оқиғалары туралы және/немесе дабыл белгілері туралы есептер қалыптастырылуы мүмкін. Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу үлгісі 1-суретте көрсетілген.



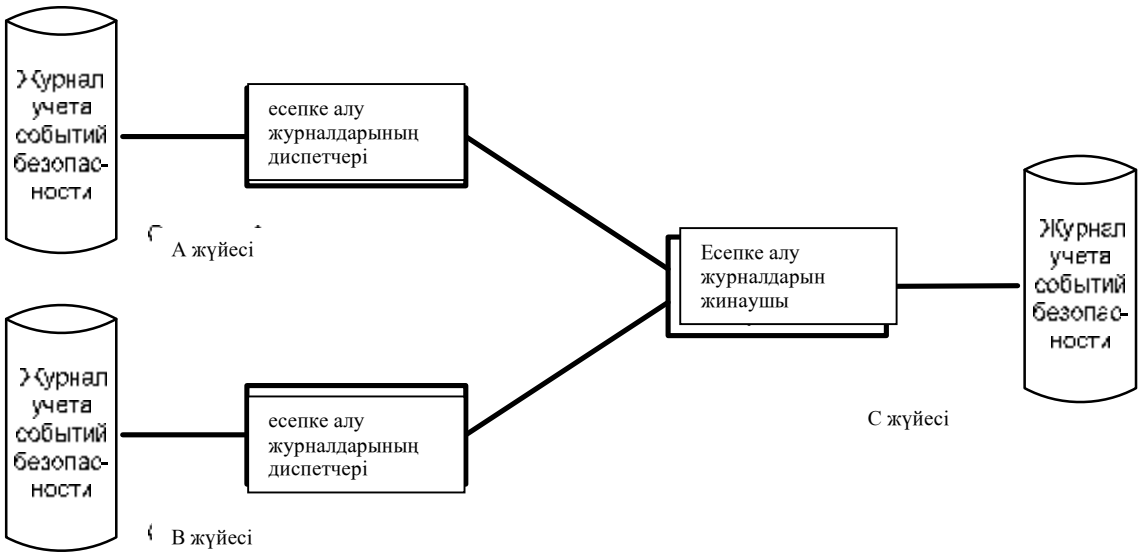
1-сурет − Қауіпсіздік оқиғасын және оларды жедел хабарлауды есепке алу үлгісі

4.1.3 Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу қызметін топтау

Үлгіде ұсынылған қызметтер жүйенің бір құрамдас бөлігінде оқшауланууы немесе жүйенің бірнеше құрамдас бөліктеріне бөлінуі мүмкін. Бұл қызметтер сонымен қатар әр түрлі түпкі жүйелерде орналасуы мүмкін және қайталануы мүмкін. Кейбір жағдайларда, мысалы, тиімділікті бағалау кезінде бұл топтауға қатысты қызмет үшін пайдалы. Көбінесе, бір қауіпсіздік оқиғасын есепке алу журналмен жұмыс істейтін **қауіпсіздік оқиғасын тіркеуші, есепке алу журналының диспетчері, жазба провайдері** және **есепке алуды талдаушы**, автоматты түпкі жүйе бөлігін қалыптастыра алады.

Топтың басқа мысалы – қорғау аудиторы үшін пайдалы болуы мүмкін **есепке алу журналының инспекторы** және **есепке алу журналының талдаушысы.**

Сатылау тәсілімен орналастырылған қызметтердің бірізділігі болуы мүмкін, мысалы, бөлінген қауіпсіздік оқиғаларын есепке алу журналы түрінде. (2-сурет). Мұнда бір жүйенің *есепке алу журналын жинаушы* басқа жүйенің *есепке алу журналы диспетчерінен* мәліметтерді жинайды. Мұндай бірізділік, егер жүйе *есепке алу журналдарының диспетчері* қызметін қолдамаса, аяқталады: мұндай жағдайда бұл жүйе өзінің *қауіпсіздік оқиғасын есепке алу журналын* мұрағаттау үшін мүмкіндігі болу үшін *есепке алу журналының мұрағатшысы* қызметін қолдауы тиіс.



2-сурет − Қауіпсіздік оқиғасын есепке алудың бөлінген деректері үлгісі

Қандай қызметтерді топтау туралы шешім, егер мұндайлар бар болса, іске асыру мәселесі болып табылады. Жоғарыда айтылған мысалдар тек безендіру ретінде беріледі.

4.2. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу кезеңдері

Қауіпсіздік оқиғасын есепке алу сервисі қауіпсіздік оқиғаларын есепке алу журналында табылуы және тіркелуі тиіс оқиғаны, сондай-ақ дабыл белгілерін және қауіпсіздік оқиғасы туралы хабарлама шақыруы тиіс оқиғаны анықтау және таңдау мүмкіндігімен тексеруге рұқсат береді.

Қауіпсіздік оқиғасын есепке алу тәртібі мынадай кезеңдерден тұруы мүмкін:

– табу кезеңі, қорғаныс жүйесімен байланысты оқиғаны табу жүзеге асырылады;

– анықтау кезеңі, оқиғаны қауіпсіздік оқиғасын есепке алу журналына жазу немесе дабыл белгісін көтеру қажеттігі анықталады;

– дабыл белгісін өңдеу кезеңі, дабыл белгісі немесе қауіпсіздік оқиғасы туралы хабарлама беріледі;

– талдау кезеңі, қорғаныспен байланысты оқиғамен бірге және есепке алу журналында тіркелген алдын ала табылған оқиғамен түпнұсқада бағаланатын, сондай-ақ әрекетердің бірізділігі анықталады;

– агрегирлеу кезеңі, бөлінген қауіпсіздік оқиғаларын есепке алу журналдарындағы жазбалар бірыңғай есепке алу журналына жиналады;

– есепті қалыптастыру кезеңі, есепке алу журналдары жазбаларынан қауіпсіздік оқиғалары туралы есептер қалыптасады;

– мұрағаттау кезеңі, есепке алу журналының жазбалары есепке алу журналының мұрағатына беріледі.

Суреттелген кезеңдердің әр түрлі уақытта болуы міндетті емес, олар уақытта «жабылып қалуы» мүмкін.

4.2.1. Табу кезеңі

Табу кезеңі қорғаныс жүйесімен байланысы болуы мүмкін оқиға болды ма, әлде жоқ екендігін анықтаудан тұрады. Мұндай оқиғаға қандай әрекеттердің жауап ретінде қабылдануы тиістігін іс жүзінде анықтау оқиға дискриминаторының міндеті (4.2.2- тармақты қараңыз), бірақ кейбір жағдайларда қауіпсіздік саясатымен анықталғандай, дабыл тез арада қосылуы мүмкін.

4.2.2. Анықтау кезеңі

Қорғаныспен байланысты оқиға табылса, оқиға дискриминаторы әрекеттердің тиісті бастапқы бірізділігін анықтайды. Әрекеттер мыналар қатарынан болуы мүмкін:

– ешқандай әрекет жасамау;

– қауіпсіздік оқиғасы туралы хабарлама беру;

– дабыл белгісін қалыптастыру және қауіпсіздік оқиғасы туралы хабарлау.

Нақты оқиғаға қандай қатысты әрекеттер бірізділігі таңдалып алынатыны туралы шешім қолданыстағы қауіпсіздік саясатына байланысты.

4.2.3. Дабыл белгілерін өңдеу кезеңі

Дабыл белгілерін өңдеу кезеңінде процессор әрекеттердің дұрыс бірізділігін анықтау мақсатымен мұндай оқиғаны талдайды.

Әрекет мыналар қатарынан болады:

1) ешқандай әрекет жасамау;

2) қалпына келтіру әрекетін инициализациялау;

3) қалпына келтіру әрекетін инициализациялау және қауіпсіздік оқиғасы туралы хабарлама шығару.

Әрбір оқиға үшін әрекеттердің қандай бірізділігі таңдалып алынатыны туралы шешім қолданыстағы қауіпсіздік саясатына байланысты.

Ескертпе − 2) және 3) тармақтары аталған оқиғаны қабылдауды белгілі бір тұлғаның, мысалы, қорғау офицерінің немесе қауіпсіздік оқиғасын есепке алу әкімшісінің назарына салуы мүмкін.

4.2.4. Талдау кезеңі

Талдау кезеңінде қорғаумен байланысты оқиға әрекеттердің тиісті бірізділігін анықтау мақсатымен өңделеді. Бұл процесс қауіпсіздік оқиғасын есепке алу журналында жазылғандай бұрынғы қорғаумен байланысты оқиғалар жүйесіне қатысты ақпаратты қолдануы мүмкін.

Әрекет мыналар қатарынан болады:

– ешқандай әрекет жасамау;

– дабыл белгісін беру;

– қауіпсіздік оқиғалары туралы есеп қалыптастыру;

– дабыл белгісін беру және қауіпсіздік оқиғалары туралы есеп.

Келтірілген төрт әрекет бірізділігінің қайсысының таңдалып алынуы тиістігі туралы шешім қолданыстағы қауіпсіздік саясатына байланысты.

Талдау процесінің бөлігі ретінде қауіпсіздік оқиғасын есепке алу журналындағы және қауіпсіздік оқиғасын есепке алу журналы мұрағатындағы жазбаларды талдау жолымен алдыңғы оқиғаларға сілтемелер жасалуы мүмкін.

4.2.5. Агрегирлеу кезеңі

Есепке алу журналының бөлінген деректерінен қауіпсіздік оқиғалары туралы жеке жазбалар мерзімді түрде бірыңғай есепке алу журналына жиналуы тиіс. Бұл *есепке алу журналын жинаушыны* (жинау нүктесіне) қолдану және *есепке алу журналы диспетчері* (жойылған жүйелерде) қызметін пайдалану кіретін процесс агрегирлеу деп аталады (4.1.3. тармағында белгіленгендей бұл процесс иерархиялық болуы мүмкін)

4.2.6. Есепті қалыптастыру кезеңі

Қауіпсіздік оқиғаларын есепке алу журналы қажет болған кезде немесе қауіпсіздік саясатына сәйкес өңделуі мүмкін. Бұл өңдеуге талдау элементі кіруі тиіс және тиісті форматта есепке алу журналы жазбаларымен айлалы әрекетті жаулап алуы мүмкін. Қауіпсіздік оқиғаларын есепке алу журналын талдау нәтижелерінің қорытындылары – бұл қорғаныс қалпына келтіру жөніндегі әрекет қажет болған кезде жүйе шабуылдау әрекетіне көрсететін қауіпсіздік оқиғалары туралы есеп. Қауіпсіздік оқиғаларын есепке алу журналын талдау әсер ету деңгейін бағалау және залалды бақылаудың тиісті тәртібін анықтау үшін қолданылуы мүмкін.

Қауіпсіздік оқиғалары туралы есеп шабуыл нәтижесіндегі залал деңгейін сәйкестендіруге қорғанысты қалпына келтіру үшін қолданылуы мүмкін. Көбінесе, бұл өз құқықтарын жол берілмейтін тәсілмен іске асырушы уәкілетті қолданушымен пайдаланылған ресурстарды сәйкестендіру үшін қолданылуы мүмкін. Қауіпсіздік оқиғалары туралы есеп сонымен қатар, кез келген залалды бағалау және қажетті қалпына келтіру әрекеті мүмкіндігін қамтамасыз ету үшін қолданылуы мүмкін.

4.2.7. Мұрағаттау кезеңі

Қауіпсіздік оқиғаларын есепке алу журналын ұзақ уақыт бойы сақтау қажет етілуі мүмкін. Мұрағаттау кезеңінде қауіпсіздік оқиғаларын есепке алу журналы ақпаратының бөлігі ұзақ уақытты жады ұстаушысына кіргізілуі мүмкін. Мұрағаттау үшін қолданылатын жады алғашқы жазбалардың тұтастығын қамтамасыз етуі тиіс. Қауіпсіздік оқиғаларын есепке алу журналдарын мұрағаттау есепке алу журналы жазбаларының алғашқы қайнар көзінен оқшауланған және алыстатылған болуы тиіс. Қашықтықтан мұрағаттау мүмкіндігі қамтамасыз етілуі мүмкін.

4.3. Қауіпсіздік оқиғаларын есепке алу деректерінің өзара байланыстылығы

Бір немесе одан көп есепке алу журналдарындағы қауіпсіздік оқиғалары туралы әр түрлі жазбалар қандай да бір жолмен бір-бірімен байланысты болуы мүмкін. Мысалы, біріктіру сұрау салуы көптеген аралық жүйелер арқылы берілуі мүмкін, және нәтижесінде қауіпсіздік оқиғаларын есепке алудың әр түрлі журналдарындағы бірнеше жазбаларды қалыптастыруы мүмкін. Бұл жазбалар уақыт бойынша анағұрлым нақты сәйкес келуі немесе өзара әрекет етуші ретінде сәйкестендірілуі үшін маңызды болуы мүмкін. Басқа мысал, екі әр түрлі оқиғаны әр түрлі қауіпсіздік оқиғаларын есепке алу журналдарында тіркеуде қай оқиғаның ертерек болғандығын анықтау мүмкіндігі қай жерде маңызды. Әр түрлі оқиғаларды уақыты бойынша өзара байланыстылығын қамтитын мәселелерді талқылау Г қосымшада берілген.

5 Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу саясаты және басқа да аспектілер

5.1. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу саясаты

Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу саясаты қауіпсіздіктің әр түрлі оқиғаларын жинау, жазу (қауіпсіздік оқиғаларын есепке алу журналына) және талдау үшін қолдануға болатын қорғаныспен байланысты оқиғаларды және ережелерді анықтайды. Ереже ретінде бірнеше

түсініктер қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу саясатына енгізілуі мүмкін. Осы түсініктердің бір немесе одан көбі нақты бір қауіпсіздік саясатына қолданылуы мүмкін.

Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу саясаты әр түрлі деңгейдегі және түрдегі қауіпсіздік оқиғаларын есепке алуды орындауға арналған талаптарды, сондай-ақ дабыл белгілерін қалыптастыру өлшемдерін анықтауы тиіс. Жүйені басқару құралдарының баламалығын сынау, қауіпсіздік саясатымен келісуді растау кезінде және саясатта анықталған өзгерістерді анықтау кезінде қауіпсіздік оқиғаларын есепке алу журналы жазбаларын және жүйелерді жобалаудың, құрылысын салудың және қызмет жасауының көптеген басқа аспектілерін талдау үшін басқару құралдары мен тәртіптері қажет болуы мүмкін.

Ескертпе − Саясатқа сәйкес қорғаныспен байланысты оқиғаны анықтау тәсілі *ҚР осы* стандарттың қолданылу аумағынан тыс жерде болып табылады.

5.2. Заңдық аспектілер

Көптеген елдерде азаматтардың жеке құпиясын қорғауға арналған заңдар бар. Кейбір жағдайларда бұл ресми емес сипаттағы қауіпсіздік оқиғаларын есепке алу журналындағы жазба ұлттық, мысалы, жеке меншікті және жеке ақпаратқа қол жетушілікті қорғауға жататын заңдар шегінде екендігін білдіреді. Мұндай жазбалар рұқсат етілмеген қол жетушіліктен қорғауды талап етуі мүмкін.

Заңды негізделген айғақтар ретінде есепке алу журналы жазбаларын қолдану кезінде мұндай деректерді қолдануға, сақтауға және қорғауға қатысты арнайы талаптар болуы тиіс.

5.3. Қорғауды талап ету

Қорғаудың екі аспектісін қарастыруға болады:

– қауіпсіздік оқиғаларын есепке алу журналын және қауіпсіздік оқиғаларын есепке алу ақпаратын қорғау;

– қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу сервисін қорғау.

5.3.1. Қауіпсіздік оқиғаларын есепке алу деректерін қорғау

Қауіпсіздік оқиғаларын есепке алу журналына жиналған ақпарат қауіпсіздік оқиғалары туралы хабарламадан немесе қауіпсіздік оқиғаларын есепке алудың басқа журналдарынан тікелей берілуі мүмкін. Сәйкесінше, қауіпсіздік оқиғаларын есепке алу журналы қауіпсіздік оқиғаларын есепке алу журналдарының бір немесе одан көп қайнар көздерден жазбаларын агрегирлеу ретінде қарастырылуы мүмкін. Жай жағдайда, қауіпсіздік оқиғаларын есепке алу журналында бір жүйемен қалыптастырылған қауіпсіздік оқиғалары туралы барлық жазба болады.

Қауіпсіздік оқиғаларын есепке алу журналы рұқсатсыз ашудан және/немесе рұқсат етілмеген түрлендіруден қорғалуы тиіс. Оны қорғау үшін қол жетімді, құпиялылықты, біртұтастықты және тең түпнұсқалық механизмдерін бақылау қолданылуы мүмкін. Қолданылатын қорғау әдістемесі мысалдарының бірі – бұл жазбаларды салуға немесе бұрынғы жазылған деректерді жоюға жол бермес үшін қауіпсіздік оқиғалары туралы жазбаны бір реттік жазу мүмкіндігі бар ұстаушыда сақтау.

Қауіпсіздік оқиғалары туралы хабарламалар, дабыл белгілері және қауіпсіздік оқиғалары туралы есептер де заңсыз ашу және/немесе құқықсыз түрлендіруге қарсы қорғалуы тиіс. Бұдан басқа, ақпаратты жіберуші мен алушыда ақпараттың бұзылуын кез келген тәсілмен болдырмау үшін деректер мекен-жайы және қайнар көз үшін белгіленген құпиялылықтың тиісті деңгейі болуы тиіс.

Сонымен қатар бұл ақпараттың ең болмаса бір бөлігінің құпиялылығын сақтау талап етілуі мүмкін. Мұның себептері бірнеше болуы мүмкін:

– жеке меншікке қатысты заңдық аспектілер;

– қандай оқиғалардың тіркелгендігін, қайсыларының тіркелмегендігін ашу;

– жедел хабарлау нәтижесі болып табылатын ықпал етулерді алушылардың (немесе алмаушылардың) сәйкестігін ашу.

5.3.2. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу сервисін қорғау

Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу сервисі оның қол жетімділік деңгейінің қаншалықты жоғарылығына байланысты. Сервистен бас тарту қауіпсіздік оқиғаларын және олар туралы жүйеде жедел хабарлауларды есепке алу үшін қауіпті болып табылады. Жедел хабарлау жүйесі әкімшісі немесе қорғау аудиторы үшін арналған ақпарат өзінің құндылығын жоғалтқанға дейін кешіктірілуі мүмкін. Мұндай ақпараттың мекен-жай иесіне уақтылы жетуі төтенше маңызды.

Бұл қорғау аспектілерін әрі қарай талқылау 8-тармақта берілген.

6 Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпараты мен құралдары

Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу ақпаратын өңдеу екі аспектіде қарастырылуы мүмкін:

– күтпеген оқиғаға жауап ретінде қалыптасқан хабарламаны өңдеу (мысалы, қауіпсіздік оқиғаларын есепке алудың алдын ала болжанбаған ақпараты немесе қауіпсіздік оқиғалары туралы жедел хабарлау ақпараты);

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алудың ерекше ақпаратына сұрау салуларын (мысалы, сұрау салынған ақпаратты) өңдеу.

Басқарушы сервистер қауіпсіздік оқиғаларын есепке алу журналына қызмет көрсету механизмдерін, қауіпсіздік оқиғасы табылған кезде нақты әрекетті анықтайтын өлшемдерді, сондай-ақ қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпаратын өңдеуді қоса алғанда, қауіпсіздік оқиғаларын және жедел хабарлауды есепке алудың бірнеше аспектілерін бақылау үшін қажет.

6.1. Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу ақпараты

Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу ақпаратына дабыл белгілері, қауіпсіздік оқиғалары туралы хабарламалар/жазбалар/есептер кіреді

6.1.1. Қауіпсіздік оқиғалары туралы хабарламалар

Қауіпсіздік оқиғасы туралы хабарлама - тексерілген қауіпсіздік оқиғасы нәтижесінде қалыптастырылған хабарлама.

Қауіпсіздік оқиғасы туралы хабарлама, мысалы, **оқиға дискриминаторы** көмегімен оқиға жүйесін қорғаумен байланысты бастапқы талдау нәтижесінде немесе **дабыл белгілерін өңдеу процессорымен** немесе **есепке алу журналын талдаушымен** мынадай бақылау нәтижесінде қалыптастырылуы мүмкін.

6.1.2. Қауіпсіздік оқиғалары туралы жазбалар

«**Қауіпсіздік оқиғалары туралы жазбалар**» термині қауіпсіздік оқиғаларын есепке алу журналында жалғыз жазбаны сипаттау үшін қолданылады. Көптеген жағдайларда бұл жүйені қорғаумен байланысты жалғыз оқиғаға сәйкес келеді, бірақ іске асырудың кейбір нұсқаларында мұндай жазбалардың қорғаумен байланысты біреуден артық оқиға нәтижесінде қалыптастырылуына жол беріледі.

Қауіпсіздік оқиғаларын есепке алу журналындағы типтік жазба хабарлама көзі мен себебіне қатысты ақпараттан тұрады, және табу және хабарламаны өңдеу процесстеріне тартылған объектілерге қатысты деректерден тұруы мүмкін.

6.1.3. Дабыл белгісі

Дабыл белгісі – бұл қауіпсіздіктің ықтимал бұзылуы және дабыл белгісінің беру шартын қанағаттандырушы ретінде сәйкестендірілген, қауіпсіздік оқиғасы табылғаннан кейін қалыптасқан хабарлама. Бұл бір реттік жағдай және тапсырылған бастамалық мақсат жетістігінің нәтижесі

болуы мүмкін. Кез келген жағдайда дабыл белгісін беру шартын анықтау қауіпсіздік саясатынан кілтті шарт болып табылады.

Дабыл белгісі дабыл белгісін беруді талап ететін штаттық емес шарттардың бар-жоқтығын анықтаған жағдайда **оқиға дискриминаторымен** (штаттық емес оқиғаны бастапқы бағалау нәтижесі ретінде) немесе **есепке алу журналының талдаушысымен** бастама жасалуы мүмкін.

6.1.4. Қорғау есептері

Қорғау есептері – бұл қауіпсіздік оқиғаларын есепке алу журналын талдау нәтижесінде қалыптастырылған ақпарат. **Есепке алу журналының инспекторы** бір немесе одан көп қауіпсіздік оқиғаларын есепке алу журналдарынан есептерді қалыптастыру үшін қолданылады.

6.1.5. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпаратын құрастыру мысалы

Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу ақпараты:

– ақпарат/хабарлама түрінен (яғни дабыл белгісі, қауіпсіздік оқиғалары туралы хабарлама немесе қорғаныс есебі);

– элементтер айырмашылығын сәйкестендіргіш (мысалы, қорғаныспен байланысты оқиғаға арналған қайнар көзден/мақсаттардан);

– хабарлама себебінен;

– оқиға дискриминаторының, жазбалар провайдерінің және/немесе қауіпсіздік оқиғасы тіркеушісінің айырмашылығын сәйкестендіргіштен тұрады.

6.2. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу құралдары

Қорғаныста тексеруді тиімді қолдану және оқиғаларды тиімді талдауды қамтамасыз ету үшін жүйені қорғаумен байланысты оқиғаларды және оларды өңдеу тәсілдерін анықтау әдістемесі қажет етіледі. Хабарламалар талдауы қауіпсіздік оқиғасы туралы хабарламаны алғаннан кейін жасалуы тиіс тиісті іс-әрекетті анықтайтын сүзгіден өткізу механизмімен жүзеге асырылады. Сүзгі әрбір түрдегі хабарламаны алған кезде орындалуы тиіс әрекетті анықтайтын (аудиторлық өкілеттіктермен белгіленген) өлшемдерге сәйкес әрекет жасайды. Ықпал жасауы тиіс өлшемдер:

– тәулік уақыты;

– бастапқы мәнге жету оқиғаларының есептеуші;

– оқиға түрі;

– оқиға себебі болып табылатын объект.

Сүзгі тиімді басқару мақсатында нақты қасиеттері және параметрлері бар басқарылатын объект ретінде анықталуы мүмкін.

Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу құралдары қауіпсіздік оқиғаларын және жедел хабарлауды есепке алуды іске асыру үшін қажетті ақпаратты пайдаланушыға өңдеуге мүмкіндік беретін іріктеу өлшемдерін орнату тәсілдерін қамтамасыз етеді. Кең мағынада бұл құралдар мыналар:

– қауіпсіздік оқиғасын өңдеу өлшемдерін жасау, түрлендіру және жою;

– қауіпсіздік оқиғалары туралы нақты хабарламаны қалыптастыруға рұқсат беру және тыйым салу;

– қауіпсіздік оқиғалары туралы жазбаларды қалыптастыруға рұқсат беру және тыйым салу;

– дабыл белгілерін және/немесе оларға жауап қайтаруды қалыптастыруға рұқсат беру және тиым салу.

Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алудың атқарымдық мүмкіндіктері мынадай:

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпаратын қалыптастыру (мысалы, дабыл белгісін беру, қауіпсіздік оқиғасы туралы хабарлама беру, қауіпсіздік оқиғасы туралы есепті қалыптастыру);

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпаратын жазу;

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпаратын жинау/агрегирлеу;

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпаратын талдау;

– қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу ақпаратын мұрағаттау.

6.2.1. Қауіпсіздік оқиғасын анықтау және талдау. Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу қызметтері үшін өлшемдер

Дабыл белгісі де, қауіпсіздік оқиғасы хабарлама да оқиға түрін, оның себебін, табу уақытын, аталған оқиғамен байланысты оқиға көрсеткіші мен объект қасиеттері ақпаратының ұқсастығын (яғни, оқиғаның алғашқы себебі болып табылатын әрекеттің субъектісі мен объектісі) сәйкестендіреді.

Өлшемдер ақпараттың әр түрлі түрлерін өңдеу кезінде алдын ала қолданылатын әрекетті анықтау үшін белгіленген. Мынадай өлшемдер анықталған:

1-өлшем. Оқиғаны анықтау

Бұл өлшемдер жүйені қорғаумен байланысты оқиғаны тапқаннан кейін қолданылатын әрекетті анықтайды.

Мүмкін болатын кіру параметрлері:

– қорғаумен байланысты оқиға түрі;

– тәулік уақыты;

– оқиға себебі болып табылатын объектіні анықтау.

Мүмкін болатын шығу параметрлері:

– қолданылатын әрекет;

– қалыптастырылатын дабыл белгісі;

– қауіпсіздік оқиғасы туралы қалыптастырылатын хабарлама.

2-өлшем. Қауіпсіздік оқиғасын есепке алу журналын инспекциялау

Бұл өлшемдер қорғаныс есептерін келісу мақсатында бір немесе одан көп журналдардағы ақпаратты таңдау үшін негіздеме береді.

Мүмкін болатын кіру параметрлері:

– қауіпсіздік оқиғасы туралы жазба түрі;

– қауіпсіздік оқиғасының түрі;

– қаралып отырған оқиғаның пайда болған уақыты;

– ақпарат сұралып отырған объектіні анықтау;

Мүмкін болатын шығу параметрлері:

– таңдалып алынған жазбалар тізімі.

3-өлшем. Қауіпсіздік оқиғасын есепке алу журналын талдау өлшемі

Бұл өлшем есепке алу журналы деректері есепке алу журналының талдаушысымен қалай өңделетінін анықтайды. Қауіпсіздік оқиғасын есепке алу журналы қолданылатын әрекетті анықтағанға дейін пайда болу уақытын және оқиғалардың жиілігін бағалау арқылы талдануы тиіс.

Мүмкін болатын кіру параметрлері:

– оқиға түрі;

– оқиғалар саны;

– оқиғаның пайда болу уақытының кезеңі.

Мүмкін болатын шығу параметрлері:

– қолданылатын әрекет.

Ескертпе − қауіпсіздік оқиғасын тіркеу немесе олар туралы ақпаратты мұрағатқа орналастыру үшін өлшемдер талап етілмейді.

7 Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу тетіктері

Қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу сервисі *ҚР СТ ИСО/МЭК 10181* стандарттарының осы сериясында сипатталған басқа қорғаныс сервистерінен аталған сервистің қызмет істеуін қамтамасыз ету үшін қолданылуы мүмкін қорғаныстың ешқандай да белгілі бір механизмінің жоқтығымен ерекшеленеді. Есепке алу механизмдері әкімшілік және функционалдық амалдар қатарына негізделген тәртіптер ретінде сипатталуы мүмкін. Сондықтан есепке алу механизміне ешқандай да толық суреттеу енгізілмеген. Бірақ қауіпсіздік оқиғаларын есепке алу үшін қолданылатын амал мысалы сияқты, қауіпсіздік оқиғаларын талдау механизмдерінде:

– белгілі мысалға қатысты объект қызметін салыстыру, мысалы, уақыт және орналасуы бойынша дәстүрлі емес қол жетім, ресурстарды әдеттегідей емес қолдану және т.б.;

– біршама уақыт кезеңі шегінде оқиғаның бір немесе бірнеше типтерінің жиналуын табу;

– біршама уақыт ішінде жағдайдың бір немесе бірнеше типтерінің пайда болуының жоқтығын бақылау болуы тиіс.

Мысалдардың жоғарыда аталған тізбегі – мұнымен бітпейді.

8 Басқа сервистермен және қорғаныс тетіктерімен өзара байланысы

8.1. Объектіні сәйкестендіру

Есепке алу журналдарының диспетчері мен **есепке алу журналдарын жинаушы** арасындағы есепке алу журналы деректерінің орын ауыстыруы **есепке алу журналдарының диспетчері есепке алу журналын жинаушыға** арналған қауіпсіздік оқиғаларын есепке алу журналын беретіндей етіп, ал **есепке алу журналын жинаушы** өз кезегінде тағайындалған диспетчерден есепке алу журналын алатындай етіп өзара тең түпнұсқалауды қажет етеді.

8.2. Деректердің шығу тегін сәйкестендіру

Деректердің шығу тегін тең түпнұсқалау қауіпсіздік оқиғалары туралы хабарламалардың және дабыл белгілерінің шығу тегі нақты анықтау үшін қолданылады. Ол сонымен қатар, есепке алу журналын талдаушымен оқиғаның таныс емес көздерінен немесе таныс емес есепке алу журналын талдаушылардан хабарламаларды елемеуге кепілдік беру үшін қолданылады.

8.3. Қол жетімділікті басқару

Қол жетімді басқару құралдары қауіпсіздік оқиғаларын есепке алу журналдарын сақтау және беру кезінде қолданылуы тиіс. Қол жетімді басқару сонымен қатар қауіпсіздік оқиғасын есепке алу журналының ақпаратына рұқсат етілмеген қол жетімді болдырмау үшін қолданылуы мүмкін.

8.4. Құпиялылық

Құпиялылықты қамтамасыз ету құралдары қауіпсіздік оқиғаларын есепке алу журналдарын, қауіпсіздік оқиғалары туралы таңдалып алынған жазбаларды, қауіпсіздік оқиғалары туралы хабарламаларды және дабыл белгілерін беру уақытында қолданылуы мүмкін. Құпиялылықты қамтамасыз ету құралдары сонымен қатар сақталатын қауіпсіздік оқиғалары туралы жазбаларды қорғау үшін қолданылуы мүмкін.

8.5. Тұтастық

Қауіпсіздік оқиғаларын есепке алу журналын, қауіпсіздік оқиғалары туралы таңдалып алынған жазбалар пакеттерін, қауіпсіздік оқиғалары туралы хабарламаларды немесе дабыл белгілерін кез келген заңсыз түрлендірулер табылатындай болуы ең маңызды. Деректердің тұтастығы мен бүтіндігін қамтамасыз ету құралдары осы мақсат үшін арналған.

8.6. Бас тартпаушылық

Есепке алу журналдарының орнын ауыстыру бір қауіпсіздік доменінің шегінде болатындықтан бас тартпаушылықты қамтамасыз ету құралдары әдетте қолданылмайды.

А қосымшасы
(анықтамалық)
АЖБ негізгі эталондық үлгі негізінде қауіпсіздік оқиғаларын және жедел хабарлауды есепке алу

Қауіпсіздік оқиғаларының мынадай түрлерін міндетті түрде есепке алу ұсынылады:

– қорғау деректерін басқаруға қатысты операциялар;

– оқиғаларды есепке алуға арналған бірізділікті өзгерту операциялары;

– тексерілетін объектілерді сәйкестендіруді өзгертуші операциялар.

Осы қосымша жүйені қорғаумен байланысты ықтимал оқиғалар болуы мүмкін ВОС негізгі эталондық үлгісінен оқиғаларды анықтайды. Қалыпты, сол сияқты штаттық емес жағдайларды есепке алу қажет болуы мүмкін. Мысалы, әрбір қосылу сұранысы штаттық емеске сұрау салынды ма, жоқ па, және ол қабылдады ма, жоқ па оған тәуелсіз қауіпсіздік оқиғаларын есепке алу журналында жазба объектісі болуы мүмкін.

Басқалардың арасында мынадай оқиғалар есепке алу объектісі болуы мүмкін. Бұл тізім толық емес, және тек ұсыныс ретінде ғана болып табылады.

Нақты біріктіруге жататын қауіпсіздік оқиғалары:

– біріктіру сұрау салулары;

– біріктіруді мақұлдау;

– ажыратуға сұрау салу;

– ажыратуды мақұлдау;

– біріктіру статистикасы.

Қорғаныс сервисін қолдануға қатысы бар қауіпсіздік оқиғалары:

– қорғаныс сервистерін тартуға сұрау салу;

– қорғаныс механизмдерін қолдану;

– дабыл белгісі.

Басқаруға қатысы бар қауіпсіздік оқиғалары:

– басқару операциялары.

– басқару хабарламалары.

– тексерілетін оқиғалар тізімінде кем дегенде мыналар болуы тиіс:

– еркін кіруге тыйым салу;

– өкілеттікті растау;

– өзгеру анықтауышы;

– объектіні жасау;

– объектіні жою;

– объектіні түрлендіру;

– тұтынушылар артықшылықтары.

Нақты қорғау сервистері терминдерінде оқиға жүйесін қорғаумен байланысты мыналар өте маңызды:

- сәйкестендіру:	нәтижелі іс-әрекеттерді верификациялау;
- сәйкестендіру:	істен шығудың верификациясы;
- қол жетімді басқару:	Сәтті қол жетім туралы шешім;
- еркін кіруді басқару:	Қол жетімге тыйым салу туралы шешім;
- бас тартпаушылықты	куәландырылған хабарламаны жасау;

қамтамасыз ету:	
- бас тартпаушылықты қамтамасыз ету:	куәландырылған хабарламаны алу;
- бас тартпаушылықты қамтамасыз ету:	орынды оқиғадан келеңсіз бас тарту;
- бас тартпаушылықты қамтамасыз ету:	орынды оқиғадан нәтижелі бас тарту;
- тұтастық:	Қорғаныс өзгертілуін қолдану;
- тұтастық:	Кері қорғаныс өзгертілуін қолдану;
- тұтастық:	Сәтті операцияның дұрыстығын тексеру;
- тұтастық:	істен шығудың дұрыстығын тексеру;
- құпиялылық:	Деректерді жасыруды қолдану;
- құпиялылық:	деректерді ашуды қолдану;
- оқиғаларды есепке алу:	есепке алу үшін оқиғаны таңдау;
- оқиғаларды есепке алу:	есепке алу үшін оқиғаны таңдауды жою;
- оқиғаларды есепке алу:	Есеп беретін оқиғаларды таңдау өлшемдерін өзгерту.

Ескертпе − Егер қол жетімді басқару құпиялылық тұтастығының немесе механизмдерінің негізін салу ретінде қолданылатын болса, онда «қол жетімге тыйым салу шешімімен» байланысты қауіпсіздік оқиғалары туралы жазбалар нақты құпиялылықты индикациялаумен деректерге немесе тұтастылықты бұзу әрекетіне өзгертілуі мүмкін.

Коммуникацияның нақты мысалына қатысы бар қауіпсіздік оқиғаларын есепке алу журналының барлық жазбалары оларды тіркеуге кепілдік беру үшін бір мағыналы сәйкестендірілуі тиіс.

[1]-ден алынған оқиғалармен ілесіп жүру сервисін басқару үшін және есепке алынуы тиіс қауіпсіздік оқиғаларын тіркеу таңдау өлшемдерін анықтайтын оқиғалармен ілесе жүретін анықтауыштарды кескіндеу үшін қолданылуы мүмкін.

[4]-тен алынған қауіпсіздік оқиғалары туралы есептерді жасау жөніндегі ұсыныстар қауіпсіздік оқиғалары туралы хабарламаны қалыптастыру үшін объектілермен қолданылуы мүмкін.

[2]-ден алынған ақпарат қауіпсіздік оқиғаларын есепке алу журналында сақталған қауіпсіздік оқиғалары туралы хабарламаларды таңдауды анықтау үшін қолданылуы мүмкін.

[3]-да сипатталған оқиғалар туралы жедел хабарлау сервисі дабыл белгісін беру үшін қауіпсіздік оқиғаларын есепке алу құралдарында қолданылуы мүмкін.

Б қосымшасы
(анықтамалық)
Қауіпсіздік оқиғаларын есепке алуды және олар туралы жедел хабарлауды іске асыру

Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу үлгісінің қызметтері Б.1 суретінде көрсетілген. Тәртіп толығымен әрбір жүйе тәртіптің бір немесе одан көп аспектілеріне жауапты болған жағдайда көптеген ашық жеке жүйелер арасында бөлінуі мүмкін. Мұның үлгісі Б.1 суретінде көрсетілген.

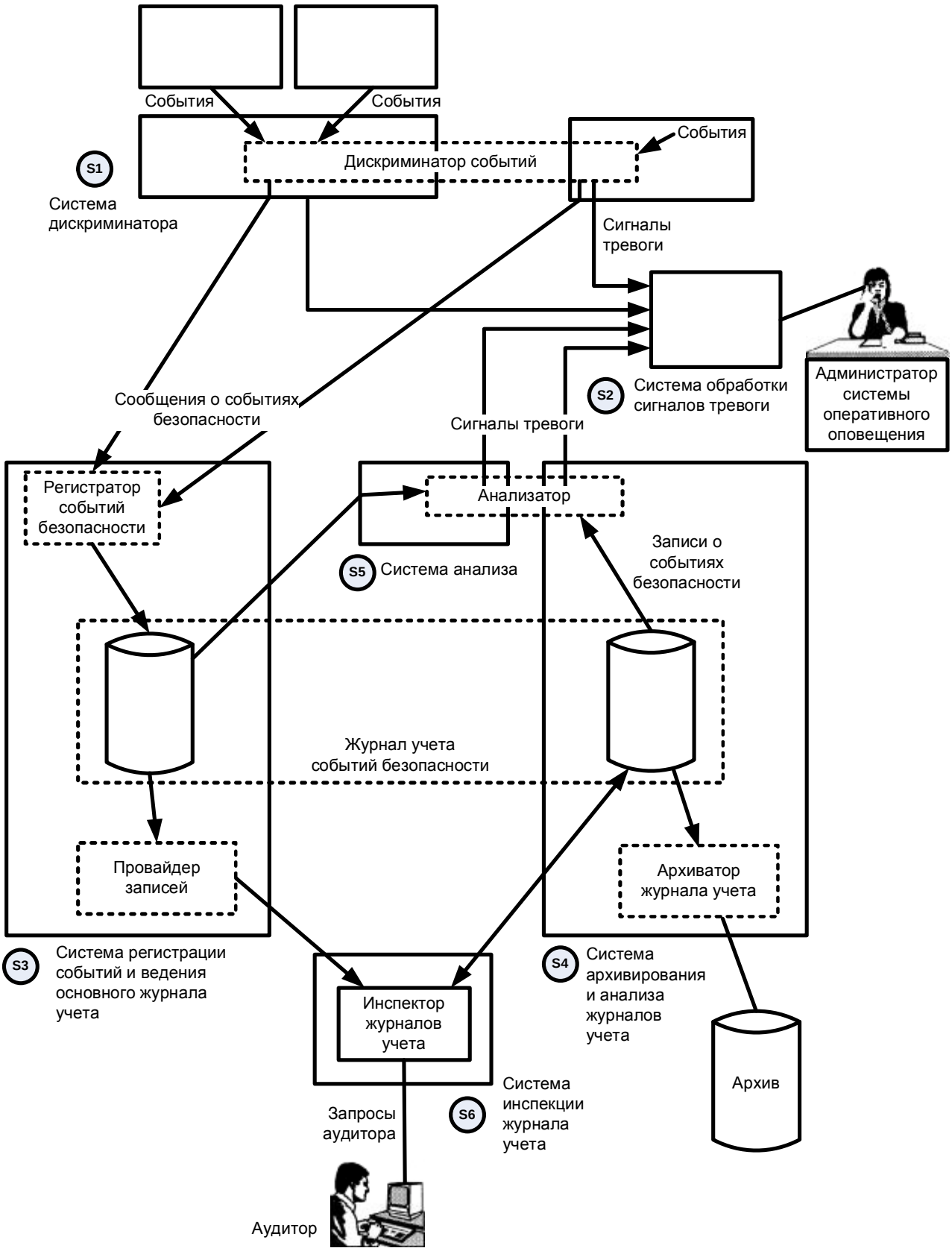
Қауіпсіздік оқиғасының мысалына, есепке алу жазбасы үшін жол берілмейтін құпия белгіні пайдалану арқылы жүйеге қосылуға талаптану себеп болуы мүмкін. Қауіпсіздік оқиғаларын есепке алу журналын талдау өтірік құпия белгімен есепке алу жазбасына қосылуға әрекет жасаулардың бірі болғандығын көрсете алуы және қорғаныс бастапқы мәнге қол жеткізілген жағдайда дабыл берілуі мүмкін еді.

S1 объектісі жүйені қорғаумен байланысты оқиғаны табуға және оларды белгілі бір өлшемдерге (1-өлшемдер) сәйкес талдауға қабілетті, бірақ оның қауіпсіздік оқиғаларын есепке алу журналына иелік ету мүмкіндігі жоқ, және де сондықтан оның қауіпсіздік оқиғалары туралы хабарламалар S2 объектісіне, ал оның қауіпсіздік оқиғалары туралы хабарламалар қауіпсіздік оқиғаларын тіркеу журналына енгізу үшін S3 объектісіне жібереді.

S3 объектісі қауіпсіздік оқиғаларын есепке алу журналының түрленуіне жауап береді. S3 сонымен қатар S6 объектісі үшін қауіпсіздік оқиғаларын есепке алу журналына және бұл журналдың мұрағаттық деректеріне қол жетімді есепке алу журналының жазбалары белгілі бір өлшемдерге (2-өлшемдер) сәйкес таңдалып, қорғаныс есебіне жинала алатындай қамтамасыз етеді.

S4 объектісі мұрағаттау және қауіпсіздік оқиғаларын есепке алу журналы жазбаларын іздеу үшін жауапты болып табылады.

S5 объектісі белгілі бір өлшемдерге (3-өлшемдер) сәйкес қауіпсіздік оқиғаларын есепке алу журналының жазбаларын талдайтын және қорғаныс бастама мәндері көтерілгенде немесе егер басқа дабыл белгілері табылған жағдайда S2 объектісіне дабыл белгісін беретін қосымша құралдардан тұрады.



1-сурет − Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу сервисін іске асыру мысалы

События – Оқиғалар

Дискриминатор событий – Оқиғалар дискриминаторы

Система дискриминатора – Дискриминатор жүйесі

Сигналы тревоги – Дабыл белгілері

Сообщения о событиях безопасности – Қауіпсіздік оқиғалары туралы хабарламалар

Система обработки сигналов тревоги – Дабыл белгілерін өңдеу жүйесі

Администратор системы оперативного оповещения – Жедел хабарлау жүйесінің әкімшісі

Регистратор событий безопасности – Қауіпсіздік оқиғаларын тіркеуші

Анализатор – Талдаушы

Система анализа – Талдау жүйесі

Записи о событиях безопасности - Қауіпсіздік оқиғалары туралы жазбалар

Журнал учета событий безопасности – Қауіпсіздік оқиғаларын есепке алу журналы

Провайдер записей – Жазбалар провайдері

Архиватор журнала учета – Есепке алу журналын мұрағаттаушы

Система регистрации событий и ведения основного журнала учета – Оқиғаларды тіркеу және негізгі есепке алу журналын жүргізу жүйесі

Система архивирования и анализа журналов учета – Есепке алу журналдарын мұрағаттау және талдау жүйесі

Инспектор журналов учета – Есепке алу журналының инспекторы

Запросы аудитора – Аудитордың сұрау салулары

Система инспекции журнала учета – Есепке алу журналы инспекциясы жүйесі

Архив – мұрағат

Аудитор - аудитор

В қосымшасы
(анықтамалық)
Қауіпсіздік оқиғаларын және олар туралы жедел хабарлауды есепке алу құралдарының сызбанұсқасы

<table>
<tr><td colspan="3" rowspan="4">Қорғаныс құралдарының сызбанұсқасы</td><td rowspan="4">Элемент</td><td>Объектілер:</td><td colspan="3">Бақылаудың өкілетті тұлғасы; жедел хабарлау жүйесінің әкімшісі; қорғаныс аудиторы.</td></tr>
<tr><td>Қызметтер:</td><td colspan="3">Оқиғалар дискриминаторы; қауіпсіздік оқиғаларын тіркеуші; дабыл белгілерін өңдеу процессоры; есепке алу журналының талдаушысы; есепке алу журналдарының инспекторы; жазбалар провайдері; есепке алу журналдарының диспетчері; есепке алу журналдарын жинаушысы.</td></tr>
<tr><td>Ақпараттық объектілер:</td><td colspan="3">Қауіпсіздік оқиғалары туралы хабарламалар; қауіпсіздік оқиғалары туралы жазбалар; қауіпсіздік оқиғалары туралы есептер.</td></tr>
<tr><td>Сервис мақсаты</td><td colspan="3">Ашық жүйелерді қорғаумен байланысты ақпараттың тіркелгендігі, және қажет болған кезде есепке кіргізілгендігінің кепілдігі</td></tr>
<tr><td rowspan="6">І С-ӘРЕКЕТТЕР</td><td rowspan="2"></td><td>Объект</td><td colspan="4">Бақылаудың өкілетті тұлғасы</td></tr>
<tr><td>Қызмет</td><td colspan="4">Оқиғаны қорғаумен байланысты болатын анықтау және талдау</td></tr>
<tr><td colspan="2">Басқарумен байланысты іс-әрекет</td><td colspan="4">1-өлшемдер: оқиғаны анықтау
2-өлшемдер: қауіпсіздік оқиғаларын есепке алу журналын тексеру
3-өлшемдер: қауіпсіздік оқиғаларын есепке алу журналын талдау</td></tr>
<tr><td rowspan="4"></td><td>Объекті</td><td>Жедел хабарлау жүйесінің әкімшісі</td><td>Қорғаныс аудиторы</td><td>Бастамашы/мақсат субъект/объект</td></tr>
<tr><td>Қызмет</td><td>- оқиғалар дискриминаторы;
- дабыл белгілерін өңдеу процессоры;
- қауіпсіздік оқиғаларын есепке алу журналын талдаушы</td><td>- оқиға;
- дискриминатор;
- қауіпсіздік оқиғаларын есепке алу журналын талдаушы;
- қауіпсіздік оқиғаларын тіркеуші;
- есепке алу журналы;
- есепке алу журналының</td><td></td></tr>
</table>

				инспекторы; - жазбалар провайдері; - есепке алу журналының мұрағатшысы	
	Жұмыспен байланысты қызмет		- ИНФ қалыптастыру - ИНФ жинау (ИНФ - жедел хабарлау ақпараты деп түсініледі)	- ИНФ қалыптастыру - ИНФ жинау - ИНФ сараптау (ИНФ қауіпсіздік оқиғалары туралы хабарламалар түсініледі)	
И Н Ф О Р М А Ц И Я	Бақылаудың өкілетті тұлғасымен басқарылатын деректер элементі		1 - өлшемдер - Оқиға түрі - уақыт - объект	2-өлшемдер - жазба түрі - оқиға түрі	3 -өлшемдер - оқиға түрі - оқиға саны - уақыт кезеңі
			- алдын ала жасалатын іс-әрекет - қалыптастырылатын қорғау туралы ақпарат	- жазбалар тізімдері	- алдын ала жасалатын іс-әрекет
	Жұмыста қолданылатын ақпарат түрі		- хабарлама/ ақпарат түрі - бөлшектерді ажыратушы идентификаторы - хабарламалар себебі - оқиғалар дискриминаторын ажыратушы идентификатор, жазбалар провайдері және/немесе қауіпсіздік оқиғаларын тіркеуші		
	Басқару ақпараты		- пайда болған уақыты және оқиғалар саны		

Г қосымшасы
(анықтамалық)
Қауіпсіздік оқиғалары үшін уақытты тіркеу

Оқиғалардың әр түрлі қайнар көздері немесе оқиғаларды тіркеушілер арасында синхронизациялау іс жүзінде мүмкін емес. Мұндай жағдайда қауіпсіздік оқиғаларын есепке алу журналы аясында уақытша параметрлердің ара қатынасын белгілеу үшін құралдар қажет. Қауіпсіздік оқиғасы туралы жазба уақыты белгісі бар немесе жоқ қауіпсіздік оқиғасы туралы хабарламадан құралады. Егер бұл хабарламада уақыт белгісі бар болса, онда қауіпсіздік оқиғасы туралы хабарламадағы уақыт индикациясын қолдана отырып, қауіпсіздік оқиғасы туралы жазба қалыптасады. Сонымен бірге есепке алынуы тиіс оқиғаны қабылдау нәтижесінде жасалған қауіпсіздік оқиғасы туралы жазбада *қауіпсіздік оқиғасын тіркеушінің* тіректік үйлестіру белгісін қолдана отырып, уақыт белгісі болады. Екі жағдайда да оқиға көзі мен *қауіпсіздік оқиғасын тіркеуші* арасындағы өзара іс-әрекет уақыты туралы жазба жасалуы тиіс.

Алдыдағы жағдайда оқиға көзі уақытын есептеу басы мен *қауіпсіздік оқиғасын тіркеушінің* тіректік үйлестіру белгісі арасындағы айырмашылықты бағалау орындалуы тиіс.

Жазбада оқиға көзін сәйкестендіру, оқиға көзі уақытын есептеу басы, *қауіпсіздік оқиғасын тіркеушінің* тіректік үйлестіру белгісі, көрсетілген тіректік уақыт нүктелері мен бөгелуге жол беру көлемі арасындағы уақыт бойынша бөгеліс болуы тиіс. Соңғы жағдайда, жазба оқиға көзін сәйкестендіруді, *қауіпсіздік оқиғасын тіркеушінің* үйлестіру белгісін және оқиға көзі мен *қауіпсіздік оқиғасын тіркеуші* арасындағы бөгелісті бағалауға, сондай-ақ осы бөгелістің жол берілетін шектерін көрсетуі тиіс.

Әр оқиға үшін мұндай жазбаларды жасаудың іс жүзінде мәні жоқ. Мұндай жазбалар уақытша тіректік нүктелерді біріктіру немесе ауытқыма сипатына байланысты жасалуы мүмкін. Егер бақылау кезеңінен кейін бөгелістің маңызды емес мөлшері белгіленетін болса, мұндай жазбалар төмен түсірілуі мүмкін. Бөгелісті өлшеу болмаған кезде сызықтық қосымша жазу әдісі қолданылуы мүмкін.

Нақ осындай мәселе *қауіпсіздік оқиғасын тіркеуші* мен жүйенің басқа жағында орналасқан *есепке алу журналы диспетчерінің* тіректік уақыт нүктелері арасында болады. Бірақ бұл жағдайда екі жүйе де уақыт бойынша синхронизациялау болады. Бұл екі корреспондент арасындағы уақыттық айырмашылықтарды өлшеу кез келген уақытта немесе қауіпсіздік оқиғаларын есепке алу журналын жіберу кезінде орындалуы мүмкін. Оқиға туралы жазбада оқиға көзін сәйкестендіру, *есепке алу журналы диспетчерін* сәйкестендіру, *қауіпсіздік оқиғасын тіркеушінің* тіректік үйлестіру белгісі, *қауіпсіздік оқиғасын тіркеуші* мен *есепке алу журналы диспетчерінің* арасындағы уақыттық бөгелісті бағалау, және осы бөгеліске жол беру алаңы болуы тиіс.

Екі оқиғаның қайсысының бірінші болғандығын анықтау тіректік үйлестіру белгілері сериялары арасындағы бөгелісті қосу немесе шегеру және жол берудің барлық алаңдарын қосу арқылы жасалуы мүмкін. Егер нәтижеленетін бөгеліс жол беру алаңының төменгі шегінен төмен болса, онда мұндай айырмашылық жоқ болуы мүмкін.

Егер қауіпсіздік оқиғалары туралы есепті жасау қажет етілсе, осы параметр қолданылады. Есепке алу журналындағы ақпаратты қолдану кезінде әр түрлі тіректік уақыт нүктелеріне сәйкес оқиғаларды сұрыптауға болады. Бірақ, егер бөгеліске жол беру алаңы жол беру алаңына қосылған мынадай оқиғаның көрсетілген уақыттық айырмашылығынан басым болмаса ғана оқиғаларды ретке келтіруге кепілдік беруге болады. Осы мақсатпен әрбір оқиға үшін жиынтық жол беру алаңын есептеу мүмкіндігін қамтамасыз ету қажет.

Қосымша
(анықтамалық)

Библиография

[1] ИСО/МЭК 10164-5:1993 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Жүйелерді басқару. 5-бөлім. Оқиғаларды тіркеуді басқару қызметі.

[2] ИСО/МЭК 10164-6:1993 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Жүйелерді басқару. 6-бөлім. Жүйелік журналды басқару қызметі.

[3] ИСО/МЭК 10164-7:1992 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Жүйелерді басқару. 7-бөлім. Қауіпсіздік режимінің бұзылғандығы туралы белгі беру қызметі.

[4] ИСО/МЭК 10164-8:1993 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Жүйелерді басқару. 8-бөлім. Қауіпсіздік оқиғаларын есепке алу қызметтері.

[5] Ұсыныстар МККТТ X.700 (1992) МККТТ қосымшалары үшін ашық жүйелердің байланысын арналған басқару негіздері.

[6] Ұсыныстар МККТТ X.800 (1991) МККТТ қосымшалары үшін ашық жүйелердің байланысына арналған қорғаныс архитектурасы

[7] ИСО/МЭК 7498-4:1989 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Базалық эталондық үлгі. 4-бөлім. Басқару негіздері.

ӘОЖ 681.324:006.354 **МСЖ 35.100.01**

Түйінді сөздер: деректерді өңдеу, ақпараттық алмасу, желілердің байланысы, ашық жүйелердің байланысы, коммуникациялық тәртіптер, ақпаратты қорғау, қауіпсіздік технологиялары, шолу.

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ

Основы безопасности для открытых систем
Часть 7
Основы учета событий безопасности и оперативного оповещения

СТ РК ИСО/МЭК 10181-7-2008

(ИСО/МЭК 10181-7:1996 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы учета событий безопасности и оперативного оповещения», IDT)

Издание официальное

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

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан № 107-од от 25.02.2008.

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 10181-7:1996 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы учета событий безопасности и оперативного оповещения» («Information technology. Open Systems Interconnection. Security frameworks for open systems. Security audit and alarms framework»), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

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

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

Настоящий стандарт уточняет концепцию учета событий безопасности, описанную в стандарте *СТ РК ИСО/МЭК 10181-1-2008*. Концепция включает как обнаружение событий безопасности в системе, так и оперативное реагирование на них. Поэтому Основы безопасности открытых систем затрагивают как учет событий безопасности, так и схемы оперативного оповещения о них.

Учет событий безопасности является независимым рассмотрением и экспертизой событий в системе. К целям учета событий безопасности относятся:

– помощь при идентификации и анализе несанкционированных действий или атак;
– анализ гарантий того, что определенные действия могут быть приписаны объектам, ответственным за такие действия;
– вклад в разработку усовершенствованных процедур контроля ущерба;
– подтверждение соответствия действующей политике безопасности;
– отчетные данные, которые могут указывать на несоответствия системного контроля требованиям;
– идентификацию возможных необходимых изменений управления, политики и процедур защиты.

В рамках рассматриваемых Основ безопасности учет событий безопасности включает обнаружение, сбор и регистрацию различных связанных с защитой событий как из журналов учета, так и по результатам анализа этих журналов.

Требования учета событий безопасности и подотчетности заключаются в необходимости регистрации определенной информации. Учет событий безопасности гарантирует достаточность записанной информации об

установившемся порядке работы и исключительных случаях. Таким образом, более позднее расследование может выявить, имело ли место нарушение защиты, и какая именно информация или иные ресурсы были подвергнуты опасности. Соблюдение учета гарантирует регистрацию относящейся к делу информации о действиях пользователей или процессах, происходящих от их имени. Таким образом, дальнейшие выводы о действиях определенных пользователей могут быть непосредственно связаны с ними, и эти пользователи могут привлекаться к ответственности за свои действия. Ведение учета событий безопасности способствует повышению степени подотчетности.

Оперативное оповещение – это выдача предупреждений (сигналов тревоги) для определенного лица или процесса, чтобы указать на возникновение ситуации, требующей немедленного вмешательства. Цели функционирования сервиса оперативного оповещения следующие:

– сообщать о реальных или вероятных попытках нарушения защиты;

– сообщать о событиях безопасности, включая «нормальные» события;

– сообщать о случаях достижения пороговых значений.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ Основы безопасности для открытых систем Часть 7 Основы учета событий безопасности и оперативного оповещения

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт устанавливает основные положения безопасности, предназначенные для решения задачи применения сервисов безопасности в среде открытых систем. Под термином «Открытые системы» понимаются такие области, как базы данных, распределенные приложения, открытая распределенная обработка и взаимодействие открытых систем (ВОС). Основные положения безопасности не имеют отношения к методологии построения систем и к их механизмам.

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

Цель учета событий безопасности и оперативного оповещения, как описано в настоящем стандарте, должна гарантировать, что события в открытых системах обрабатываются в соответствии с действующей в данной системе политикой безопасности.

Настоящий стандарт устанавливает:

– основные концепции учета событий безопасности и оперативного оповещения;

– обобщенную модель учета событий безопасности и оперативного оповещения;

– взаимосвязи учета событий безопасности и оперативного оповещения с другими сервисами защиты.

Как и в отношении других сервисов защиты, учет событий безопасности может проводиться исключительно в контексте действующей политики безопасности.

Модель учета событий безопасности и оперативного оповещения о них, приведенная в разделе 4, преследует множество целей, не все из которых могут быть необходимы или желательны в конкретной среде. Сервис учета событий безопасности включает в себя орган регистрации, позволяющий зада-

вать события, подлежащие включению в журнал учета событий безопасности.

Данный стандарт может быть применен в различных стандартах, включая:

1) Стандарты, которые включают в себя концепцию учета событий безопасности и оперативного оповещения.

2) Стандарты, которые определяют абстрактные сервисы, включая учет событий безопасности и оперативное оповещение.

3) Стандарты, которые описывают использование учета событий безопасности и оперативного оповещения.

4) Стандарты, которые определяют средства обеспечения учета событий безопасности и оперативного оповещения в пределах архитектуры открытой системы.

5) Стандарты, описывающие учет событий безопасности и механизмы оперативного оповещения.

Эти стандарты могут применять настоящий стандарт следующим образом:

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

– стандарты типов 2), 3), 4) и 5) могут использовать средства, описанные в разделе 6;

– стандарты типа 5) могут быть основаны на характеристиках механизмов оперативного оповещения, приведенных в разделе 7.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 1.9-2003 Государственная система стандартизации Республики Казахстан. Порядок применения международных, региональных и национальных стандартов и нормативных документов по стандартизации, метрологии, сертификации и аккредитации.

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

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

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

3 Определения

В настоящем стандарте применяются термины по *СТ РК ГОСТ Р ИСО/МЭК 7498-1, СТ РК ИСО/МЭК 10181-1-2008,* ГОСТ ИСО 7498-2, [7], а также следующие термины с соответствующими определениями:

3.1 Процессор обработки сигналов тревоги (alarm processor) - функция, вызывающая соответствующее действие в ответ на сигнал тревоги и формирующая сообщение о событии безопасности.

3.2 Полномочное лицо контроля (audit authority) - администратор, ответственный за аспекты политики безопасности, применимые к проведению учета событий безопасности.

3.3 Анализатор журнала учета (audit analyzer) - функция, которая анализирует журнал учета событий безопасности в целях выявления ситуаций, требующих подачи сигнала тревоги или сообщения о событии безопасности.

3.4 Архиватор журнала учета (audit archiver) - функция, архивирующая некоторую часть журнала учета событий безопасности.

3.5 Диспетчер журналов учета (audit dispatcher) - функция, обеспечивающая перенаправление распределенных данных журнала учета событий безопасности сборщику журналов учета, частично или полностью.

3.6 Инспектор журналов учета (audit trail examiner) - функция, которая формирует отчет о событиях безопасности в системе из материалов одного или более журналов учета.

3.7 Регистратор событий безопасности (audit recorder) - функция, которая формирует записи о событиях безопасности и заносит их в журнал учета событий безопасности.

3.8 Провайдер записей (audit provider) - функция, обеспечивающая предоставление записей из журнала учета, удовлетворяющих заданному критерию.

3.9 Сборщик журналов учета (audit trail collector) - функция, которая собирает полученные записи из распределенных журналов учета в журнал учета событий безопасности.

3.10 Дискриминатор событий (event discriminator) - функция, которая обеспечивает начальный анализ события безопасности и при необходимости – инициирование учета данного события и/или оперативного оповещения о нем.

3.11 Сигнал тревоги (security alarm) - сообщение системы оперативного оповещения, которое формируется в случае обнаружения события безопасности в системе, требующего незамедлительной реакции в соответствии с политикой безопасности. Подача сигналов тревоги необходима для того, чтобы немедленно обратить внимание соответствующих сущностей на конкретную ситуацию.

3.12 Администратор системы оперативного оповещения (security alarm administrator) - конкретное лицо или процесс, ответственные за решение вопросов по оперативному оповещению.

3.13 Событие безопасности (security-related event) - любое событие, которое определено политикой безопасности как потенциальное нарушение безопасности или как событие, возможно имеющее отношение к защите системы. Пример такого события – достижение заранее определенного порогового значения.

3.14 Сообщение о событии безопасности (security audit message) - сообщение, образованное как результат учета для определенного события безопасности.

3.15 Запись о событии безопасности (security audit record) - однократная запись в журнал учета событий безопасности.

3.16 Аудитор защиты (security auditor) - конкретное лицо или процесс, которому разрешается доступ к журналу учета событий безопасности и формирование отчетов о событиях безопасности.

3.17 Отчет защиты (security report) - отчет, который является результатом анализа данных журнала учета событий безопасности и который может быть использован для определения факта нарушения защиты.

4 Учет событий безопасности и оперативного оповещения о них

Данный раздел описывает модель учета событий безопасности и оперативного оповещения о них для открытых систем.

Учет событий безопасности позволяет оценивать адекватность рассматриваемой политики безопасности, средства обнаружения нарушений защиты, способствует повышению чувства ответственности должностных лиц за свои действия (или за действия объектов, действующих от их имени), помогает в обнаружении неправильного использования ресурсов и действует как средство устрашения в отношении лиц, способных попытаться нанести ущерб системе. Механизмы учета событий безопасности не участвуют непосредственно в предотвращении нарушений защиты, они скорее связаны с их обнаружением, осуществляя регистрацию и анализ таких событий. Это позволяет оперативно вносить изменения в процедуры, осуществляемые в ответ на нештатные события, например, на нарушения безопасности.

Сигнал тревоги формируется после обнаружения любого события безопасности, которое определяется политикой защиты как требующее незамедлительной реакции. Это может быть случай достижения уровня предварительно установленного порогового значения. Некоторые из событий могут требовать немедленного восстановительного действия, в то время как другие могут требовать дальнейшего расследования, чтобы определить, требуются ли какие-то действия и какие именно.

При реализации модели учета событий безопасности и оперативного оповещения о них может потребоваться привлечение других сервисов защиты, чтобы обеспечить функционирование средств учета событий безопасности и оперативного оповещения, а также их корректное и эффективное функционирование. Данная тема рассматривается подробно в разделе 8 настоящего стандарта.

Несмотря на то, что журналы и процедуры учета событий безопасности имеют особенные характеристики, другие журналы учета (не относящиеся к учету событий безопасности) могут использовать средства и механизмы, описанные в настоящем стандарте.

Как и в отношении других аспектов защиты, максимальная эффективность может быть достигнута при гарантии того, что требования конкретного учета событий безопасности имеют внутрисистемное назначение. Следовательно, системные разработчики должны принимать во внимание необходимость проверяемости (то есть готовности к экспертизе и анализу) процесса проектирования и самой системы при разработке.

Примечание. Модель учета событий безопасности и оповещения о них не может проявить взаимоотношения управления другой системой и соответствующих функциональных возможностей с описываемой моделью.

4.1 Модель и функции

Модель, представленная ниже, описывает функции, используемые для обеспечения учета событий безопасности и оперативного оповещения о них.

4.1.1 Функции учета событий безопасности и оперативного оповещения о них

Чтобы обеспечить учет событий безопасности и оперативное оповещение о них, необходим следующий набор функций:

– **дискриминатор событий**, который обеспечивает начальный анализ события и определяет, отправить ли его регистратору событий безопасности для записи в журнал и/или процессору обработки сигналов тревоги;

– **регистратор событий безопасности**, который формирует записи о событиях безопасности из сообщений, полученных и хранимых в журнале учета событий безопасности;

– **процессор обработки сигналов тревоги**, который формирует сообщение о событии безопасности и соответствующее действие в ответ на сигнал тревоги;

– **анализатор журнала учета**, который проверяет журнал учета событий безопасности и при необходимости формирует сигнал тревоги и сообщение о событии безопасности;

– **инспектор журнала учета**, который формирует отчеты о событиях безопасности из одного или более журналов учета событий безопасности;

– **провайдер записей**, который обеспечивает запись о событии безопасности согласно определенным критериям;

– **архиватор журнала учета**, который архивирует часть журнала учета событий безопасности.

Для поддержания распределенных данных журналов учета событий безопасности и данных оперативного оповещения могут потребоваться следующие дополнительные функции:

– **сборщик журналов учета**, осуществляющий сбор распределенных журналов учета в журнал учета событий безопасности;

– **диспетчер журналов учета**, передающий сборщику журнала учета распределенные данные учета событий безопасности частично или полностью.

4.1.2 Модель учета событий безопасности и оперативного оповещения о них

Модель процесса учета событий безопасности и оперативного оповещения о них, описанная ниже, предусматривает несколько этапов. Выполняются обнаружение события и идентификация его на предмет отношения к защите системы. **Дискриминатор событий** оценивает событие, чтобы определить необходимость формирования сообщения о событии безопасности и/или сигнала тревоги. Сообщения о событиях безопасности пересылаются **регистратору событий безопасности**, сигналы тревоги пересылаются **процессору обработки сигналов тревоги** для оценки и определения дальнейшего действия. Затем сообщения о событиях безопасности форматируются и преобразуются в записи о событиях безопасности, которые далее включаются в журнал учета событий безопасности. Прежние записи в журнале учета могут быть архивированы, а сам журнал учета и его архив могут использоваться для образования сообщений о событиях безопасности посредством выбора конкретных записей журнала учета событий безопасности согласно заданным критериям. Иными словами, результат учета событий безопасности может быть проанализирован, и отчеты о событиях безопасности и/или о сигналах тревоги могут быть сформированы. Модель учета событий безопасности и оперативного оповещения о них изображена на рисунке 1.

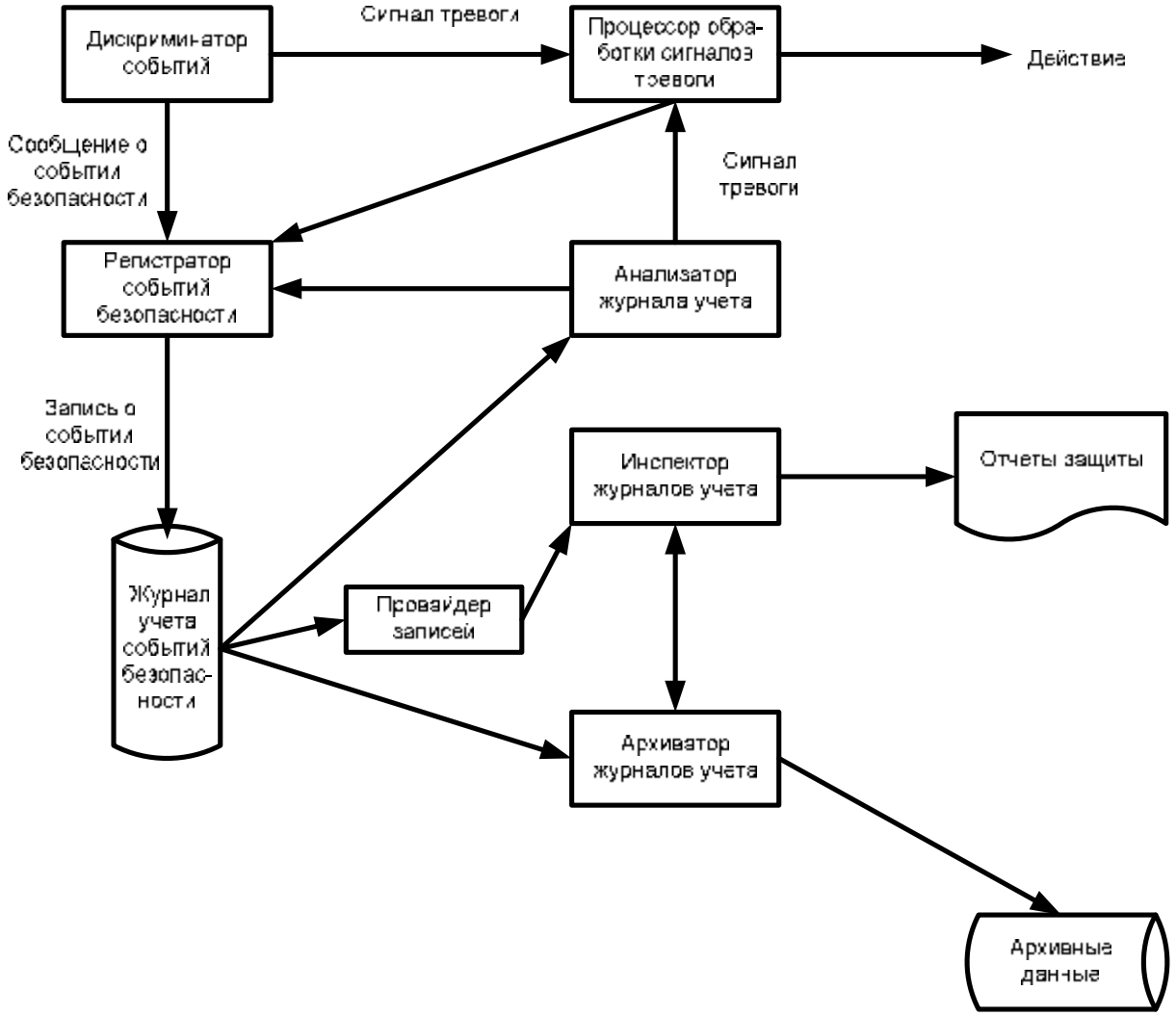


Рисунок 1. Модуль учета событий безопасности и оперативного оповещения о них

4.1.3 Группирование функций учета событий безопасности и оперативного оповещения

Функции, представленные в модели, могут быть локализованы в одном компоненте системы или распределены по нескольким компонентам системы. Кроме того, эти функции могут быть расположены в различных конечных системах и могут дублироваться. В некоторых случаях, например, при оценке эффективности, выгодно группировать функции. В частности, **регистратор событий безопасности**, **диспетчер журналов учета, провайдер записей** и **анализатор журнала учета**, работающие с одним и тем же журналом учета событий безопасности, могут формировать часть автоматической конечной системы.

Другой пример группы – **инспектор журнала учета** и **анализатор журнала учета**, которые могут быть полезны для аудитора защиты.

Может существовать последовательность функций, размещенных иерархическим способом, например, в виде распределенных журналов учета событий безопасности (рисунок 2). **Сборщик журналов учета** одной системы собирает данные от **диспетчера журналов учета** другой системы. Если система не поддерживает функции **диспетчера журналов учета,** то система должна поддерживать функцию **архиватора журнала учета**, чтобы иметь возможность архивировать свой журнал учета событий безопасности.

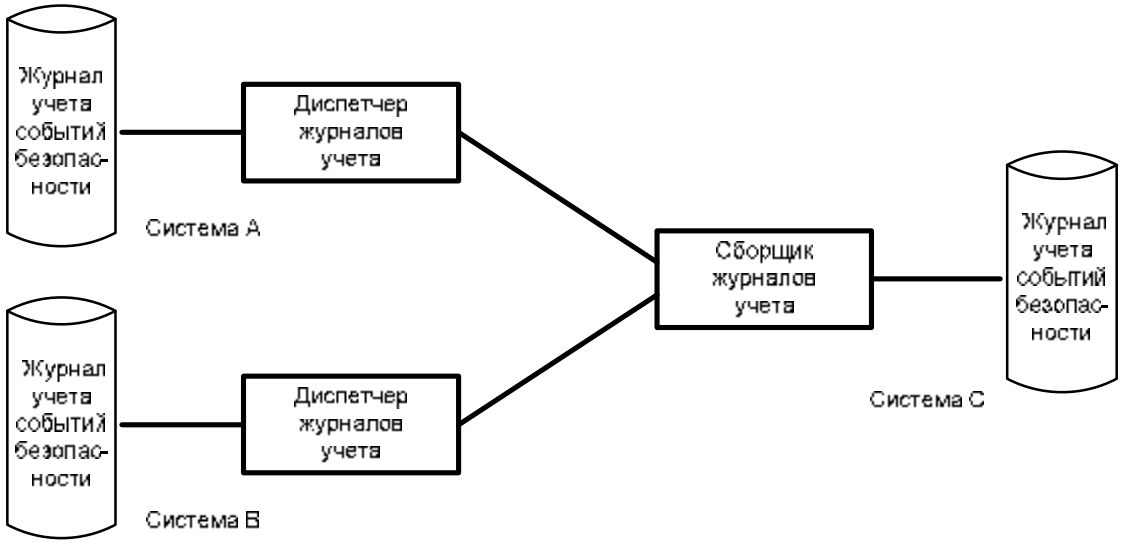


Рисунок 2. Модель распределенных данных
учета событий безопасности

Решение о том, какие функции группировать, если таковые вообще имеются, является вопросом реализации. Примеры приведены исключительно для иллюстрации.

4.2 Этапы учета событий безопасности и оперативного оповещения

Сервис учета событий безопасности дает санкцию на проверку с возможностью определения и выбора событий, которые должны быть обнаружены и зарегистрированы в журнале учета событий безопасности, а также событий, которые должны вызвать сигналы тревоги и сформировать сообщения о событии безопасности.

Процедуры учета событий безопасности могут включать в себя следующие этапы:

– этап обнаружения, на котором обнаруживаются события, связанные с защитой системы;

– этап определения, на котором определяется, необходимо ли делать запись события в журнале учета событий безопасности или поднимать сигнал тревоги;

– этап обработки сигнала тревоги, на котором выдается сигнал тревоги или формируется сообщение о событии безопасности;

– этап анализа, на котором связанное с защитой событие оценивается совместно и в контексте с предварительно обнаруженными событиями, зарегистрированными в журнале учета, а также определяется последовательность действий;

– этап агрегирования, на котором записи распределенных журналов учета событий безопасности собираются в единый журнал учета;

– этап формирования отчета, на котором отчеты о событиях безопасности формируются из записей журнала учета;

– этап архивирования, на котором записи журнала учета передаются в архив журнала учета.

Описанные этапы не обязательно должны происходить в разное время, они могут «перекрываться» во времени.

4.2.1 Этап обнаружения

На этапе обнаружения определяется, произошло ли событие, которое может быть связано с защитой системы, или нет. Фактическое определение того, какие действия должны быть предприняты в ответ на такое событие – задача дискриминатора событий (см. 4.2.2), но в некоторых случаях, как определено политикой безопасности, тревога может быть включена немедленно.

4.2.2 Этап определения

Если обнаружено связанное с защитой событие, дискриминатор событий определяет соответствующую начальную последовательность действий. Действие может быть одним из следующих:

– не предпринимать никаких действий;

– выдать сообщение о событии безопасности;

– сформировать сигнал тревоги и сообщение о событии безопасности.

Решение о том, какая последовательность действий относительно данного события будет выбрана, зависит от действующей политики безопасности.

4.2.3 Этап обработки сигналов тревоги

На этапе обработки сигналов тревоги процессор анализирует событие с целью определения правильной последовательности действий.

Действие может быть одним из следующих:

1) не предпринимать никаких действий;

2) инициализировать восстановительное действие;

3) инициализировать восстановительное действие и выдать сообщение о событии безопасности.

Решение о том, какая последовательность действий будет выбрана для каждого события, зависит от действующей политики безопасности.

Примечание. Пункты 2) и 3) могут потребовать внимания со стороны определенного лица, например, офицера защиты или администратора учета событий безопасности.

4.2.4 Этап анализа

На этапе анализа связанное с защитой событие обрабатывается с целью определения соответствующей последовательности действий. Этот процесс может также использовать информацию о прежних связанных с защитой системы событиях, как записано в журнале учета событий безопасности. Действие может быть одним из следующих:

– не предпринимать никаких действий;

– выдать сигнал тревоги;

– сформировать отчет о событиях безопасности;

– выдать сигнал тревоги и отчет о событиях безопасности.

Решение о том, какое из приведенных четырех действий должно быть выбрано, зависит от действующей политики безопасности.

В качестве части процесса анализа могут быть сделаны ссылки на предыдущие события посредством анализа записей в журнале учета событий безопасности и в архиве журнала учета событий безопасности.

4.2.5 Этап агрегирования

Индивидуальные записи о событиях безопасности от распределенных данных журнала учета должны периодически собираться в единый журнал учета. Этот процесс, включающий в себя использование **сборщика журналов учета** (в точке сбора) и использование функции **диспетчера журналов учета** (в удаленных системах), называется агрегированием. (Как отмечено в п.4.1.3, этот процесс может быть иерархическим.)

4.2.6 Этап формирования отчета

Журнал учета событий безопасности может подвергаться обработке при необходимости или в соответствии с политикой безопасности. Эта обработка должна включать в себя элемент анализа и может также охватывать манипуляцию с записями журнала учета в соответствующем формате. Результатом анализа журнала учета событий безопасности является отчет о событиях безопасности, который может указывать на попытку атаки системы, когда могут понадобиться действия по восстановлению защиты. Анализ журнала учета событий безопасности может использоваться для оценки уровня воздействия и определения соответствующих процедур контроля ущерба.

Отчет о событиях безопасности может использоваться при восстановлении защиты для идентификации степени ущерба в результате атаки. В частности, отчет может применяться для идентификации ресурсов, которые использовались уполномоченным пользователем, реализующим свои права недопустимым способом. Отчет о событиях безопасности может также применяться для оценки любого ущерба и обеспечения возможности необходимого восстановительного действия.

4.2.7 Этап архивирования

Может понадобиться хранение журнала учета событий безопасности в течение длительного времени. На этапе архивирования часть информации журнала учета событий безопасности переносится на носитель долговременной памяти. Память, используемая для архивирования, должна обеспечивать целостность первоначальных записей. Архивирование журналов учета событий безопасности может быть локальным или удаленным от первоначального источника записей журнала учета. Возможно дистанционное архивирование.

4.3 Корреляция данных учета событий безопасности

Разные записи о событиях безопасности в одном или более журналах учета могут быть каким-либо образом связаны друг с другом. Например, запрос соединения может быть передан через множество промежуточных систем и может в результате сформировать несколько записей в различных журналах учета событий безопасности. Может быть важно, чтобы эти записи имели более точную синхронизацию по времени или идентифицировались как взаимодействующие. Другой пример – регистрация двух различных событий в двух различных журналах учета событий безопасности, где важна возможность определения того, какое событие произошло раньше. Обсуждение проблем, охватывающих корреляцию во времени событий различного происхождения, приводится в Приложении Г.

5 Политика и другие аспекты учета событий безопасности и оперативного оповещения о них

5.1 Политика учета событий безопасности и оперативного оповещения

Политика учета событий безопасности и оперативного оповещения определяет связанные с защитой события и правила, которые можно использовать для сбора, записи (в журнал учета событий безопасности) и анализа различных событий безопасности. Несколько соображений могут быть включены в политику учета событий безопасности и оперативного оповещения в качестве правил. Одно или более из этих соображений могут быть применены в конкретной политике безопасности.

Политика учета событий безопасности и оперативного оповещения должна определять требования для выполнения учета событий безопасности различных уровней и типов, а также критерии формирования сигналов тревоги. При испытании адекватности средств управления системы, подтверждении согласования с политикой безопасности и при изменении политики могут понадобиться средства и процедуры управления для анализа записей журнала учета событий безопасности и многих других аспектов проектирования, архитектуры и функционирования систем.

Примечание. Способ определения связанных с защитой событий в соответствии с политикой находится вне области действия настоящего стандарта.

5.2 Юридические аспекты

Во многих странах имеются законы, предназначенные для защиты личных секретов граждан. В некоторых случаях это означает, что запись в журнале учета событий безопасности, содержащая информацию приватного характера, находится в пределах национальных законов, например, относящихся к охране частной собственности и доступа к частной информации. Такие записи могут потребовать защиты от несанкционированного доступа.

При использовании записей журнала учета в качестве юридически обоснованных улик должны существовать специальные требования к использованию, хранению и защите таких данных.

5.3 Требования защиты

Можно рассматривать два аспекта защиты:

– защита журнала учета событий безопасности и информации учета событий безопасности;

– защита сервиса учета событий безопасности и оперативного оповещения о них.

5.3.1 Защита данных учета событий безопасности

Информация, собранная в журнале учета событий безопасности, может передаваться непосредственно от сообщений о событиях безопасности или из других журналов учета событий безопасности. Следовательно, журнал учета событий безопасности может рассматриваться как агрегирование записей журналов учета событий безопасности от одного или более источников. В простейшем случае журнал учета событий безопасности содержит все записи о событиях безопасности, сформированные одной системой.

Журнал учета событий безопасности должен быть защищен от несанкционированного открытия и/или неразрешенной модификации. Для его защиты может использоваться контроль доступа, конфиденциальность, целостность и механизмы аутентификации. Один из примеров используемой методики защиты − хранение записей о событиях безопасности на носителе с однократной возможностью записи, что не допускает наложения записей или стирания записанных данных.

Сообщения о событиях безопасности, сигналы тревоги и отчеты о событиях безопасности также должны быть защищены против неправомочного раскрытия и/или неправомочной модификации. Кроме того, для предотвращения разрушения информации важно, чтобы отправитель и получатель информации имели соответствующий уровень конфиденциальности, установленный для источника и адресата данных.

Также может потребоваться соблюдение конфиденциальности, по крайней мере, части этой информации. Причиной этого могут служить:

– юридические аспекты в отношении частной собственности;

– скрытие того, какие события зарегистрированы и какие нет;

– скрытие идентичности получателей (или неполучателей) воздействий, являющихся следствием оперативного оповещения.

5.3.2 Защита сервиса учета событий безопасности и оперативного оповещения

Сервис учета событий безопасности и оперативного оповещения зависит от того, насколько высок уровень ее доступности. Отказ сервиса является угрозой для учета событий безопасности и оперативного оповещения о них в системе. Информация, предназначенная для администратора системы оперативного оповещения или аудитора защиты, может быть задержана настолько, что потеряет свою ценность. Чрезвычайно важно, чтобы такая информация приходила к адресату своевременно.

Дальнейшее обсуждение этих аспектов защиты содержится в разделе 8.

6 Информация и средства учета событий безопасности и оперативного оповещения

Обработка информации учета событий безопасности и оперативного оповещения о них может рассматриваться в двух аспектах:

– обработка сообщений, сформированных в ответ на неожиданное событие (например, непредусмотренная информация учета событий безопасности или информация оперативного оповещения о событиях безопасности);

– обработка запросов специфичной информации учета событий безопасности и оперативного оповещения (например, запрошенной информации).

Управляющие сервисы необходимы для контроля нескольких аспектов учета событий безопасности и оперативного оповещения, включая механизмы обслуживания журнала учета событий безопасности, критерии, определяющие конкретные действия при обнаружении событий безопасности, а также процессы обработки информации учета событий безопасности и оперативного оповещения.

6.1 Информация учета событий безопасности и оперативного оповещения о них

Информация учета событий безопасности и оперативного оповещения включает в себя сигналы тревоги, сообщения/записи/отчеты о событиях безопасности.

6.1.1 Сообщения о событиях безопасности

Сообщение о событии безопасности – это сообщение, сформированное в результате проверки события безопасности.

Сообщение о событии безопасности может быть сформировано, например, в результате начального анализа связанного с защитой системы события с помощью **дискриминатора событий** или в результате последующей оценки **процессором обработки сигналов тревоги,** или **анализатором журнала учета**.

6.1.2 Записи о событиях безопасности

Термин **«запись о событии безопасности»** используется для описания одиночной записи в журнале учета событий безопасности. Во многих случаях это соответствует одиночному связанному с защитой системы событию, однако допустимо также, чтобы в некоторых вариантах реализации такая запись формировалась в результате более, чем одного связанного с защитой события.

Типовая запись в журнале учета событий безопасности включает в себя информацию об источнике и причине сообщения и может также содержать данные об объектах, вовлеченных в процессы обнаружения и обработки сообщений.

6.1.3 Сигналы тревоги

Сигнал тревоги − это сообщение, сформированное после обнаружения события безопасности, идентифицированного как потенциальное нарушение безопасности и удовлетворяющего условию подачи сигнала тревоги. Это может быть одиночный случай или результат достижения заданного порогового значения. В любом случае определение условия подачи сигнала тревоги является ключевым условием политики безопасности.

Сигналы тревоги могут быть инициированы **дискриминатором событий** (как результат начальной оценки нештатного события) или **анализатором журнала учета** при условии определения наличия нештатных условий, требующих подачи сигнала тревоги.

6.1.4 Отчеты защиты

Отчеты защиты – это информация, сформированная в результате анализа журнала учета событий безопасности. **Инспектор журналов учета** используется для формирования отчетов из одного или более журналов учета событий безопасности.

6.1.5 Пример компоновки информации учета событий безопасности и оперативного оповещения

Информация учета событий безопасности и оперативного оповещения о них обычно включает в себя:

– тип информации/сообщения (т.е. сигнал тревоги, сообщение о событиях безопасности или отчет защиты);

– идентификатор различия элементов (например, источника/цели для связанного с защитой события);

– причину сообщения;

– идентификаторы различия дискриминатора событий, провайдера записей и/или регистратора событий безопасности.

6.2 Средства учета событий безопасности и оперативного оповещения

Чтобы эффективно использовать проверку защиты и обеспечить эффективный анализ событий, требуется методика определения событий, связанных с защитой системы, и способа их обработки. Анализ сообщений осуществляется механизмом фильтрации, который определяет, какое действие должно быть предпринято после получения сообщения о событии безопасности. Фильтр действует согласно критериям (установленным аудиторскими полномочиями), определяющим действие, которое должно выполняться при получении сообщения каждого типа. К критериям, подлежащим воздействию, относятся:

– время суток;

– счетчик событий достижения пороговых значений;

– тип события;

– объект, являющийся причиной события.

В целях эффективного управления фильтр может быть определен как управляемый объект с конкретными свойствами и параметрами.

Средства учета событий безопасности и оперативного оповещения обеспечивают способы установки критериев отбора, позволяющих пользователю обрабатывать информацию, необходимую для реализации учета событий безопасности и оперативного оповещения. В широком смысле это следующие средства:

– создание, модификация и удаление критериев обработки событий безопасности;

– разрешение и запрещение формирования конкретных сообщений о событиях безопасности;

– разрешение и запрещение формирования записей о событиях безопасности;

– разрешение и запрещение формирования сигналов тревоги и/или реагирования на них.

Функциональные возможности учета событий безопасности и оперативного оповещения следующие:

– формирование информации учета событий безопасности и оперативного оповещения (например, подача сигнала тревоги, выдача сообщения о событии безопасности, формирование отчета о событиях безопасности);

– запись информации учета событий безопасности и оперативного оповещения;

– сбор/агрегирование информации учета событий безопасности и оперативного оповещения;

– анализ информации учета событий безопасности и оперативного оповещения;

– архивирование информации учета событий безопасности и оперативного оповещения.

6.2.1 Определение и анализ событий безопасности. Критерии для функций учета событий безопасности и оперативного оповещения

И сигнал тревоги, и сообщение о событии безопасности идентифицируют тип события, его причину, время обнаружения, идентичность информации датчика событий и свойств объектов, связанных с данным событием (т.е. субъект и объект действия, являющегося первопричиной события).

Критерии устанавливаются с целью определения действия, предпринимаемого при обработке различных типов информации. Определены следующие критерии:

Критерий 1. Определение события

Этот критерий определяет действие, предпринимаемое после обнаружения связанного с защитой системы события.

Возможные входные параметры:

– тип связанного с защитой события;

– время суток;

– определение объекта, являющегося причиной события.

Возможные выходные параметры:

– действие, которое будет принято;

– сигнал тревоги, который будет сформирован;

– сообщение о событии безопасности, которое будет сформировано.

Критерий 2. Инспекция журналов учета событий безопасности

Этот критерий дает основание для выбора информации, содержащейся в одном или более журналов учета, с целью согласования отчетов защиты.

Возможные входные параметры:

– тип записи о событии безопасности;

– тип события безопасности;

– время появления рассматриваемого события;

– определение объекта, информация о котором запрашивается.

Возможные выходные параметры:

– список выбранных записей.

Критерий 3. Критерий анализа журнала учета событий безопасности

Этот критерий определяет, как данные журнала учета будут обработаны анализатором журнала учета. Журнал учета событий безопасности должен быть проанализирован посредством оценки времени возникновения и частоты событий до определения предпринимаемого действия.

Возможные входные параметры:

– тип события;

– количество событий;

– период времени появления событий.

Возможные выходные параметры:

– действие, которое будет принято.

Примечание. Не требуются критерии для регистрации событий безопасности или помещения информации о них в архив.

7 Механизмы учета событий безопасности и оперативного оповещения о них

Сервис учета событий безопасности и оперативного оповещения отличается от других сервисов защиты, описанных в настоящей серии стандартов *СТ РК ИСО/МЭК 10181-2008*, в том смысле, что не имеется определенного механизма защиты, который может использоваться для обеспечения функционирования данного сервиса. Механизмы учета могут быть охарактеризованы как процедуры, основанные на ряде административных и функциональных подходов. Поэтому никакое подробное описание не включено в механизмы учета. Как пример подхода, используемого для учета событий безопасности, механизмы анализа событий безопасности должны включать в себя:

– сравнение деятельности объекта с известным примером, например, нетрадиционный по времени и расположению доступ, необычное использование ресурсов и т.д.;

– обнаружение накопления одного или нескольких типов событий за некоторый период времени;

– наблюдение отсутствия возникновения одного или нескольких типов событий в течение некоторого времени.

Приведенный список – далеко не исчерпывающий.

8 Взаимодействие с другими сервисами и механизмами защиты

8.1 Аутентификация объекта

Перемещение данных журнала учета между **диспетчером журналов учета** и **сборщиком журналов учета** требует взаимной аутентификации таким образом, чтобы **диспетчер журналов учета** выдавал журнал учета событий безопасности, предназначенный **сборщику журналов учета**, а тот, в свою очередь, получал журнал учета от назначенного диспетчера.

8.2 Аутентификация происхождения данных

Аутентификация происхождения данных используется для того, чтобы точно определить происхождение сообщений о событиях безопасности и сигналов тревоги. Она также используется **анализатором журнала учета**, чтобы гарантировать игнорирование сообщений от неизвестных источников событий или от неизвестных анализаторов журнала учета.

8.3 Управление доступом

Средства управления доступом должны использоваться при хранении и передаче журналов учета событий безопасности. Управление доступом может также применяться с целью предотвращения несанкционированного доступа к информации журнала учета событий безопасности.

8.4 Конфиденциальность

Средства обеспечения конфиденциальности могут использоваться во время передачи журналов учета событий безопасности, выбранных записей о событиях безопасности, сообщений о событиях безопасности и сигналов тревоги. Средства обеспечения конфиденциальности могут также использоваться для защиты хранимых записей о событиях безопасности.

8.5 Целостность

Важно, чтобы любые неправомочные модификации журнала учета событий безопасности, пакетов выбранных записей о событиях безопасности, сообщений о событиях безопасности или сигналов тревоги могли быть обнаружены. Средства обеспечения целостности и сохранности данных предназначены для этой цели.

8.6 Неотказуемость

Поскольку перемещение журналов учета обычно производится в пределах одного и того же домена безопасности, средства обеспечения неотказуемости обычно не используются.

Приложение А
(справочное)
Учет событий безопасности и оперативного оповещения в рамках базовой эталонной модели (ВОС)

Настоятельно рекомендуется вести учет следующих типов событий безопасности:

– операции, относящиеся к управлению данными защиты;

– операции, изменяющие последовательность предназначенных для учета событий;

– операции, изменяющие идентификацию проверяемых объектов.

Настоящее приложение определяет события из базовой эталонной модели ВОС, которые потенциально могут стать событиями, связанными с защитой системы. Может потребоваться учет как нормальных, так и нештатных состояний, например, каждый запрос соединения может быть объектом записи в журнале учета событий безопасности независимо от того, был ли запрос нештатным и был ли он принят или нет.

Следующие события могут быть объектами учета. Список не исчерпывающий и является рекомендательным.

События безопасности, относящиеся к конкретному соединению:

– запрос соединения;

– подтверждение соединения;

– запрос разъединения;

– подтверждение разъединения;

– статистика соединения.

События безопасности, имеющие отношение к использованию сервисов защиты:

– запросы привлечения сервисов защиты;

– использование механизмов защиты;

– сигнал тревоги.

События безопасности, имеющие отношение к управлению:

– операции управления;

– сообщения управления.

Список проверяемых событий должен включать в себя как минимум:

– отказ в доступе;

– подтверждение полномочий;

– изменение атрибута;

– создание объекта;

– удаление объекта;

– модификацию объекта;

– изменение привилегий пользователей.

В терминах конкретных сервисов защиты особенно важны следующие связанные с защитой системы события:

– аутентификация - верификация успешных операций;

– аутентификация - верификация сбоев;

– управление доступом - решение об успешном доступе;

– управление доступом - решение об отказе в доступе;

– обеспечение неотказуемости - засвидетельствованное создание сообщения;

– обеспечение неотказуемости - засвидетельствованное получение сообщения;
– обеспечение неотказуемости - неудачный отказ от события, имевшего место;
– обеспечение неотказуемости - успешный отказ от события, имевшего место;
– целостность - использование защитного преобразования;
– целостность - использование обратного защитного преобразования;
– целостность - проверка правильности успешной операции;
– целостность - проверка правильности сбоя;
– конфиденциальность - использование скрытия данных;
– конфиденциальность - использование раскрытия данных;
– учет событий - выбор события для учета;
– учет событий - отмена выбора события для учета;
– учет событий - изменение критериев выбора подотчетных событий.

Примечание. Если управление доступом используется в качестве основания целостности или механизмов конфиденциальности, записи о событиях безопасности, связанные с «решением отмены в доступе», могут быть преобразованы в данные с явной индикацией конфиденциальности или в данные попытки нарушения целостности.

Все записи журнала учета событий безопасности, имеющие отношение к конкретному примеру коммуникации, должны быть однозначно идентифицированы, чтобы гарантировать их регистрацию.

Информация из [1] может использоваться для управления сервисом сопровождения событий и для конфигурирования определителей сопровождения событий, которые определяют критерии выбора событий безопасности, подлежащих учету.

Рекомендации по составлению отчетов о событиях безопасности из [4] могут использоваться объектами для формирования сообщений о событиях безопасности.

Информация из [2] может использоваться для определения выбора сообщений о событиях безопасности, хранимых в журнале учета событий безопасности.

Сервис оперативного оповещения о событиях, описанный в [3], может быть использован в средствах учета событий безопасности для подачи сигнала тревоги.

Приложение Б
(справочное)
Реализация учета событий безопасности и оперативного оповещения о них

Функции модели учета событий безопасности и оперативного оповещения о них показаны на рис. Б.1. Полностью процедура может быть распределена между множеством отдельных открытых систем при условии, что каждая система ответственна за один или более аспектов процедуры.

Примером события безопасности может служить попытка подключения к системе с использованием недопустимого пароля для учетной записи. Анализ журнала учета событий безопасности может показать, что это одна из ряда попыток подключения к учетной записи с ложным паролем, и тревога может быть поднята при достижении защитного порогового значения.

Объект S1 способен обнаружить связанные с защитой системы события и проанализировать их согласно определенным критериям (Критерии 1), однако не обладает возможностью иметь журнал учета событий безопасности, и поэтому его сообщения о событиях безопасности пересылаются объекту S2, а его сообщения о событиях безопасности передаются объекту S3 для включения в журнал учета событий безопасности.

Объект S3 отвечает за модификацию журнала учета событий безопасности. S3 также обеспечивает для объекта S6 доступ к журналу учета событий безопасности и к архивным данным этого журнала таким образом, чтобы записи журнала учета могли выбираться согласно определенным критериям (Критерии 2) и могли быть собраны в отчет защиты.

Объект S4 является ответственным за архивирование и поиск записей журнала учета событий безопасности.

Объект S5 содержит дополнительные средства, которые анализируют записи журналов учета событий безопасности (и архивированные записи) согласно определенным критериям (Критерии 3) и выдает объекту S2 сигнал тревоги, как только превышаются защитные пороговые значения или если обнаруживаются другие сигналы тревоги.

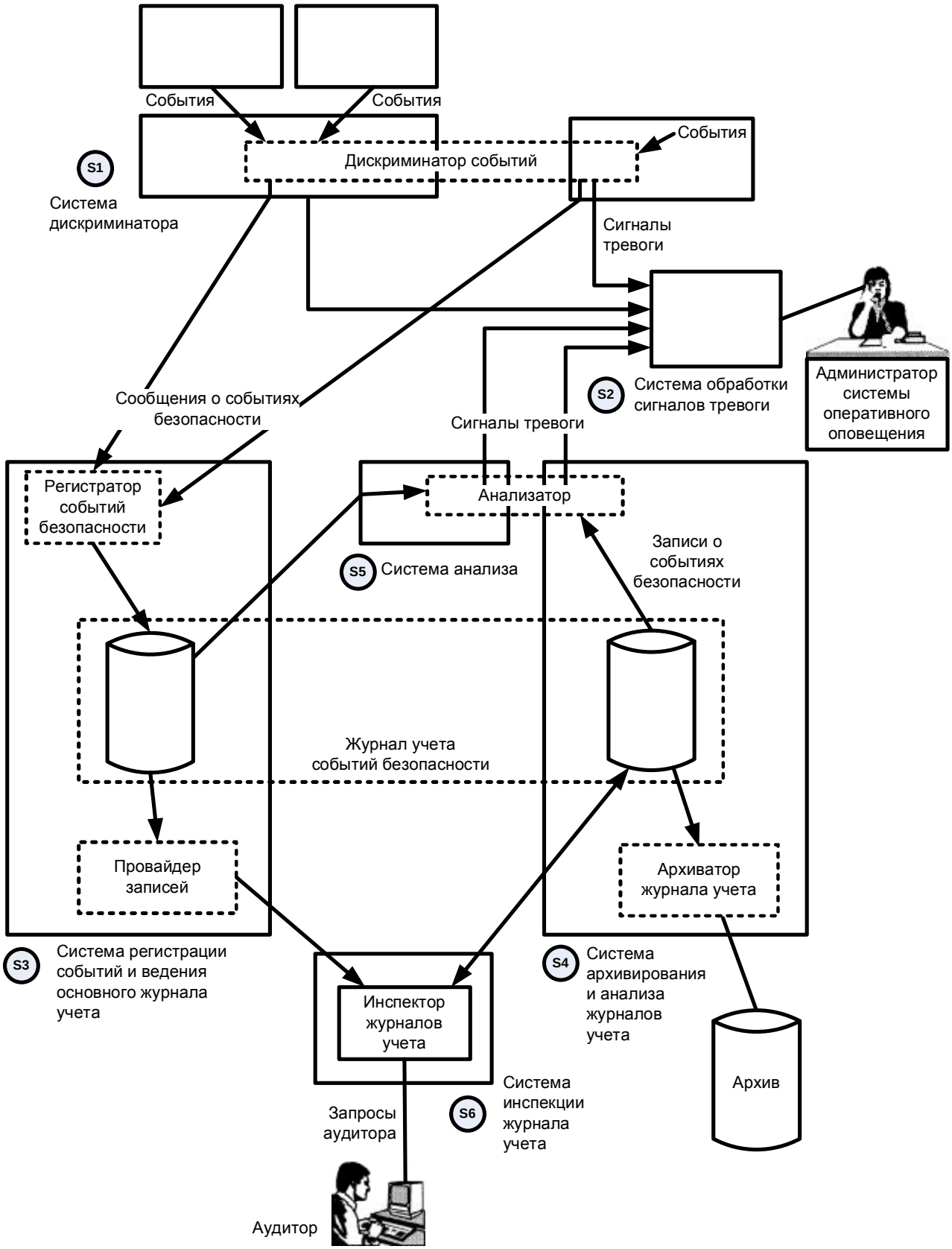


Рисунок Б.1. Пример реализации сервиса
учета событий безопасности и оперативного оповещения о них

Приложение В
(справочное)
Схема средств учета событий безопасности и оперативного оповещения о них

<table>
<tr><td colspan="3" rowspan="4">Схема средств защиты</td><td rowspan="4">Элемент</td><td>Объекты</td><td colspan="3">полномочное лицо контроля; администратор системы оперативного оповещения; аудитор защиты</td></tr>
<tr><td>Функции</td><td colspan="3">дискриминатор событий; регистратор событий безопасности; процессор обработки сигналов тревоги; анализатор журнала учета; инспектор журналов учета; провайдер записей; диспетчер журналов учета; сборщик журналов учета</td></tr>
<tr><td>Информационные объекты</td><td colspan="3">сообщения о событиях безопасности; записи о событиях безопасности; отчеты о событиях безопасности</td></tr>
<tr><td>Цель сервиса</td><td colspan="3">гарантия того, что информация, связанная с защитой открытых систем, зарегистрирована и при необходимости включена в отчет</td></tr>
<tr><td rowspan="6">Деятельность</td><td rowspan="2"></td><td>Объект</td><td colspan="4">Полномочное лицо контроля</td></tr>
<tr><td>Функция</td><td colspan="4">Определение и анализ связанных с защитой событий</td></tr>
<tr><td colspan="2">Деятельность, связанная с управлением</td><td colspan="4">Критерий 1: определение события
Критерий 2: инспекция журнала учета событий безопасности
Критерий 3: анализ журнала учета событий безопасности</td></tr>
<tr><td rowspan="2"></td><td>Объект</td><td>Администратор системы оперативного оповещения</td><td colspan="2">Аудитор защиты</td><td>Инициатор/цель субъект/объект</td></tr>
<tr><td>Функция</td><td>- дискриминатор событий;
- процессор обработки сигналов тревоги;
- анализатор журнала учета событий безопасности</td><td colspan="2">- событие;
- дискриминатор;
- анализатор журнала учета событий безопасности;
- регистратор событий безопасности;
- журнал учета;
- инспектор журналов учета;
- провайдер записей;
- архиватор журнала учета</td><td></td></tr>
<tr><td colspan="2">Деятельность, связанная с работой</td><td>- Формирование ИНФ
- Сбор ИНФ
(под ИНФ подразумевается информация оперативного оповещения)</td><td colspan="2">- Формирование ИНФ
- Сбор ИНФ
- Анализ ИНФ
(под ИНФ подразумевается сообщение о событии безопасности)</td><td></td></tr>
<tr><td rowspan="3">Информация</td><td rowspan="2">Элемент данных, управляемый полномочным лицом контроля</td><td>Критерий 1
- тип события
- время
- объект</td><td>Критерий 2
- тип записи
- тип события</td><td>Критерий 3
- тип события
- число событий
- период времени</td></tr>
<tr><td>- действие, которое будет предпринято
- информация о защите, которая будет сформирована</td><td>- списки записей</td><td>- действие, которое будет предпринято</td></tr>
<tr><td colspan="2">Тип информации, используемый в работе</td><td colspan="3">- тип сообщения/информации
- отличительный идентификатор элементов
- причина сообщения
- отличительный идентификатор дискриминатора событий, провайдер записей и/или регистратор событий безопасности</td></tr>
<tr><td></td><td colspan="2">Информация управления</td><td colspan="3">- время появления и число событий</td></tr>
</table>

Рисунок В.1. Схема средств
учета событий безопасности и оперативного оповещения о них

Приложение Г
(справочное)
Регистрация времени для событий безопасности

Совершенная синхронизация между различными источниками событий или регистраторами событий практически невозможна. В таком случае необходимы средства, позволяющие соотнести временные параметры в пределах журнала учета событий безопасности. Запись о событии безопасности создается из сообщения о событии безопасности, которое может содержать или не содержать временную метку. Если это сообщение содержит временную метку, то с использованием индикатора времени, содержащегося в сообщении о событии безопасности, формируется запись о событии безопасности. При этом запись о событии безопасности, созданная в результате приема события, подлежащего учету, содержит временную метку, сформированную с использованием опорного синхросигнала **регистратора событий безопасности**. В обоих случаях должна создаваться запись о времени взаимодействия между источником события и **регистратором событий безопасности**.

В первом случае должна быть выполнена оценка различия между началом отсчета времени источника события и опорным синхросигналом **регистратора событий безопасности**. Запись должна содержать идентификатор источника события, начало отсчета времени источника события, опорный синхросигнал **регистратора событий безопасности**, задержку по времени между указанными опорными временными точками и величиной допуска задержки. Во втором случае запись должна указывать идентификацию источника события, синхросигнал **регистратора событий безопасности** и оценку задержки между источником события и **регистратором событий безопасности**, а также допустимые пределы этой задержки.

Практически нет смысла создавать такие записи для каждого события. Записи могут создаваться в зависимости от характера соединения или девиации временных опорных точек. Если после периода наблюдений отмечается незначительная величина задержки, записи могут опускаться. При отсутствии измерений задержки может использоваться метод линейной интерполяции.

Такая же проблема возникает для опорных временных точек **регистратора событий и диспетчера журналов учета**, расположенного на другом конце системы. Однако в этом случае обе системы будут иметь синхронизацию по времени. Измерение временных различий между этими двумя корреспондентами может быть выполнено в любое время или же во время пересылки журнала учета событий безопасности. Запись о событии должна содержать идентификатор источника события, идентификатор **диспетчера журналов учета**, опорный синхросигнал **регистратора событий безопасности**, оценку временной задержки между **регистратором событий безопасности** и **диспетчером журналов учета** и поле допуска этой задержки.

Определение того, какое из двух событий произошло первым, может быть сделано посредством прибавления или вычитания задержки между сериями опорных синхросигналов и прибавления всех полей допуска. Если результирующая задержка будет меньше нижнего предела поля допуска, то различие может отсутствовать.

Тот же параметр применяется, если требуется создание отчета о событиях безопасности. При использовании информации, содержащейся в журнале учета, можно сортировать события согласно различным опорным временным точкам. Однако упорядочение событий можно гарантировать, только если поле допуска задержки не превосходит указанной временной разницы, прибавленной к полю допуска следующего события. С этой целью необходимо обеспечить возможность вычисления совокупного поля допуска для каждого события.

Приложение
(справочное)
Библиография

[1] ИСО/МЭК 10164-5:1993 Информационная технология. Взаимосвязь открытых систем. Управление системами. Часть 5. Функция управления регистрацией событий.

[2] ИСО/МЭК 10164-6:1993 Информационная технология. Взаимосвязь открытых систем. Управление системами. Часть 6. Функция управления системным журналом.

[3] ИСО/МЭК 10164-7:1992 Информационная технология. Взаимосвязь открытых систем. Управление системами. Часть 7. Функция передачи сигнала о нарушении режима безопасности.

[4] ИСО/МЭК 10164-8:1993 Информационная технология. Взаимосвязь открытых систем. Управление системами. Часть 8. Функция учета событий безопасности.

[5] Рекомендации МККТТ X.700 (1992) Основы управления для взаимодействия открытых систем для приложений МККТТ.

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

[7] ИСО/МЭК 7498-4:1989 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы управления.

УДК 681.324:006.354 **МКС 35.040**

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

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074