ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
Ақпарат қауіпсіздігінің бұзылуларын басқару

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Управление нарушениями безопасности информации

ҚР СТ ИСО/МЭК ТО 18044-2009

ISO/IEC TR 18044:2004 Information technology Security techniques.Information security incident management, IDT

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

Ақпарат қауіпсіздігінің бұзылуларын басқару

ҚР СТ ИСО/МЭК ТО 18044-2009

ISO/IEC TR 18044:2004 Information technology
Security techniques.Information security incident management, IDT

Ресми басылым

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

Астана

Алғысөз

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

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

3 Осы стандарт ISO/IEC TR 18044:2004 Information technology - Security techniques- Information security incident management (Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпарат қауіпсіздігі оқыс оқиғаларының менеджменті) халықаралық стандартымен бірдей.

Ағылшын тілінен (en) аударылған

Сәйкестік дәрежесі – сәйкес (IDT)

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ **2014 жыл**

ТЕКСЕРУ КЕЗЕҢДІЛІГІ **5 жыл**

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

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

Мазмұны

Кіріспе

Ақпараттық қауіпсіздіктің типтік саясаты немесе ақпараттық қауіпсіздіктің (АҚ) қорғау шаралары ақпаратты, ақпараттық жүйелерді, сервистерді немесе желілерді қорғауға толық кепілдік бере алмайды. Сондықтан қорғау шараларын енгізу толық қорғанышты қамтамасыз етпейді, кейіннен ақпараттық қауіпсіздіктің оқыс оқиғасы болуы мүмкін. Ақпараттық қауіпсіздіктің оқыс оқиғалары ұйымның қызметіне тікелей немесе жанама жағымсыз әсер етуі мүмкін. Одан басқа жаңа, бұрын сәйкестендірілмеген қауіп еріксіз пайда болуы мүмкін. Нақты ұйымның осындай оқыс оқиғаларға жеткіліксіз дайындығы оқыс оқиғаларға арналған практикалық әсерді аз тиімді етеді және бұл ұйымның қызметіне жағымсыз әсердің дәрежесін әлеуетті арттырады. Сол себепті, ақпараттық қауіпсіздікке оң көзбен қарайтын кез келген ұйым үшін мыналарға:

- ақпараттық қауіпсіздіктің оқыс оқиғалары туралы хабарлауға, анықтауға, оларды бағалауға;
- жағымсыз әсерлерден кейінгі салдарларды болдырмау, төмендету және (немесе) қалпына келтіру үшін тиісті қорғаныш шараларын белсендіруді қоса алғанда ақпараттық қауіпсіздіктің оқыс оқиғаларына жауап беруге (мысалы, жұмыс процесінің үздіксіздігін қолдау және жоспарлау аясында);
- ақпараттық қауіпсіздік оқыс оқиғаларынан алынған сабақтардың үзінділеріне, қорғаныш шараларының ескертулерін енгізуге және ақпараттық қауіпсіздіктің оқыс оқиғаларының менеджментіне жалпы тәсілді жақсартуға құрылымдық және жоспарлы әдіс қабылдау маңызды.

Осы стандарттың ережесі халықаралық деңгейде қалыптасқан практиканы есепке ала отырып, ұйымдағы ақпараттық қауіпсіздіктің оқыс оқиғаларының менеджменті туралы ұсыныстан тұрады.

Осы стандарт ақпараттық қауіпсіздікті қамтамасыз ету кезінде оқыс оқиғалардың менеджменті процесінде қызметтің барлық саласындағы ұйымдардың пайдалануына арналған. Оның ережесін басқа стандарттармен, оның ішінде ақпараттық қауіпсіздік менеджменті жүйесіне және ұйымның сапа менеджменті жүйесіне қойылатын талаптарды қамтитын стандарттармен бірге пайдалануға болады.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

Ақпарат қауіпсіздігінің бұзылуларын басқару

Information technology. Security techniques.Information security incident management

Енгізілген күні 2010-07-01

1 Қолданылу саласы

Осы стандарт ақпарат қауіпсіздігінің бұзылуларын басқару тәртібін белгілейді, ақпараттық технологияларды (бұдан әрі - АТ), ақпараттық жүйелерді, сервистерді және желілерді қолдану кезінде ақпараттық қауіпсіздікті (бұдан әрі - АҚ) қамтамасыз ету жөніндегі бөлімшелердің басшылары үшін ұйымдарда ақпараттық қауіпсіздіктің оқыс оқиғалары менеджменті жөніндегі ұсынымнан тұрады.

2 Нормативтік сілтемелер

Осы стандартты қолдану үшін мынадай сілтемелік нормативтік құжаттар қажет:

ҚР СТ ИСО/МЭК 13335-1-2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпаратты қорғау технологияларын басқару. 1-бөлім. Ақпаратты қорғау және коммуникациялық технологияларды басқаруға арналған жалпы ұғымдар мен модельдер.

ҚР СТ ИСО/МЭК 17799-2006 Ақпараттық технология. Қорғанышты қамтамасыз ету әдістері. Ақпаратты қорғауды басқару жөніндегі ережелер жиынтығы.

ЕСКЕРТПЕ «Осы стандартты пайдалану кезінде ағымдағы жылғы жай-күйі бойынша «Стандарттау жөніндегі нормативтік құжаттар» жыл сайын жарияланатын ақпараттық көрсеткіші және ағымдағы жылы жарияланған тиісті ай сайын жарияланып тұратын ақпараттық көрсеткіштер бойынша сілтемелік стандарттар мен жіктеуіштердің қолданылуын тексерген дұрыс. Егер сілтемелік құжат ауыстырылса (өзгертілсе), онда осы стандартты пайдалану кезінде ауыстырылған (өзгертілген) құжатты басшылыққа алу керек. Егер сілтемелік құжат ауыстырылмай жойылған болса, онда оған сілтеме берілген ереже осы сілтемені қозғамайтын бөлімде қолданылады».

3 Терминдер мен анықтамалар

Осы стандартта ҚР СТ ИСО/МЭК 13335-1, ҚР СТ ИСО/МЭК 17799 бойынша терминдер, сондай-ақ тиісті анықтамалары бар мынадай терминдер қолданылады:

3.1 **Қызметтік үздіксіздігін жоспарлау** (business continuity planning): Ұйым қызметінің үздіксіздігіне және оның элементтерін ұстап тұруға жағымсыз әсер етуге қабілетті қандай да бір күтпеген немесе қажет етілмеген оқыс оқиғалар пайда болған жағдайда операцияларды қалпына келтіруді қамтамасыз ететін процесс.

ЕСКЕРТПЕ: Осы процесс сондай-ақ берілген уақыттың кезеңділігін және аралығын және ұйымның барлық функциясын жұмыс жағдайына одан әрі қалпына келтіруді есепке ала отырып, қызметті қалпына келтіруді қамтамасыз етуге тиіс. Осы процестің түйінді элементтері қажетті жоспарлар мен құралдарды қолдануды және тесттеуді, оған ақпаратты, бизнес-процестерді, ақпараттық жүйелер мен сервистерді, сөз байланысын енгізуді және деректерді беруді, дербес және физикалық құрылғыларды қамтамасыз етуге тиіс.

3.2 **Ақпараттық қауіпсіздік оқиғасы** (information security event): АҚ саясатының бұзылушылығы немесе қорғау шараларының күші жойылуы немесе қауіпсіздікке қатысы болуы мүмкін бұрынғы белгісіз жағдайлардың пайда болуы мүмкіндігін көрсететін жүйелердің, сервистің немесе желінің белгіленген жағдайының сәйкестендірілген көрінісі.

3.3 **Ақпараттық қауіпсіздіктің оқыс оқиғалары** (information security incident): Операциялардың компрометациялау мен АҚ қауіп қатерінің жасалуының елеулі ықтималдығымен байланысты АҚ-нің бір немесе бірнеше ұнамсыз немесе күтпеген оқиғаларының пайда болуы.

ЕСКЕРТПЕ: АҚ-нің оқыс оқиғаларының мысалы 6-бөлімде келтірілген.

3.4 Ақпараттық қауіпсіздіктің оқыс оқиғаларына жауап беру тобы (АҚОЖТ) (Information Security Incident Response Team (ISIRT)): Ұйымның оқытылған және сенімділікті пайдаланатын мүшелерінің тобы.

3.5 **Ақпараттық қауіпсіздік (АҚ):** Ақпарат алу, көшірмелеу, тарату, бұрмалау, жою немесе бұғаттау бойынша заңсыз әрекеттерді қоса алғанда электронды ресурстарға, ақпараттық жүйелерге рұқсатсыз қолжетімділікті болдырмауға, сақтауға бағытталған құқықтық, ұйымдастыру және техникалық іс-шаралар кешені.

ЕСКЕРТПЕ: Осы топ АҚ оқыс оқиғаларын олардың өмірлік циклі уақытында өңдейді және кейде, мысалы, компьютерлік оқыс оқиғаларға жауап беретін көпшілікке танылған топтың немесе жылдам жауап беретін компьютерлік топтардың (КТЖЖБ) сыртқы сарапшылары толтыруы мүмкін.

3.6 **Ақпараттық технология (АТ):** Ақпаратты жинауды, құруды, сақтауды, жинақтауды, өңдеуді, іздеуді, қорытындылауды, көшірмелеуді, беруді және таратуды қамтамасыз ететін технологиялық кешенге біріктірілген әдістердің, өндірістік процестердің және бағдарламалық-техникалық құралдардың жиынтығы.

4 Жалпы ережелер

4.1 Мақсаттар

Ұйымның АҚ жалпы стратегиясы ретінде АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсіл пайдаланылуы қажет. Осындай тәсілдердің мақсаттары:

- АҚ* және оларды тиімді өңдеуге байланысты ұйымның оқыс оқиғаларын анықтау;
- АҚ сәйкестендірілген оқыс оқиғаларын бағалау және оларға неғұрлым мақсатқа лайықты және нәтижелі әдіспен жауап беру;
- оқыс оқиғаға жауап берудің бір бөлігі болып табылатын тиісті қорғау шараларының көмегімен, кейде ұйым қызметінің үздіксіздігін қамтамасыз ету жоспар(-лар)ының тиісті элементтерін қолданумен қатар ұйымға және оның қызметіне арналған АҚ-ның оқыс оқиғаларының әсерін азайту;
- АҚ-ін және олардың менеджментін алдағы уақытта оқыс оқиғаларға айналдыруды болдырмау жөнінде мүмкіндіктерді арттыру, АҚ қорғау шараларын енгізуді және пайдалануды жетілдіру, АҚ-нің оқыс оқиғалар менеджментінің жалпы жүйесін жетілдіру мақсатында олар жөнінде сабақтар алуды қамтамасыз ету болып табылады.

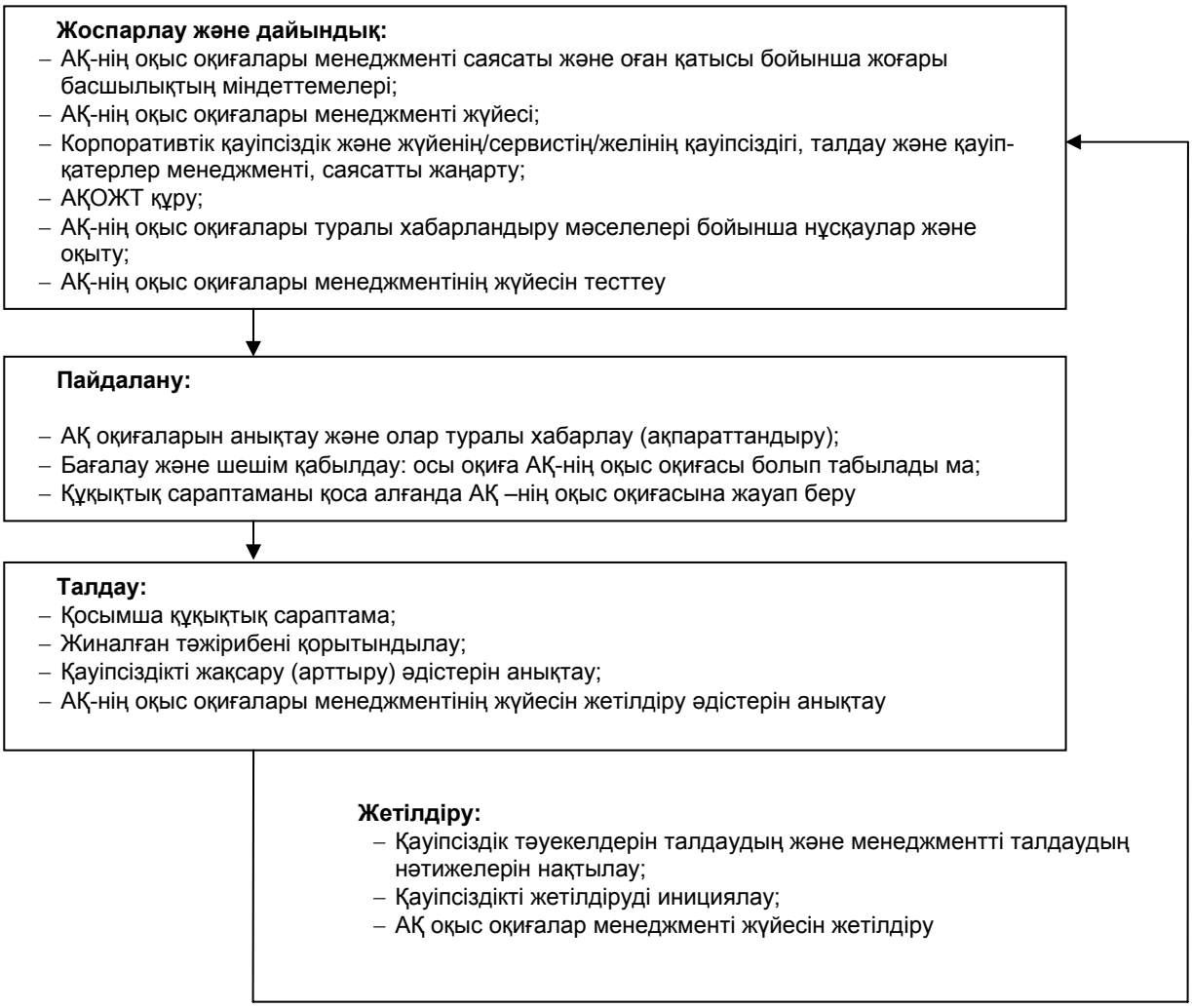
4.2 Кезеңдер

4.1-бөлімге сәйкес мақсаттарға қол жеткізу үшін АҚ-нің оқыс оқиғалар менеджменті төрт жеке кезеңге бөлінеді:

1) жоспарлау және дайындық;
2) пайдалану;
3) талдау;
4) жетілдіру.

ЕСКЕРТПЕ: АҚ-нің оқыс оқиғалар менеджменті кезеңдері [4] сериялы стандарттарда пайдаланылатын PDCA моделінің процестеріне ұқсас.

Осы кезеңдердің негізгі мазмұны 1-суретте көрсетілген.



1-сурет — АҚ оқыс оқиғалары менеджменті кезеңдері

4.2.1 Жоспарлау және дайындық

АҚ-нің оқыс оқиғаларының тиімді менеджмент тиісті жоспарлауды және дайындықты қажет етеді. АҚ-нің оқыс оқиғаларына тиімді реакцияны қамтамасыз ету үшін:

- АҚ-нің оқыс оқиғалары менеджментінің саясатын әзірлеу және құжаттау, сондай-

ақ осы саясатты мүдделі тараптардың және әсіресе жоғары басшылықтың қолдауын алу;

- АҚ-нің оқыс оқиғаларының менеджменті саясатын қолдау үшін АҚ-нің оқыс оқиғалары менеджментінің жүйесін әзірлеу және толық көлемде құжаттау қажет. АҚ-нің оқыс оқиғаларының нысандары, процедуралары және анықтауды, хабарлауды, бағалауды және жауап беруді қолдау құрал-саймандары, сондай-ақ оқыс оқиғалардың шын мәнінің шкалалары басқыштары нақты жүйеге арналған құжатта көрсетілуге тиіс (кейбір ұйымдарда мұндай жүйе «АҚ оқыс оқиғаларына жауап беру жоспары» деп аталуы мүмкін);

- АҚ менеджментінің саясатын және барлық, яғни корпоративтік деңгейлердегі қауіп-қатерлерді және АҚ-нің оқыс оқиғалары менеджментінің жүйелерін есепке ала отырып, әрбір жүйе, сервис және желі үшін жеке жаңарту;

- ұйымда АҚ-нің оқыс оқиғалары менеджментінің тиісті құрылымдық бөлімшесін, яғни АҚ-нің оқыс оқиғаларының барлық белгілі типтеріне барабар жауап беруге қабілетті қызметкерлердің берілген міндеттері мен жауапкершілігімен бірге АҚОЖТ-ыны құру қажет. АҚОЖТ ұйымының көпшілігі қызметтің нақты бағыттары жөніндегі мамандардан тұратын топ болып табылады, мысалы, зиянды тасымалдағы бағдарламаның қарсы әрекеті сипатталған кезде ұқсас типтегі оқыс оқиғалар жөніндегі мамандар шақыртылады;

- ұйымның барлық қызметкерлеріне нұсқаулар арқылы және (немесе) басқа да әдістермен АҚ-нің оқыс оқиғалары менеджментінің жүйесінің бар екендігімен, оның артықшылықтарымен және АҚ-нің оқиғалары туралы хабарламаның тиісті әдістерімен таныстыру қажет. АҚ-нің оқыс оқиғалары менеджментінің жүйесін басқаруға жауапты қызметкерлерді, оқиға оқыс оқиға болып саналатындығын анықтау жөнінде шешімді қабылдайтын тұлғаларды және оқыс оқиғаларды зерттейтін адамдарды тиісті оқыту қажет;

- АҚ-нің оқыс оқиғалары менеджментінің жүйесін мұқият тесттеу қажет. «Жоспарлау және дайындық» кезеңі – 7-бөлімге сәйкес.

4.2.2 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің жүйесін пайдалану

АҚ-нің оқыс оқиғалары менеджментінің жүйесін пайдалану кезінде мынадай процестерді жүзеге асыру қажет:

- АҚ-нің оқиғаларды анықтау және олардың туындауы туралы хабарлау (адам немесе автоматты құрал арқылы);

- АҚ-нің оқиғаларымен байланысты ақпаратты жинау және қандай оқиғаларды АҚ-нің оқыс оқиғаларының санатына жатқызуға болатындығын анықтау мақсатында осы ақпаратты бағалау;

- АҚ-нің оқыс оқиғаларына жауап беру;

- тез арада, уақыттың шынайы немесе шынайылыққа жақын масштабында;

- егер АҚ-нің оқыс оқиғалары бақылауда болса, шұғылдығы аздау әрекетті орындау (мысалы, апаттан кейін толық қалпына келтіруге мүмкіндік беретін);

- егер АҚ-нің оқыс оқиғалары бақылауда болса, онда «дағдарысқа қарсы» әрекетті орындау (мысалы, өрт командасын/бөлімшесін шақыру немесе ұйым қызметінің үздіксіздігі жоспарын орындауға бастамалық ету);

- АҚ-нің оқыс оқиғаларының болуы және оған қатысты кез келген егжей-тегжейлері туралы өз ұйымының қызметкерлеріне, сондай-ақ өзге ұйымның қызметкерлеріне хабарлау (бұл одан әрі бағалау және (немесе) шешім қабылдау мақсатында, кем дегенде, оқыс оқиғалардың егжей-тегжейін таратуды қамтиды);

- құқықтық сараптама;

- кейіннен талдау үшін барлық әрекеттер мен шешімдерге тиісті тіркеу;

- оқыс оқиғалар проблемаларын шешу.

«Пайдалану» кезеңі – 8-бөлімге сәйкес.

4.2.3 Талдау

АҚ-нің оқыс оқиғаларына рұқсат етілгеннен/жабылғаннан кейін АҚ жағдайын талдау бойынша мынадай әрекеттер жасалуы қажет:

- қосымша құқықтық сараптама жүргізу (қажет болғанда);
- АҚ-нің оқыс оқиғаларынан алынған сабақтармен танысу;
- АҚ-нің бір немесе бірнеше оқыс оқиғаларынан жинақталған сабақтардан алынған АҚ-нің қорғау шараларын енгізу үшін жақсартуды анықтау;
- жалпы кәсіпкерлік тәсілдің сапасын талдау нәтижелерінен жинақталған сабақтарды есепке ала отырып, АҚ-нің оқыс оқиғаларының менеджменті жүйесі үшін жақсартуды анықтау (мысалы, процестерінің, процедураларының, есеп беру және ұйым нысандарының нәтижелілігін талдаудан).

«Талдау» кезеңі – 9-бөлімге сәйкес.

4.2.4 Жетілдіру

АҚ-нің оқыс оқиғалары менеджментінің процестері АҚ-нің элементтерінің қатарына уақыт ішінде жетілдіруді тұрақты енгізу отырып итеративті болып табылады. Бұл жетілдірулер АҚ-нің оқыс оқиғалары және оларға жауап беру туралы деректердің, сондай-ақ тенденция динамикасы туралы деректердің негізінде ұсынылады. «Жақсарту» кезеңі мыналарды:

- АҚ-нің қауіп-қатерін талдаудың және ұйым менеджментін талдаудың нәтижелерін қайта қарауды;
- АҚ-нің оқыс оқиғалары менеджментінің жүйесін және оның құжаттамасын жетілдіруді;
- АҚ-нің жаңа және (немесе) жаңартылған қорғау шараларын енгізуді қоса алғанда, қауіпсіздік саласында жетілдіруді бастамалық етуді қамтиды.

«Жетілдіру» кезеңі - 10-бөлімге сәйкес.

5 Құрылымдық тәсілдің артықшылықтары және ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің түйінді мәселелері

Осы бөлімде мынадай:

- АҚ-нің оқыс оқиғалары менеджментінің сапалы жүйелерінен алынатын артықшылықтар туралы;
- жоғары корпоративтік басшылықтың және жүйеге есептер беретін әрі одан ақпарат алатын қызметкерлердің осындай артықшылықтарына сендіру мақсатында қарау қажет түйінді мәселелер туралы ақпарат ұсынылған.

5.1 Артықшылықтар

АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсілді пайдаланатын кез келген ұйым олардан мынадай топтарға біріктіруі мүмкін маңызды артықшылықтарды алуы мүмкін:

- АҚ жетілдіру;
- ұйым қызметіне жағымсыз әсерді төмендету, мысалы, ұйымның қызметін тоқтату және АҚ-нің оқыс оқиғаларының салдары ретінде қаржылық шығын;
- оқыс оқиғаларды болдырмау мәселелеріне көңіл аударуды күшейту;
- басымдылықтарды белгілеуге және айғақтарды жинауға көңіл аударуды күшейту;
- бюджетті және ресурстарды қалыптастыруға үлес қосу;
- менеджмент нәтижелерін және қауіп-қатерлер талдауларын неғұрлым жоғары

деңгейде жаңарту;

- АҚ-нің саласында хабарлануды және оқытуды арттыру бағдарламасы үшін материал ұсыну;
- АҚ-нің саясатын талдау үшін кіріс деректерін және тиісті құжаттамаларды ұсыну.

Осы артықшылықтардың әрқайсысы төменде қаралады.

5.1.1 Қауіпсіздікті жетілдіру

Анықтаудың, хабарлаудың, бағалаудың және АҚ-нің оқыс оқиғалары менеджментінің және оқиғасының құрылымдық процессі АҚ-нің кез келген оқиғасын немесе оқыс оқиғасын дереу сәйкестендіруге және дұрыс шешімді тез арада анықтау және жауап беру есебімен жалпы қауіпсіздікті жақсарта отырып, сондай-ақ алдағы уақытта АҚ-нің ұқсас оқыс оқиғаларын болдырмау құралын қамтамасыз ете отырып, жауап беруге мүмкіндік береді.

5.1.2 Ұйымның қызметіне жағымсыз әсерлерді төмендету

АҚ-нің оқыс оқиғаларының менеджментіне құрылымдық тәсіл ұйым қызметіне АҚ-нің оқыс оқиғаларымен байланысты жағымсыз әсердің деңгейін төмендетуге ықпал береді. Осындай әсерлердің зардаптарына тез арада болатын қаржылық шығындар, сондай-ақ ұйымның атағына және несие қабілеттілігіне келтірілген шығыннан туындайтын ұзақ мерзімді шығындар кіреді.

5.1.3 Оқыс оқиғалардың алдын алуға назар аударуды күшейту

АҚ-нің оқыс оқиғаларының менеджментіне құрылымдық тәсілді пайдалану ұйым ішінде оқыс оқиғалардың алдын алуға назар аударуды күшейтуге ықпал ете алады. Оқыс оқиғаларға байланысты деректерді талдау оқыс оқиғалардың алдын алуға назар аударуды күшейтуге және кейіннен оқыс оқиғалардың туындауын болдырмау бойынша тиісті әрекеттерді анықтауға мүмкіндік бере отырып, оқыс оқиғалардың пайда болуы моделін және тенденциясын анықтауға мүмкіндік береді.

5.1.4 Басымдылықтарды және куәландыруларды белгілеу жүйесіне көңіл аударуды күшейту

АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсіл АҚ-нің оқыс оқиғаларын зерттеу кезінде басымдылықтарды белгілеу жүйесі үшін мықты негізді құрайды.

Нақты процедуралар болмаған жағдайда зерттеу оқыс оқиғаларға жауап беру олардың пайда болу шамасы бойынша немесе тиісті басшының өкіміне реакция ретінде жүзеге асырылатын тұрақты емес режімде жүргізілетін қауіп-қатері болады. Бұл кейіннен басымдықтарды сол шын мәнінде қажет жерде тиісті идеалды белгілеуге зерттеу жүргізуге кедергі келтіреді.

Оқыс оқиғаларды зерттеудің нақты процедуралары деректердің дұрыстығын және оларға құқықтық қол жеткізуді және оларды өңдеуді қамтамасыз ете алады. Бұл сотпен қудалануға немесе тәртіптік талқылауға бастамалық жасалған жағдайда үлкен маңызы бар. Бірақ АҚ-нің оқыс оқиғадан кейін қалпына келтіру үшін қажетті әрекеттер жиналған куәландырудың тұтастығына қауіп төнуі мүмкін екендігін мойындау керек.

5.1.5 Бюджеттер мен ресурстар

АҚ-нің оқыс оқиғаларының менеджментіне жақсы ойластырылған құрылымдық тәсіл ұйым бөлімшелерінің ішінде бюджеттер мен ресурстарды бөлуді негіздеуге және жеңілдетуге ықпал етеді. Одан басқа АҚ-нің оқыс оқиғалары менеджментінің жүйесі де пайда табады. Мұндай пайдалар мынадай шарттармен байланысты:

- дабылдың жалған сигналдарын сәйкестендіру және електен өткізу үшін неғұрлым

біліктілігі аз қызметкерлерді пайдалану;

- білікті қызметкерлердің дағдыларын нағыз қажетті бағытта қолдану;

- білікті қызметкерлерді оның дағдысы қажет етілетін процесстер үшін ғана және оның араласуы қажет процестің сатысында ғана тарту.

Одан басқа, АҚ-нің оқыс оқиғаларының менеджментіне құрылымдық тәсіл ұйымдағы АҚ-нің оқыс оқиғаларын өңдеудің «санды» бағалауды орындау мүмкіндігі мақсатында «уақытты белгілеу» деген тоқтату процедурасын қамтиды. Бұл, мысалы, әр түрлі басымдықтағы оқыс оқиғаларды әр түрлі платформаларда рұқсат ету уақыты туралы ақпаратты ұсынуды мүмкін етеді. АҚ-нің оқыс оқиғалары менеджментінің процесінде әлсіз орын болған кезде бұл әлсіз орындар да сәйкестендірілген болуға тиіс.

5.1.6 АҚ-нің менеджменті және қауіп-қатерін талдау

АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсілді пайдалану мыналарға мүмкіндік береді:

- қауіп-қатердің әр түрлі типтерінің және олармен байланысты осалдықтардың сипатын сәйкестендіру және анықтау үшін неғұрлым сапалы деректерді жинау;

- қауіптердің сәйкестендірілген типтерінің пайда болу жиілігі туралы деректерді ұсыну.

Ұйымның қызметіне арналған АҚ-нің оқыс оқиғаларының жағымсыз салдары туралы алынған деректер осы салдарларды талдау үшін пайдалы болады. Қауіптердің әр түрлі типтерінің пайда болу жиілігі туралы деректер қауіп бағасының сапасын анағұрлым арттырады. Тиісінше, осалдық туралы деректер осалдықтың келешектегі бағасы сапасын анағұрлым арттырады.

Жоғарыда аталған деректер АҚ-нің менеджментін талдаудың және қауіп-қатер талдауының нәтижелерін айтарлықтай жақсартады.

5.1.7 АҚ-ның мәселелерінде хабарлану

АҚ-ның оқыс оқиғаларының менеджментіне құрылымдық тәсілі АҚ-нің мәселелерінде хабарлануды қамтамасыз ету бағдарламалары туралы заңға бағытталған ақпаратты ұсынады. Бұл ақпарат басқа жерде емес, нақты осы ұйымда шын мәнінде болып жатқан АҚ-нің оқыс оқиғаларын көрсететін шынайы мысалдардың көзі болып табылады. Сондықтан шешімдер туралы ақпаратты тез арада алудың пайдасын көрсетуге болады. Одан басқа АҚ-нің мәселелерінде осыған ұқсас хабарлама АҚ-нің оқыс оқиғасының пайда болуы жағдайында адамдардың үрейін және (немесе) абыржуын тудыратын қателіктердің болуын төмендетуге мүмкіндік береді.

5.1.8 АҚ-нің **саясатын талдауға арналған кіріс деректер**

АҚ-нің оқыс оқиғалары менеджментінің жүйесін беретін ақпарат АҚ-нің (және АҚ-мен байланысты басқа құжаттың) саясатының нәтижелігін талдау және одан әрі жетілдіру үшін бағалы кіріс деректерді қамтамасыз етеді. Бұл ұйым деңгейінде де және жеке жүйелер, сервистер және желілер үшін де саясаткерлерге және басқа да құжаттамаға қатысты.

5.2 Түйінді мәселелер

АҚ-нің оқыс оқиғаларының менеджменті қалай жүзеге асырылатыны туралы ақпарат келіп түсетін кері байланыстың болуы ұйымның жүйелері, сервистері және желілері үшін шынайы қауіп-қатермен күресуге қызметкерлердің іс-әрекетінің жұмылуын сақтауға көмектеседі. Бұл маңызды кері байланыс АҚ-нің оқыс оқиғалары тұрақты болмағандықтан, АҚ-нің оқыс оқиғаларына жауап беру процесі арқылы тиімді іске асырылуы мүмкін емес. Кері байланыс ұйымның барлық бөлімшелері үшін жалпы

құрылымды қабылдайтын АҚ-нің оқыс оқиғалары менеджментінің құрылымды, жақсы ойластырылған жүйесі болған жағдайда айтарлықтай нәтижелі болуы мүмкін. Осы жалпы құрылым неғұрлым толық нәтижелерінің жүйеден алуды үздіксіз қамтамасыз етуі және АҚ-нің оқыс оқиғасы пайда болғанға дейін оның туындауының мүмкін шарттарын жылдам анықтау үшін сенімді негіз болуға, сондай-ақ хабарлаудың тиісті сигналын беруге тиіс.

АҚ-нің менеджменті және менеджменті жүйесінің аудиті қызметкерлермен бірлескен жұмысты кеңейту үшін қажетті сенімнің негізін және пайдалы нәтижелердің құпиялығын, қауіпсіздігін және қолжетімділігін сақтауға қатысты сенімсіздікті төмендетуді қамтамасыз етеді. Мысалы, ұйымның басшысы мен қызметкерлері хабарлау сигналы күтілетін оқыс оқиғаға қатысты қазіргі заманғы, нақты және толық ақпарат беруіне сенімді болуға тиіс.

АҚ-нің оқыс оқиғалары менеджменті жүйесін енгізу кезінде ұйымдар дербес деректердің қолжетімсіздігі проблемаларына байланысты мәселелер бойынша оң нәтижелер және алаңдаушылық болмауы тәрізді әлеуетті проблемаларды болдырмау керек. Мүдделі тараптарды жоғарыда аталған проблемалардың туындауын болдырмау үшін белгілі бір қадамдар қабылданғанына сендіру қажет.

Сондықтан АҚ-нің оқыс оқиғалары менеджментінің оңтайлы жүйесін құру үшін мыналарды:

- басшылықтың міндетін;
- хабарлауды;
- құқықтық және нормативтік аспектілерді;
- пайдалану тиімділігін және сапасын;
- жасырын;
- құпиялығын;
- АҚОЖТ қызметінің тәуелсіздігін;
- типологияны қоса алғанда түйінді мәселелердің бір қатарын қарау қажет.

Осы мәселелердің әрқайсысы төменде қаралады.

5.2.1 Басшылықтың міндеттері

АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсілді қабылдау үшін басшылық тарапынан тұрақты қолдау қажет. Ұйымның қызметкерлері АҚ-нің оқыс ақпараттарын тануға және олар пайда болған кезде өз іс-әрекеттерін білуге, сондай-ақ ұйым үшін құрылымдық тәсілдің үлкен артықшылығын білуге тиіс. Бірақ басшы тарапынан қолдау болмаған жағдайда, бұл жеткіліксіз болуы мүмкін. Ұйым оқыс оқиғаларға жауап берудің қабілеттілігін қолдауды және ресурстарды қамтамасыз ету бойынша міндеттерді орындауға тиіс.

5.2.2 Хабарлану

АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсілді қабылдаудың басқа елеулі проблемасы хабарлану болып табылады. Ұйым жұмысына қатысу үшін тұтынушылардағы қажеттілікке қарамастан ақпараттық қауіпсіздіктің оқыс оқиғаларын басқаруға құрылымдық тәсілге қатысқаннан олар және оның бөлімшелері қандай пайда алатыны туралы хабарлану болмаған жағдайда ұйым жұмысына олардың тиімді қатысуын есептеу мүмкін емес.

АҚ-нің оқыс оқиғалары менеджментінің кез келген жүйесі мыналарды:

- ұйым үшін де, оның қызметкерлері үшін де АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсілдің артықшылығын;
- АҚ-нің оқиғалардың және (немесе) оқыс оқиғаларының деректер базасында сақталатын оқыс оқиғалар туралы ақпаратты және одан шыққан шығыс деректерді;

- ұйымның типіне байланысты жеке бағдарлама немесе АҚ-нің мәселелерінде хабарланудың неғұрлым кең бағдарламасының бір бөлігі болуы мүмкін хабарланудың бағдарламалық қамтамасыз етілуіне арналаған стратегияны және механизмді қамтитын хабарлануды бағдарламалық қамтамасыз етуді анықтау арқылы құжатпен қоса жүруге тиіс.

5.2.3 Құқықтық және нормативтік аспектілер

АҚ-нің оқыс оқиғалары менеджментінің саясатында тиісті жүйеде АҚ-нің оқыс оқиғалары менеджментінің мынадай құқықтық және нормативтік аспектілерін есепке алу қажет:

1) дербес деректерді барабар қорғауды және дербес ақпараттың бейтараптылығын қамтамасыз ету.

Деректердің құпиялығын және тұтастығын сақтайтын арнайы заңнамасы бар елдерде ол әдетте дербес деректерді бақылаумен шектелген. Әдетте АҚ-нің оқыс оқиғалары қызметкерлердің немесе бөгде адамның қызметі нәтижесінде туындайтындықтан, жеке сипаттауға тиісінше тіркеу және оны басқару қажеті етілуі мүмкін. Ендеше, АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсіл кезінде дербес деректерге тиісінше қорғау қажеттілігі, сондай-ақ мынадай шарттар есепке алынуы қажет:

- дербес деректерге қолжетімділігі бар адамдар танысып отырған ақпаратта көрсетілген адамдармен жеке таныс болмауға тиіс;
- дербес деректерге қолжетімділігі бар адамдар оған қолжетімді болғанға дейін оларды таратпау туралы келісімге қол қоюға тиіс;
- дербес деректер тек АҚ-нің оқыс оқиғаларын зерттеуге алынған мақсатта пайдаланылуға тиіс;

2) Жазбаларды тиісінше сақтау.

Басқа елдердің кейбір заңдары компаниядан ұйымның жыл сайынғы аудиті процесінде талдау үшін өз қызметінің тиісті жазбасын жүргізуді талап етеді. Осындай талаптар әр түрлі ұйымдарда бар. Кейбір елдерде ұйымнан әр түрлі органдар үшін есеп беруді және мұрағат жасауды талап етеді (мысалы, қауіпті қылмыс болған немесе құпия ақпарат бар үкіметтік жүйеге кірген жағдайда);

3) коммерциялық келісім-шарттық міндеттерді орындауды қамтамасыз етуге арналған қорғау шаралары болғанда.

АҚ-нің оқыс оқиғалары менеджменті бойынша қызметті ұсыну жөніндегі міндеттелетін талаптар болған жағдайда (мысалы, жауап беру уақытына талаптар) ұйым кез келген жағдайларда (осыған байланысты ұйым тарапынан шарт ұйымының қорытындысы кезінде (7.5.4 бөлімін қараңыз), мысалы, АҚОЖТ, ұйым тарапынан шартқа уақытша жауап берумен қатар барлық қажетті талаптарды енгізу қажет) осы міндеттерді орындауды қамтамасыз ету мақсатында тиісті АҚ қамтамасыз етуді қарастыруға тиіс;

4) саясаттаррмен және рәсімдермен байланысты құқықтық мәселелер.

АҚ-нің оқыс оқиғалар менеджментінің жүйесімен байланысты саясаттарды және процедураларды құқықтық және нормативтік проблемалардың болуына тексеру қажет, мысалы, кейбір елдерде қызметкерлерді жұмыстан босату айтарлықтай қиын процесс болып табылатындықтан, оқыс оқиғаларды жасаудағы кінәлі қызметкерлерді тәртіптік жазаға тарту және (немесе) сотқа жауапқа тарту туралы хабарлау болуына;

5) жауапкершілікті мойындамаудың заңдылығын тексеру

АҚ-нің оқыс оқиғалары менеджментінің тобы немесе сыртқы көмекші қызметкерлер қабылдаған іс-әрекетке жауапкершілікті шектеу туралы барлық өтініштердің заңдылығы тексерілуге тиіс;

6) Тараптық қызметкерлермен жасалған келісім-шарттарға барлық қажетті аспектілерді енгізу.

Тараптық көмекші қызметкерлермен жасалған шарттар мысалы, КГБР ақпаратты таратпау, қызметтің қолжетімділігі және дұрыс емес кеңестің салдарлары бойынша міндеттердің бұзылуына жауапкершілікті келісім-шартқа енгізілгеніне мұқият тексерілуге тиіс;

7) құпия ақпаратты таратпау туралы келісімдер.

АҚ-нің оқыс оқиғалары менеджментінің топтары мүшелерінен жұмысқа түсер және жұмыстан босатылар кезінде де құпия ақпаратты таратпауы туралы келісімге қол қоюлары талап етіледі. Кейбір елдерде мұндай келісімдердің заңды күші жоқ. Осындай аспект тексерілуге тиіс;

8) Құқық қолданатын органдардың талаптарын орындау.

Құқық қолдану органдары заң негізінде АҚ-нің оқыс оқиғалары менеджментінің жүйесінен ақпарат талап етуі мүмкін мүмкіндіктерімен байланысты мәселелердің анықтығын қамтамасыз етуі қажет. Кейбір жағдайларда оқыс оқиғалар құжатталуы қажет заңда анықталатын барынша аз деңгей туралы және осы құжаттың сақталу мерзімі туралы анықтылығы талап етілуі мүмкін;

9) Жауапкершілік мәселелеріндегі айқындық

Әлеуетті жауапкершілік және қажетті тиісті қорғау шаралары мәселелерін нақтылау қажет. Жауапкершілік жүктеуге қатысы бар оқиғалардың мысалы төменде келтірілген:

- егер АҚ-нің оқыс оқиғалары уақтылы хабарландырмайтын және нәтижесінде шығын әкелетін басқа ұйымның қызметіне әсер ететін болса (мысалы, бірге пайдаланатын ақпаратты ашу);
- егер өнімнен жаңа осалдық анықталса, ол туралы өнім берушіге хабарламай, нәтижесінде бір немесе бірнеше ұйым айтарлықтай зардап шегіп, осы осалдықпен шын мәнінде байланысты оқыс оқиға туындағанда;
- егер қандай да бір елде ұйымдардан ауыр қылмыспен байланысы немесе қолжетімділік шектелген немесе маңызды ұлттық инфрақұрылымның сындарлы элементтерінің ақпаратынан тұратын үкіметтік жүйеге кірумен байланысы болуы мүмкін барлық жағдайларға қатысты құқық қорғау органдарына арналған мұрағаттарды құру немесе ақпараттандыруды талап ететін тиісті талаптар орындалмағанда;
- егер ақпарат ашылған болса және ұйымның ақпараттық ресурсына рұқсатсыз кіргенде, кейбір адамдардың немесе ұйымдардың қатысы болуы көрсетілгенде. Бұл дәлел нақты адамдардың немесе ұйымдардың абыройына және қызметіне зиян келтіруі мүмкін;
- егер ақпарат ашылған болса, бағдарламалық қамтамасыз етудің белгілі бір элементінде жұмыс жүрмей, бірақ нәтижесінде ақпарат жалған болғанда.

10) Арнайы нормативтік талаптар

АҚ-нің оқыс оқиғалары туралы, егер ол арнайы және нормативтік талаптармен көзделген болса, тиісті бақылау органына хабарлау керек, мысалы, атом өнеркәсібінде көзделгендей.

11) Сотпен қудалау немесе ішкі тәртіптік талқылаулар

Осы шабуылдар техникалық немесе жеке болуына қарамастан, қаскүнемдерге қатысты сот қудалауы немесе тәртіптік талқылау жүргізу сәтті болуы үшін өзгерістер енгізуден расталған түрде қорғалған аудит журналдарын қоса алғанда, АҚ-н тиісті қорғау шаралары қабылдануы қажет. Осы шабуылдар техникалық немесе жеке болуына қарамастан, қаскүнемдерге қатысты сот қудалауы немесе тәртіптік талқылау жүргізу сәтті болуы үшін сот немесе басқа да әкімшілік органдар үшін куәліктер жинау қажет. Мыналарды көрсету қажет:

- құжаттама бұрмаланбағанын және толық болып табылатынын;
- электрондық куәліктің көшірмелері түпнұсқамен бірдей екендігі расталатынын;
- куәліктер алынған АҚ-нің барлық жүйелері тіркеу кезінде штаттық режимде жұмыс істегенін.

12) Мониторинг әдістерімен байланысты құқықтық аспектілер:

Мониторинг әдістерін пайдалану салдары ұлттық заңнама контекстерінде көзделеді.

Әр түрлі әдістердің заңдылығы елдерге байланысты ауысуы мүмкін. Мысалы, кейбір елдерде мониторингтің, оның ішінде бақылау әдісімен жүргізілуі туралы адамдарға хабарлау қажет. Мониторингке кім (не) жататынын, қандай әдіспен олар (ол) мониторингке жататынын және қашан мониторинг жүргізетінін анықтайтын бірнеше факторларды ескеру қажет. Сондай-ақ мониторинг/бақылау рұқсатсыз басып кіруді анықтау жүйесінің (РБКАЖ) контекстінде арнайы қаралатынын белгілеу қажет [3].

13) Ақпараттық ресурстарды пайдалану және олармен танысу ережесін дайындау.

Ұйымда ақпараттық жүйелерді және ресурстарды пайдалану тәртібі анықталуы, құжатталуы және барлық болжанған қызметкерлердің мәліметіне жеткізілуге тиіс. (мысалы, қызметкерлер пайдаланудың рұқсат етілген саясаты туралы хабарлауы және ұйымға жұмысқа түсу немесе ақпараттық жүйелерге қолжетімділікті алу кезінде олардың осы саясатты түсінуін және қабылдауын жазбаша растауды талап етуі қажет).

5.2.4 Пайдалану тиімділігі және сапасы

АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсілді пайдалану тиімділігі және сапасы оқыс оқиғалар туралы хабарлау, хабарлау сапасын, пайдалану қарапайымдылығын, дереу әрекет ету және оқыту міндетін алатын факторлардың бір қатарына байланысты. Осы факторлардың бірнешеуі АҚ-нің оқыс оқиғалары менеджментінің маңыздылығы және олардың оқыс оқиғалар туралы хабарлаудың дәлелдігі туралы тұтынушылардың хабарлануын қамтамасыз етумен байланысты. Сол мезетте АҚ-нің оқыс оқиғалары туралы хабарламаға пайдаланылатын дереу әрекетті алсақ уақыт - бұл дара фактор емес, деректерді өңдеу және өңделген ақпаратты тарату үшін қажетті уақытты да есепке алу маңызды (әсіресе апаттық сигналдар жағдайында)

Кешігуді азайту үшін хабарлануды қамтамасыз етудің және тұтынушыларды оқытудың тиісті бағдарламалары АҚ-ның оқыс оқиғалары менеджментін жүзеге асыратын қызметкерлер қамтамасыз ететін «тікелей желі» бойынша қолдаумен толықтырылуға тиіс.

5.2.5 Құпиялық

Құпиялықты қамтамасыз ету мәселесі АҚ-нің оқыс оқиғалары менеджментінің жетістігі үшін негіз болып табылады. Тұтынушылар олардың хабарлайтын АҚ-нің оқыс оқиғалары туралы ақпарат толық қорғалғанына, ал қажет болғанда оны олардың ұйымымен немесе оның бөлімшесімен олардың келісімінсіз байланыстыру мүмкін болмайтындай иесіздендірілгеніне сенімді болуға тиіс.

АҚ-нің оқыс оқиғалары менеджментінің жүйесі ерекше жағдайлар кезінде АҚ-нің әлеуетті оқыс оқиғалары туралы хабарлайтын адамның немесе ұйымның құпиялығын қамтамасыз ету маңызды жағдайларды есепке алуға тиіс. Әрбір ұйымда АҚ-нің әлеуетті оқыс оқиғасы туралы хабарлайтын адам және ұйым үшін құпиялықты немесе оның жоқ болуын сақтаудың маңыздылығы нақты түсіндірілген жағдай болуға тиіс. АҚОЖТ-ы оқыс оқиға туралы басында хабарлайтын адам немесе ұйым хабарланбаған қосымша ақпарат қажет етіледі. Одан басқа АҚ-нің оқыс оқиғасы туралы маңызды ақпарат оны алғаш анықтаған адамнан алынуы мүмкін.

5.2.6 Құпиялылық

АҚ-нің оқыс оқиғалары менеджментінің жүйесінде құпия ақпарат болуы мүмкін және оқыс оқиғалармен айналысатын адамдардан оған қолжетімділік талап етілуі мүмкін.

Сондықтан өңдеу кезінде осы ақпараттың құпиялығы қамтамасыз етілуге немесе қызметкерлер оған қолжетімділікке рұқсат алу кезінде құпиялық (ақпаратты таратпау) туралы келісімге қол қоюға тиіс. Егер АҚ-нің оқиғалары проблемалар менеджментінің

жалпы жүйесі арқылы тіркелетін болса, онда құпиялы деректерді түсіруге, мүмкін, тура келеді.

Одан басқа АҚ-нің оқыс оқиғалары менеджментінің жүйесі БАҚ-ын, бизнес бойынша серіктестерді, ұйымдастыруды және қоғамдықты реттейтін тұтынушыларды қоса алғанда, ұйымдардан тыс оқыс оқиғалары туралы хабарламаларды беруді бақылауды қамтамасыз етуге тиіс.

5.2.7 Ақпараттық қауіпсіздіктің оқыс оқиғаларына жауап беру тобы қызметінің тәуелсіздігі

АҚ-нің оқыс оқиғалары менеджментінің тобы нақты ұйымның функционалдық, қаржылық, құқықтық және саяси қажеттіліктерін тиімді қанағаттандыруға қабілетті болуға және АҚ-нің оқыс оқиғаларын басқару кезінде абай болуға тиіс. АҚ-нің оқыс оқиғалары менеджменті тобының қызметі оның функциясының тиімділігін тексеру мақсатында тәуелсіз аудитке жатады. Бақылаудың тәуелсіздігін іске асырудың тиімді әдісі оқыс оқиғаларға жауап беруді басқару бойынша жоғары басшыға тікелей міндет жүктеуден және жалпы жедел басқарудан АҚ-нің оқыс оқиғасына жауап беру туралы хабарлама тізбегінің бөлімшесі болып табылады. Топты қаржыландыру жұмысы сырттан оған шамадан тыс әсер етуді болдырмау үшін ол да бөлек болуға тиіс.

5.2.8 Типология

АҚ-нің оқыс оқиғалары менеджментіне құрылымдық тәсілді сипаттайтын жалпы типология кейінгі сенімді нәтижелерді қамтамасыз етудің түйінді факторларының бірі болып табылады. Типология* деректер базасының жалпыға бірдей қабылданған метрикалармен және стандарттық құрылымымен қатар нәтижелерді салыстыру, ескерту ақпаратты жақсарту және ақпараттық жүйелер және олардың осалдықтары үшін қауіп туралы нақты түсінік алу мүмкіндігін қамтамасыз етеді.

6 Ақпараттық қауіпсіздіктің оқыс оқиғаларының және олардың себептерінің мысалы

АҚ-нің оқыс оқиғасы алдын ала болжанған немесе кездейсоқ болуы (мысалы, адамның қандай да қателігінің немесе табиғи көріністің салдары болып табылады) және техникалық та, техникалық емес те құралдардан болуы мүмкін. Олардың салдары ақпаратты санкцияланбай ашу немесе өзгерту, оған қолжетімсіз етіп, оны жою, сондай-ақ ұйымның активтеріне зиян келтіру немесе оларды ұрлау тәрізді осындай оқиғалар немесе басқа да оқиғалар. Хабарланбаған, бірақ оқыс оқиға ретінде анықталған ақпарат туралы АҚ-нің оқыс оқиғаларын тексеру мүмкін емес және осындай оқыс оқиғалардың қайта пайда болуын болдырмауға арналған қорғау шараларын қолдануға болмайды.

Тек түсіндіру мақсатында АҚ-нің оқыс оқиғалары және олардың себептерінің бірнеше мысалы төменде келтірілген. Осы мысалдар жоққа шығару болып табылмайтынын айта кету маңызды.

6.1 Қызмет көрсетуден бас тарту

Қызмет көрсетудегі бас тарту бір жалпы сипатқа ие АҚ-нің оқыс ақпараттарының кеңейтілген санаты болып табылады. АҚ-нің ұқсас оқыс оқиғалары жүйелердің, сервистердің немесе желілердің көбінесе авторланған тұтынушылардың қолжетімділігінде толық кері қайтару кезінде бұрынғыша өндірумен функциялауды жалғастыруға қабілетсіз болуға соқтырады.

Қызмет көрсетуден бас тартуға байланысты, техникалық құралдардан болатын АҚ-нің оқыс оқиғаларының екі негізгі типі бар: ресурстарды жою және ресурстарды азайту.

«Қызмет көрсетуден бас тарту» АҚ-нің алдын ала болжанған техникалық оқыс оқиғаларының кейбір типтік мысалдары:

- жауап хабарламаларды тарифпен өткізу желісінің жолақтарын толық толтыру мақсатында желілік кеңінен таратылған мекенжайларды аңдау;
- көзделмеген пішіндегі деректерді жүйеге, сервиске немесе желіге олардың қалыпты жұмысын бүлдіру немесе бұзу ниетінде беру;
- олардың ресурстарын жоққа шығару ниетінде нақты жүйесі, сервисі немесе желісі бар бірнеше сеанстарды бір мезетте ашу (яғни олардың жұмысын бәсеңдету, бұғаттау немесе бұзу) болып табылады.

«Қызмет көрсетуден бас тарту» АҚ-нің бірыңғай техникалық оқыс оқиғалары кездейсоқ, мысалы, оператор жасаған немесе қолданбалы бағдарламалық қамтамасыз етудің бірге болу мүмкіндігінің болмауынан, ал басқалары алдын ала болжанғаннан болған конфигурациядағы қателіктердің нәтижесінде туындауы мүмкін. «Қызмет көрсетуден бас тарту» АҚ-нің бірыңғай техникалық оқыс оқиғалары басқалар – тек басқа зиянды қызметтің жанама өнімі ғана болғанда жүйені, сервисті бұзу және өндірістік желіні төмендету мақсатындағы ниетпен инициялanады. Мысалы, жасырын сканирлеудің және сәйкестендірудің кейбір неғұрлым көп таралған әдістері ескі немесе қате конфигурацияланған жүйелердің немесе сервистердің оларды сканирлеу кезінде толық бұзылуына әкеп соқтыруы мүмкін. «Қызмет көрсетудегі кері қайтару» типінің көптеген алдын ала болжанған техникалық оқыс оқиғалар әдетте қаскүнем рұқсатсыз кіру желісі немесе жүйе туралы ақпарат ала алмағандықтан құпия түрде (яғни рұқсатсыз кіру көзі белгісіз) инициялanады.

Техникалық емес құралдардан болатын және ақпараттың, сервистің және (немесе) ақпаратты өңдеу құрылғыларының жойылуына әкеп соқтыратын «Қызмет көрсетуден бас тарту» АҚ-нің оқыс оқиғаларының мысалы мынадай факторлардан болуы мүмкін:

- ұрлануға, алдын ала болжанған шығынға немесе жабдықтың бұзылуына әкеп соқтыратын физикалық қорғау жүйесінің бұзылуы;
- аппаратураның тұрған орнына оттан немесе судан/селден кездейсоқ шығын болуы;
- қоршаған ортаның төтенше жағдайлары, мысалы, жоғары температура (ауа баптау жүйесінің істен шығуы салдарынан);
- жүйенің дұрыс жұмыс істемеуі немесе шамадан тыс жүктелуі;
- жүйедегі бақыланбайтын өзгерістер;
- бағдарламалық немесе аппараттық қамтамасыз етудің дұрыс жұмыс істемеуі.

6.2 Ақпарат жинау

«Ақпарат жинау» АҚ-нің оқыс оқиғалары рұқсатсыз кірудің әлеуетті мақсаттарын анықтаумен және рұқсат етудің сәйкестендірілмеген мақсаттарында жұмыс істейтін сервистер туралы түсініктерді алумен байланысты іс-әрекеттермен түсіндіріледі. АҚ-нің осыған ұқсас оқыс оқиғалары мыналарды анықтау мақсатында барлау жүргізуді білдіреді:

- оны қоршаған желілік топология туралы ұғымды алу мақсатының болуын және осы мақсат ақпарат алмасу әдетте кіммен байланыстылығы туралы;
- мақсаттардың әлеуетті осалдықтарын немесе рұқсатсыз кірулер үшін пайдаланылуы мүмкін оны тікелей қоршайтын желілік ортасын.

Ақпаратты техникалық құралдармен жинауға бағытталған рұқсатсыз кірулердің типтік мысалдары:

- Интернеттің (DNS аймағын беру) мақсатты домені үшін DNS (домендік атаулар жүйесі) жазбаларын шығару;
- жұмыс істеп тұрған жүйелерді табу мақсатында кездейсоқ желілік мекенжайлар бойынша тест сұрақтарын жіберу;
- хосттың операциялық жүйесін сәйкестендіру (мысалы, файлдардың бақылау

сомасы бойынша) мақсатында жүйені аңдау;

- тиісті сервистерді сәйкестендіру (мысалы, электронды пошта, FTP хаттамасы, желі) және осы сервистерді бағдарламалық қамтамасыз етудің нұсқаларын сәйкестендіру мақсатында жүйеге файлдарды беру хаттамасына арналған қолжетімді желілік порталдарды сканирлеу;

- желілік мекенжай ауқымы бойынша белгілі осалдықтары бар бір немесе бірнеше сервистерді сканирлеу (көлденең сканирлеу) болып табылады.

Кейбір жағдайларда ақпаратты техникалық жинау кеңейтіледі және санкцияланбаған рұқсатқа ауысады, егер, мысалы, қаскүнем осалдықты іздеу кезінде санкцияланбаған рұқсатты алуға ұмтылады. Әдетте, бұл тек осалдықты іздеп ғана қоймай, осал сервисті және (немесе) желін автоматты түрде пайдаланатын автоматтандырылған құралдармен кіруді жүзеге асырады.

Техникалық емес құралдардан болатын ақпаратты жинауға бағытталған оқыс оқиғалар:

- ақпараттың тікелей немесе жанама ашылуына немесе түрленуіне;

- электронды түрде сақталатын жан-жақтылық меншікті ұрлауға;

- есепке алудың бұзылуына, мысалы, есепке алу жазбаларын тіркеу кезінде;

- ақпараттық жүйені дұрыс пайдаланбауға (мысалы, заңның немесе ұйым саясатының бұзылуы) әкеп соқтырады.

Оқыс оқиғалар мысалы, мынадай фактордан болуы мүмкін:

- маңызды деректерден, мысалы, түйінді шифрдан тұратын деректерді сақтау құрылғыларының ұрлануының және ақпаратқа санкцияланбаған рұқсатқа әкеп соқтыратын қауіпсіздіктің физикалық қорғалуының бұзылуы;

- жүйедегі бақыланбайтын өзгерістердің себебінен сәтсіз және (немесе) дұрыс конфигурацияланбаған операциялық жүйелер немесе ұйымның қызметкерлері немесе бөтен қызметкерлер ақпарат алуға рұқсаты болмай-ақ оған қолжетімді болуына әкеп соқтыратын бағдарламалық немесе аппараттық қамтамасыз етудің дұрыс жұмыс істемеуі.

6.3 Санкцияланбаған рұқсат

Санкцияланбаған рұқсат оқыс оқиғалар типі тәрізді бірінші екі типке жатпайтын оқыс оқиғаларды қамтиды. Басты осы тип жүйеге рұқсаттың санкцияланбаған ұмтылысынан немесе жүйені, сервисті немесе желіні дұрыс пайдаланбағаннан тұрады. Санкцияланбаған рұқсаттың кейбір мысалдары техникалық құралдардың көмегімен мыналарды қамтиды:

- паролі бар файлдарды алып тастауға ниет етуді;

- желіге жеңілдетілген рұқсатты алу мақсатында (мысалы, жүйелік әкімшілік деңгейінде) толтырылған буферде рұқсатсыз кіруді;

- заңды желілік байланыстарды қосуды немесе жалған бағытын басып алу үшін хаттаманың осалдығын пайдалануды;

- тұтынушыда немесе әкімшілікте заңды бар ресурстар немесе ақпараттарды салыстыру бойынша ресурстарға немесе ақпараттарға жеңіл жолмен рұқсатты кеңейту ниетін.

Ақпараттың тікелей немесе жанама ашылуына немесе түрленуіне, есепке алудың бұзылуына немесе ақпараттық жүйенің дұрыс пайдаланылмауына әкеп соқтыратын техникалық емес құралдардан болатын санкцияланбаған рұқсаттың оқыс оқиғалары мынадай факторлардан болуы мүмкін:

- кейіннен ақпаратқа санкцияланбаған рұқсатпен физикалық қорғау құрылғыларының бұзылуы;

- жүйедегі бақыланбайтын өзгерістердің себебінен сәтсіз және (немесе) дұрыс конфигурацияланбаған операциялық жүйелер немесе 6.2 бөлімінің соңғы абзацында

сипатталған нәтижелерге әкеп соқтыратын бағдарламалық немесе аппараттық қамтамасыз етудің дұрыс жұмыс істемеуі.

7 «Жоспарлау және дайындық» кезеңі

АҚ-нің оқыс оқиғалары менеджментінің «Жоспарлау және дайындық» кезеңі мыналарды қамтиды:

- АҚ-нің оқиғалары және оқыс оқиғалары туралы және осы саясатқа сәйкесті жүйелер туралы хабарламаларды өңдеудің саясатын құжаттау (туысқандық рәсімдеулерді қоса алғанда);
- ұйымда АҚ-нің оқыс оқиғалары менеджментінің сәйкесті құрылымын құру және сәйкесті қызметкерлерді таңдау;
- оқыс оқиғалардың менеджменті туралы хабарлауды қамтамасыз ету мақсатында оқыту бағдарламаларын жасау және нұсқау өткізу.

Осы кезең аяқталған соң ұйым АҚ-нің оқыс оқиғаларын тиісті өңдеуге толық дайын болуға тиіс.

7.1 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджменті туралы жалпы түсінік

Қажетті жоспарлаудан кейін АҚ-нің оқыс оқиғалары менеджментін пайдалануға енгізудің нәтижелігі және тиімділігі үшін дайындық іс-әрекеттерінің бір қатарын орындау керек. Бұл дайындық іс-әрекеттері мыналарды қамтиды:

- АҚ-нің оқыс оқиғалары менеджментінің саясатын формалауды және әзірлеуді, сондай-ақ осы саясатты жоғары басшылармен бекітуді (7.2-бөлімді қараңыз);
- АҚ-нің оқыс оқиғалары менеджментінің егжей-тегжейлі жүйесін әзірлеуді және құжаттауды (7.3-бөлімді қараңыз). АҚ-нің оқыс оқиғаларының менеджменті жүйесінің құжаттамасы мына элементтерден тұруға тиіс:
- АҚ-нің оқыс оқиғаларының біліктіліктеріне арналған шкаладан 4.2.1 бөлімінде көрсетілгендей маңыздылық шкаласы, мысалы, мынадай: «маңызды» және «маңызды емес» деген екі жағдайдан тұруы мүмкін. Кез келген жағдайда шкаланың жағдайы ұйым операциясының нақты немесе болжанған шығынына негізделген.
- АҚ-нің оқиғалары** және оқыс оқиғалары*** туралы баяндаманың* нысандары (нысандар мысалдары А қосымшасында келтірілген), ұйым қызметінің үзілмеуін қамтамасыз ету жоспарларымен, жүйені, сервисті және (немесе) желілік резервтеуді және деректреді қолдану қалыпты процедураларына сілтемесімен байланысты сайкес құжатталған процедуралар мен әрекеттер.
- қызметтің әртүрлі түрлерін жүзеге асыру үшін тағайындалған жауапты адамдар**** арасында құжатталған міндеттемелері мен бөлінген функциялары бар ТЖЖБ арналған операциялық рәсімдер, мысалы мынадай:
- АТ және (немесе) ұйымның тиісті басшыларының келісімі бойынша және алдын ала келісімге сәйкес белгілі бір жағдайлар кезінде рұқсатсыз кірген жүйені, сервисті және (немесе) желіні ажырату;
- рұқсатсыз кірген жүйені, сервисті және (немесе) желіні жұмыс істеп тұрған жағдайда және желіге қосылған күйінде қалдыру;
- рұқсатсыз кірген жүйеде, сервисте және (немесе) желі деректеріне кіру, шығу және болу ағымдарының мониторингін енгізу;
- жүйенің, сервистің және (немесе) желінің қауіпсіздігі саясатына сәйкес қызметтің

* Егер мүмкін болса, осы нысандарды электронды түрде ұсынылу (мысалы, қорғалған веб-бетте) және АҚ-нің оқиғалары/оқыс оқиғалары туралы электрондық ақпаратты сақтайтын деректер базасымен байланысты болу керек. Қазіргі уақытта қағаз технологиясы өте көп уақытты қажет еткен және тиімсіз болған болар еді.

үздіксіздігін жоспарлау бойынша қалыпты көшірмелеу процедураларын және іс-әрекеттерін активтендіру;

- сот талқылауы немесе ұйым ішінде тәртіптік талқылау үшін оларды қажет ету жағдайларына электронды түрде куәліктерді қорғаныш сақтауды ұйымдастыру және мониторингті жүргізу;

- АҚ-нің оқыс оқиғасы туралы нақты деректерді өз ұйымының қызметкерлеріне және бөтен адамдарға немесе ұйымдарға беру;

- АҚ-нің оқыс оқиғалары менеджменті жүйесінің, оның процестерінің және процедураларының жұмыс істеуін тесттеу (7.3.5 бөлімін қараңыз);

- АҚ-нің оқыс оқиғалары менеджментіне сілтеме енгізу үшін жүйелерге, сервистерге және (немесе) желілерге арналған АҚ-ның менеджментінің және талдауының саясатын, АҚ-нің корпоративтік саясатын, АҚ-ның арнайы саясатын жаңарту және АҚ-нің оқыс оқиғалары менеджменті жүйелерінің шығыс деректерінің контекстіндегі осы саясаттарды тұрақты қайта қарауды қамтамасыз ету (7.4 бөлімін қараңыз);

- қызметкерлер тиісінше бағдарламалық оқыту арқылы АҚОЖТ-ын құру (7.5 бөлімін қараңыз);

- АҚ-нің қауіпсіздігінің оқыс оқиғаларының менеджменті жүйесін қолдаудың техникалық және басқа да құралдары (және АҚОЖТ қызметі) (7.6 бөлімін қараңыз);

- АҚ оқыс оқиғалары менеджменті туралы хабарлауды бағдарламалық қамтамасыз етуді жоспарлау және әзірлеу (7.7 бөлімін қараңыз), ұйымның барлық қызметкерлерін осы бағдарламамен таныстыру (кадр өзгерістері болған жағдайда, одан әрі қайта таныстыру жүргізу).

Кейінгі бөлімшелерде әрбір талап етілетін құжатты қоса алғанда, осы қызметтің әрбір түрін сипаттау келтірілген.

7.2 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің саясаты

7.2.1 Саясатты тағайындау

АҚ-нің оқыс оқиғалары менеджментінің саясаты ұйымның ақпараттық жүйесіне және олардың орналасқан орындарына авторланған рұқсаты бар барлық қызметкерлерге арналған.

7.2.2 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің саясатымен байланысты адамдар

АҚ-нің оқыс оқиғалары менеджментінің саясаты жоғары басшыдан алған өкілеттілігімен құжатпен расталған ұйымның аға лауазымды тұлғасы бекітеді. Саясат әрбір қызметкер және мердігер үшін қолжетімді болуға және нұсқау арқылы таныстырылуға және АҚ саласында олардың хабарлануын қамтамасыз ету мақсатында оқытылуға тиіс. (7.7 бөлімін қараңыз).

** нысанды хабарламаны қабылдайтын адам толтырады (яғни АҚ-нің оқыс оқиғалары менеджменті тобының мүшесі емес).

*** бұл нысан оқыс оқиғаға толық рұқсат еткенге дейін және оқыс оқиғаны бағалауды ағымды жазудың АҚ-нің оқиғасы туралы бастапқы ақпаратты толықтыру үшін АҚ-нің оқыс оқиғалары менеджментінің қызметкерлері пайдаланады. АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасының әрбір сатысында жаңарту енгізіледі. «Толтырылған» деген нысандағы деректер базасындағы жазба немесе АҚ-нің оқиғалары/оқыс оқиғалары туралы мәліметтер бұдан әрі оқыс оқиғаның рұқсаты жөніндегі қызметті пайдаланылады.

**** шағын ұйымдарда сол бір адам бірнеше функцияларды орындауы мүмкін

7.2.3 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің саясатының мазмұны

АҚ-нің оқыс оқиғалары менеджментінің саясаты мынадай мәселелерді қамтуға тиіс:

- ұйым үшін АҚ-нің оқыс оқиғалары менеджментінің мәнін, сондай-ақ менеджментті және оның жүйесін қолдауға қатысты жоғары басшылықтың міндеттерін;

- АҚ-нің оқиғаларын анықтау туралы жалпы ұғымды, олар және тиісті ақпарат туралы, сондай-ақ АҚ-нің оқыс оқиғаларын анықтау үшін осы ақпаратты пайдаланудың жолдары туралы хабарламаны. Бұл жалпы ұғым АҚ-нің АҚ-нің мүмкін оқиғаларының тізбесін, сондай-ақ ол туралы қалай, қайда және кімге хабарлау туралы, сондай-ақ АҚ-нің болған жаңа оқиғаларымен қалай жұмыс істеу қажеттігі туралы ақпаратты қамтуға тиіс;

- іс-әрекеттерді орындау үшін қажетті жауапты адамдардың тізбесін қоса алғанда, АҚ-нің оқыс оқиғаларын бағалау туралы жалпы ұғымды, оқыс оқиғалар және жауапты адамдардың одан әрі іс-әрекеті туралы хабарлауды;

- АҚ-нің оқиғасы расталғаннан кейін іс-әрекеттің қысқаша жазылуы АҚ-нің оқыс оқиғасы болып табылады. Бұл іс-әрекет мыналарды білдіреді:

- тез арада жауап қайтару;

- құқықтық сараптауды;

- тиісті қызметкерлерге немесе тараптық ұйымға ақпарат беруді;

- АҚ-нің оқыс оқиғасы бақылауда екендігін тексеру;

- одан әрі жауап беру;

- «дағдарыс жағдайын» хабарлау;

- АҚ-нің оқыс оқиғасына жауап қайтаруды күшейтудің критерийлерін анықтау;

- оқыс оқиғаға жауапты адамды анықтауды;

- сот талқылауы немесе ұйым ішінде тәртіптік талқылау үшін оларды қажет ету жағдайларына электронды түрде куәліктерді қорғаныш сақтауды қамтамасыз ету мақсатында кейінгі және үздіксіз мониторинг үшін барлық іс-әрекеттерді дұрыс тіркеудің қажеттілігіне жасалатын сілтемені;

- оқыс оқиғадан сабақ алуды және АҚ-нің оқыс оқиғаларынан кейінгі процесті жақсартуды қоса алғанда АҚ-нің оқыс оқиғасының рұқсатынан кейінгі іс-әрекеттер;

- сақтаудың процедураларын қоса алғанда, жүйе туралы құжаттаманы сақтау орнының нақты деректері;

- мынадай мәселелерді қамтитын АҚОЖТ-ның қызметі туралы жалпы ұғымды;

- АҚОЖТ-ның ұйымдастыру құрылымын;

- оқыс оқиғалар туралы жоғары басшылықты қысқаша хабарлауға;

- «дағдарыс жағдайын» хабарлағаннан кейін топ қызметкерлеріне тексеру жүргізуге және басқа да іс-әрекетіне;

- басқа ұйымдармен байланысқа (қажет болғанда) жауапты адамдарды қоса алғанда топтың барлық негізгі қызметкерлерін;

- АҚ-нің менеджменті, АҚОЖТ-ның қызметі аясы және оны жүзеге асыратын шеңбердегі өкілеттілігі туралы ережені; Бұл ереже кем дегенде мақсатты тағайындалуының тұжырымдалуын, АҚОЖТ-ның қызметінің аясын анықтауды және АҚОЖТ-ның құрылтайшысы туралы нақты деректерді және оның мынадай өкілеттіліктерін қамтуға тиіс:

- қызметкерлер тобының негізгі қызметіне қатысты АҚОЖТ-ның мақсатын тұжырымдау. Өз функцияларын орындау үшін қызметкерлер АҚ-нің оқыс оқиғаларын бағалауға, оларға жауап қайтаруға және оларды басқаруға, сондай-ақ жетістік шешімдеріне қатысуға тиіс. АҚОЖТ-ның мақсаты және тағайындалуы үшін нақты және бір мәндегі анықтау талап етіледі;

- АҚОЖТ-ның қызметі саласын анықтауды. Ұйымның АҚОЖТ-ның қызметі саласына әдетте барлық ақпараттық жүйелер, сервистер және ұйымның желілері кіреді.

Кейбір жағдайларда ұйым үшін АҚОЖТ-ның қызметі саласын тарылту қажет етілуі мүмкін. Бұл ретте оның қызметіне жататын не жатпайтын саланы нақты құжаттау қажет;

- АҚОЖТ-ның құрылтайшысының жеке басын - АҚОЖТ-ның қызметін санкциялайтын және АҚОЖТ-на берілген өкілеттіліктің деңгейін белгілейтін аға лауазымды адамды (басқару мүшесі, аға басшы). Бұл туралы хабарлану ұйымның барлық қызметкерлеріне АҚОЖТ-на сенімді қалыптастыру үшін өте маңызды ақпарат болып табылатын АҚОЖТ-ның құрылымын және құрудың сілтемесін түсінуге мүмкіндік береді. АҚОЖТ-ын құру және оның құрылымы туралы егжей-тегжейді жариялау алдында осы іс-әрекеттің заңдылығын тексеру қажет. Кейбір жағдайларда қызметкерлер тобының өкілеттілігін ашу міндеттерді бұзушылық бойынша дауларды оның анықтауына себепші болуы мүмкін;

- АҚ-нің оқыс оқиғалары менеджментін хабарлауды және оқытуды бағдарламалық қамтамасыз ету туралы жалпы ұғым;

- қарауға жататын нормативтік-құқықтық аспектілердің тізбесі (5.2.3 бөлімі).

7.3 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің бағдарламасы

7.3.1 Бағдарламаның тағайындалуы

АҚ-нің оқыс оқиғалары менеджментінің бағдарламасы АҚ-нің оқыс оқиғаларын өңдеудің процестерін және процедураларын сипаттайтын егжей-тегжейлі құжаттарды құруға және АҚ-нің оқыс оқиғалары туралы хабарлауға (ақпарат беру) арналған. АҚ-нің менеджментінің бағдарламасы АҚ-нің оқиғасын анықтаған кезде қолданысқа енгізіледі.

Ол:

- АҚ-нің оқиғаларына жауап беру;

- АҚ-нің оқыс оқиғалары болуын анықтау;

-оларға рұқсат еткенге дейін АҚ-нің оқыс оқиғаларының менеджменті;

- оқыс оқиғаларды өңдеу кезінде, сондай-ақ жалпы жүйені және (немесе) қауіпсіздікті қажетті жақсарту кезінде алынған сабақтарды сәйкестендіру;

- сәйкестендірілген жетілдіруді іске асыру кезінде нұсқау ретінде пайдаланылады.

7.3.2 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің бағдарламасымен байланысты адамдар

АҚ-нің оқыс оқиғалары менеджментінің бағдарламасы мыналарға:

- АҚ-нің оқиғалары туралы анықтауға және хабарлауға. Бұл адамдар тұрақты негіздегі немесе келісім-шарт бойынша жұмыс істейтін қызметкер болуы мүмкін.

- АҚ-нің оқыс оқиғаларының рұқсат ету кезеңіндегі сабақтарды алып тастауға және АҚ-н жақсартуға және АҚ-нің оқыс оқиғалары менеджментінің бағдарламасына қатысатын АҚ-нің оқиғаларын және АҚ-нің оқыс оқиғаларын бағалауға және оған жауап қайтаруға жауапты адамдарды қоса алғанда ұйымның барлық қызметкерлеріне арналған. Бұл адамдар АҚОЖТ–ын пайдалануды қамтамасыз ететін топтардың (немесе осыған ұқсас топтың) мүшелері, ұйымның басшысы, қоғаммен байланыс жөніндегі бөлімнің қызметкерлері және заңгерлер болып табылады.

АҚ-нің оқыс оқиғалары және олармен байланысты осалдықтар туралы үшінші тараптың тұтынушыларын, одан басқа АҚ-нің оқыс оқиғалары және осалдықтары туралы ақпарат беретін мемлекеттік және коммерциялық ұйымдарды есепке алу қажет.

7.3.3 Ақпараттық қауіпсіздіктің оқыс оқиғалары менеджментінің бағдарламасының мазмұны

Ақпараттық қауіпсіздік оқыс оқиғалары менеджментінің бағдарламасының мазмұны мыналарды қамтуға тиіс:

а) АҚ-нің оқыс оқиғалары менеджментінің саясатына шолуды;

б) жалпы АҚ-нің оқыс оқиғалары менеджментінің бағдарламасы туралы жалпы ұғымды;

в) тиісті сервистік бағдарламалар және шкалалар туралы егжей-тегжейлі процесстерді және процедураларды*, маңызды оқиғалардың/оқыс оқиғалардың қабылданған шкалаларын пайдалана отырып, АҚ-нің оқиғаларына бағалау жүргізуге (оларды бөлшектеу қажет етілсе) және АҚ-нің оқыс оқиғаларының санатына олардың өзінің санатын өзгертуге қабілеттілігін анықтауға байланысты ақпаратты;

1) «Жоспарлау және дайындық» кезеңі үшін:

– АҚ-нің оқиғаларының пайда болуы туралы анықтаумен және хабарлаумен (адам немесе автоматты түрде);

– АҚ-нің оқиғалары туралы ақпаратты жинаумен.

2) «Пайдалану» кезеңі үшін (АҚ-нің оқыс оқиғалары расталған жағдайда):

- барлық ұйымның қызметкерлеріне және бөгде адамдарға немесе ұйымға АҚ-нің оқыс оқиғаларының немесе оқыс оқиғаларға қатысты кез келген маңызды бөліктердің болуы хабарлаумен;

- оқыс оқиғаларға қатысты маңызды шкаласының қабылданған деңгейіне және талдауға сәйкес хабарламаны қалпына келтіру және (немесе) тиісті қызметкерлерге беру процедураларын активтендіруді қамтуы мүмкін жылдам жауап қайтаруды жүзеге асырумен;

- АҚ-нің оқыс оқиғаларының маңызды шкалалары деңгейлері бойынша құқықтық сараптау (қажет болғанда) жүргізумен және осы деңгейлердің өзгеруімен;

- АҚ-нің оқыс оқиғаларын бақылаудың болуын анықтаумен;

- анағұрлым кеш қажет етілуі мүмкін жауап қайтаруларды (мысалы, қандай да бір апаттың салдарларын жою кезінде) қоса алғанда (егер қажет етілсе), қосымша жауап қайтаруларды жасау арқылы;

- АҚ-нің оқыс оқиғаларына бақылау болмаған жағдайда, дағдарысқа қарсы іс-әрекеттерге бастамалық етумен (мысалы, өрт командасын шақыру немесе ұйым қызметінің үздіксіздігін қамтамасыз ету жоспарын активтендіру), одан әрі бағалау және (немесе) егер одан әрі шешу қажет етілсе, егжей-тегжейлеумен, одан әрі талдау үшін барлық қызметті тіркеудің дұрыстығын тексерумен, АҚ-нің оқиғаларының/оқыс оқиғаларының деректері базасын жаңартумен.

АҚ-нің оқыс оқиғалары менеджментінің бағдарламасында АҚ-нің оқыс оқиғаларына жедел және неғұрлым ұзақ жауап қайтару мүмкіндігі қарастырылады. АҚ-нің барлық оқыс оқиғалары үшін қысқа мерзімді және ұзақ мерзімді әлеуетті жағымсыз әсерді қазіргі заманғы бағалауды талап етеді (мысалы, үлкен масштабты апат АҚ-нің алғашқы оқыс оқиғасынан кейін бірнеше уақыттан соң болуы мүмкін).

Сонымен қатар, жауап қайтарудың бірнеше түрі арнайы қорғау шараларында қажеттілік туындаған кезде, АҚ-нің нағыз болжанбаған оқыс оқиғалар үшін қажет етілуі мүмкін. Осындай жағдайда да бағдарламаның құжаттамасында мыналар үшін қажет болуы мүмкін іс-әрекеттер жөнінде жалпы ұсынымдар.

3) «Талдау» кезеңі үшін:

– егер қажет етілсе, бұдан әрі құқықтық сараптау жүргізумен;

– АҚ-нің оқыс оқиғаларынан алынған тәжірибені сәйкестендірумен және құжаттаумен;

– алынған тәжірибе негізінде АҚ-н жақсартуды анықтаумен және талдаумен;

– АҚ-нің оқыс оқиғаларына жауап қайтару процестерінің және процедураларының тиімділігін талдаумен, АҚ-нің оқыс оқиғаларын және олардың әр қайсысынан кейін қалыпқа келтіруді бағалаумен, сондай-ақ жалпы АҚ-нің оқыс оқиғалары менеджментінің бағдарламасын жақсартуды анықтаумен (алынған тәжірибе

негізінде);

– АҚ-нің оқыс оқиғалары/оқыс оқиғаларының деректер базасын жаңартумен.

4) «Жетілдіру» кезеңі үшін – алынған тәжірибе негізінде нақтылау:

- АҚ-нің қауіп-қатерлер менеджментінің және талдауының нәтижелері,

- АҚ-нің оқыс оқиғалары менеджментінің бағдарламасы (мысалы, ұйымның хабарлау және (немесе) құрылымы нысаны, процестері және процедуралары)

– жаңа және (немесе) қорғау шараларын енгізудің жалпы қауіпсіздігі,

– оқиғалардың/оқыс оқиғалардың және тиісті басшылықтың маңыздылығы (мысалы, маңызды, маңызды емес, елеулі, шұғыл, маңызды емес, шұғыл емес) шкалаларының жоғарылау көрсеткіші,

– сәйкестендіру жүргізілуге тиіс және қандай рәсімдерге сәйкес сәйкестендірудің қажеттілігі шешімдерге басшылық етумен. АҚ-нің оқиғасын немесе оқыс оқиғасын бағалайтын қызметкерлер қалыпты жағдайларда және кім үшін процестерді сәйкестендіруге ауысу қажет болғанда АҚ-нің оқыс оқиғалары менеджментінің бағдарламалары құжаттамаларынан алынған нұсқауға негіздей отырып, білуге тиіс. Одан басқа процестерді сәйкестендіру қажет болған кезде болжанбаған жағдайлар туындауы мүмкін. Мысалы, АҚ-нің маңызды емес оқыс оқиғасы оны дұрыс өңдемеген жағдайда, «елеулі» немесе «дағдарыс жағдайы» санатына ауысуы немесе апта бойы өңделмеген АҚ-нің маңызды емес оқиғасы АҚ-нің «маңызды» болуы мүмкін. Нұсқауда АҚ-нің оқиғалары және оқыс оқиғалары типін, оны өткізуі мүмкін адамдардың және процестердің сәйкестендіру типтерін анықтауға тиіс.

– тиісті нысанда барлық іс-әрекеттерге тиісті тіркеу үшін қажетті процедуралармен және тағайындалған қызметкерлерді тіркеу журналына талдау жүргізумен,

– АҚ-нің оқиғаларын және оқыс оқиғаларын бақылауды, АҚ-нің оқыс оқиғалары туралы есеп беруді жаңартуды және бағдарламаның өзін жаңартуды қамтитын өзгерістерді бақылаудың режімін қолдаудың процедураларымен және механизмдерімен,

– құқықтық сараптау процедураларымен,

– құқықтық және нормативтік аспектілермен байланысты сақтауды қамтамасыз ететін рұқсатсыз басып кірулерді (РБК) анықтау жүйесін пайдалану жөніндегі процедуралармен және нұсқаумен (5.2.3 бөлімін қараңыз). Нұсқау қаскүнемді бақылау бойынша іс-әрекеттердің артықшылығын және кемшіліктерін қарауды қамтуға тиіс,

– бағдарламаны ұйымдастыру құрылымымен,

– жалпы АҚОЖТ-ы мүшелерінің және оның кейбір мүшелерінің құзыретімен және міндеттерімен, байланыс топтары туралы маңызды ақпаратпен жазылуға тиіс.

7.3.4 Процедуралар

АҚ-нің оқыс оқиғалары менеджментінің бағдарламасымен жұмыс істеу алдында құжатталған және тексерілген процедуралардың болуы қажет. Әрбір процедура бойынша құжаттамада пайдалануды қолдау тобының пайдалануға және осы процедуралардың менеджментіне жауапты АҚОЖТ-ның адамдары көрсетілуге тиіс. Мұндай процедуралар сот тергеуі немесе ұйымның ішінде тәртіптік талқылау жүргізу жағдайында үздіксіз бақылануға тиіс жинау процедураларын және электронды куәліктердің қорғап сақталуын қамтуға тиіс. Одан басқа, пайдалануды қолдау тобының және АҚОЖТ-ның іс-әрекеттерін ғана емес, сонымен қатар егер олар тағы басқа жерде, мысалы, ұйым қызметінің үздіксіздігін қамтамасыз ету жоспарына қатыстырылмаған құқықтық сараптауға және «дағдарысқа қарсы» іс-әрекетке қатыстырылған процедураларды қамтитын құжатталған процедуралар болуға тиіс. Осы құжатталған процедуралар АҚ-нің оқыс оқиғалары менеджментінің құжатталған саясатқа және АҚ-нің оқыс оқиғалары менеджменті бағдарламаларының басқа құжаттамасына толық сәйкес болуға тиіс.

Барлық процедуралар жалпыға бірдей қолжетімді болмайтынын білу қажет. Мысалы, ұйымның барлық қызметкерлері АҚОЖТ-мен өзара әрекет кезінде АҚОЖТ-ның жұмысы туралы білмегені дұрыс. АҚОЖТ жеңіл қолжетімді нысанда, мысалы, ұйым интернатындағы АҚ-нің оқыс оқиғаларын талдау нәтижелерінен алынған ақпаратты қоса алғанда, «жалпыға бірдей қолжетімдік» нұсқауының болуын қамтамасыз етуге тиіс. Ұйым ішіндегі құпия ақпаратты білетін адам зерттеу процесіне кедергі жасай алмайтындай АҚ-нің оқыс оқиғалары менеджменті бағдарламаларының кейбір бөліктерін ашпаған дұрыс. Мысалы, ақша қаражатын иеленген банк қызметкері бағдарламаның кейбір бөліктерімен таныс делік, онда ол өз іс-әрекетін тергеуді жасыруы немесе басқадай жолмен АҚ-нің оқыс оқиғасын анықтауға және тексеру жүргізу және кейіннен қалпына келтіруге кедергі жасауы мүмкін.

Жұмыс процедураларының мазмұны көптеген критерийлерге байланысты, әсіресе, АҚ-нің бұрын белгілі әлеуетті оқиғаларының және оқыс оқиғаларының сипатына және ақпараттық жүйелердің әрекет етілген активтерінің типтеріне және олардың ортасына байланысты. Қандай да бір жұмыс процедурасы оқыс оқиғалардың белгілі бір типімен немесе өнім типімен (мысалы, желіаралық экран, деректер базасы, операциялық жүйелер, қосымша), немесе арнайы өніммен байланысты болуы мүмкін. Әрбір жұмыс процедурасында қандай қадам қабылдау және кім қабылдау қажеттігі анық анықталуға тиіс. Ол ішкі және сыртқы көздерден (мысалы, мемлекеттік немесе коммерциялық АҚОЖТ-ы, немесе ұқсас топтары, сондай-ақ өнім берушілер) алынған тәжірибесін көрсетуге тиіс.

АҚ-нің оқиғалары және оқыс оқиғаларының бұрын белгілілі типтерін өңдеу үшін жұмыс процедуралары болуға тиіс. Сонымен қатар, егер анықталған АҚ-нің оқыс оқиғасы немесе оқиғасының типі белгілі болса, соның ізімен жүретін жұмыс процедуралары қажет. Осындай жағдайда мынадай аспектілер көзделеді:

- осындай «ерекше жағдайларды» өңдеу үшін хабарлау процесі;
- жауап қайтаруды кешіктіруді болдырмау мақсатында басшылық тарапы оқыс оқиғаға жауап қайтаруды мақұлдауды алу үшін уақытты анықтайтын нұсқау,
- мақұлдаудың қарапайым процесінсіз шешім қабылдауды алдын ала мақұлданған өкілеттілік.

7.3.5 Бағдарламаны тесттеу

АҚ-нің оқиғалары және оқыс оқиғалары менеджментінің процесінде туындауы мүмкін әлеуетті ақаулар мен проблемаларды анықтау үшін АҚ-нің оқыс оқиғалары менеджментінің процестері мен процедураларын тұрақты тексеруді және тесттеуді жоспарлауы қажет. АҚ-нің оқыс оқиғаларын және жауап қайтаруын талдау нәтижесінде туындайтын кез келген өзгерістер қатаң түрде тексеруге және тестілеуге жатуы тиіс.

7.4 Ақпараттық қауіпсіздіктің және қауіп-қатерлер менеджментінің саясаты

7.4.1 Тағайындау

АҚ-нің оқыс оқиғалары менеджментінің мазмұнын АҚ-на және қауіп-қатерлер менеджментінің корпоративтік саясатына және жүйелердің, сервистердің және желілердің АҚ-нің арнайы саясатына енгізу мақсаттары:

- АҚ-нің оқыс оқиғалары менеджментінің, әсіресе АҚ-ның оқыс оқиғаларын хабарлау және өңдеу жүйесінің маңыздылығын сипаттау;
- АҚ-нің оқыс оқиғаларына тиісті дайындыққа қатысты жоғары басшылықтың міндеттерін және АҚ-нің оқыс оқиғасы менеджментінің жүйесіне қатысты жауап қайтаруды көрсету;
- әр түрлі саясаттардың келісуін қамтамасыз ету;
- оқыс оқиғалардың жағымсыз әсерін азайту үшін АҚ-нің оқыс оқиғасына жоспарлы

және жүйелі жауап қайтаруды қамтамасыз ету болып табылады.

7.4.2 Мазмұны

АҚ-не және қауіп-қатерлер менеджментінің корпоративтік саясаты, сондай-ақ жүйелердің, сервистердің және желілердің АҚ-нің арнайы саясаты АҚ-нің және оқыс оқиғалары менеджментінің жалпы саясатына нақты сәйкестігін және оның жүйесіне сәйкес қамтамасыз ету мақсатында жаңартылуға тиіс. Тиісті бөлімдерге жоғары басшылықтың міндеттерін және сипатталуын енгізу қажет:

- саясатты;
- жүйенің және тиісті инфрақұрылымның процестерін;
- оқыс оқиғаларды анықтау, хабарлау, бағалау және оны басқару бойынша талаптарды;
- авторлауға және (немесе) белгілі бір маңызды іс-әрекетті жүргізуге жауапты қызметкерлерді анықтауды (мысалы, ақпараттық жүйені off-line режиміне ауыстыру немесе жүйені ажырату).

Одан басқа, корпоративтік саясат АҚ-не және қауіп-қатерлер менеджментінің корпоративтік саясатының, сондай-ақ жүйелердің, сервистердің және желілердің АҚ-нің арнайы саясатының тұрақты нәтижелігін қамтамасыз ету үшін кіріс деректері ретінде АҚ-нің оқыс оқиғаларын анықтау, мониторингі және рұқсат ету процестерінің нәтижесінде алынған кез келген ақпаратты пайдалануды қамтамасыз ету үшін талдаудың тиісті механизмін құру туралы талаптарды қамтуға тиіс.

7.5 Ақпараттық қамтамасыз етудің оқыс оқиғасына жауап қайтару тобын тағайындау

7.5.1 Ақпараттық қамтамасыз етудің оқыс оқиғасына жауап қайтару тобын тағайындау

АҚОЖТ-ы құру мақсаты АҚ-ның оқыс оқиғасын бағалау, оған жауап қайтару және олардан сабақ алу, сондай-ақ қажетті үйлестіру, менеджмент, ақпаратты берудің айналым байланысы және процесі үшін ұйымды тиісті қызметкерлермен қамтамасыз ету болып табылады. АҚОЖТ-ның мүшелері физикалық және қаржылық шығынды, сондай-ақ АҚ-нің оқыс оқиғаларымен байланысты ұйымның беделі үшін шығынды азайтуға қатысуы мүмкін.

7.5.2 Ақпараттық қауіпсіздіктің оқыс оқиғаларына жауап қайтару тобының мүшелері және осы топтың құрылымы

АҚОЖТ-ның құрамы және қызметкерлер саны, сондай-ақ АҚОЖТ-ның құрылымы ұйымның масштабына және құрылымына сәйкес болуға тиіс. АҚОЖТ-ы оқшау команданы немесе бөлімді білдіруі мүмкін, осы топтың қызметкерлері басқа да міндеттерді орындауы, сондай-ақ ұйымның әр түрлі бөлімшелерінен қызметкерлерді қатыстыруы мүмкін. АҚОЖТ-ның көп жағдайында 4.2.1 және 7.1 бөлімдеріне сәйкес аға басшы басқаратын жұмыс істеуші топ болуға тиіс. Жоғары басшыға нақты мәселелер бойынша, мысалы, АҚ-нің оқыс оқиғасы типіне байланысты қатыстырылатын зиян келтіретін бағдарламалардың рұқсатсыз кіруін көрсету бойынша мамандар көмек көрсетеді. Ұйым құрамы санына байланысты АҚОЖТ-ның қызметкерлері АҚОЖТ-ның ішінде бірнеше функцияларды орындай да алады. АҚОЖТ-нда ұйымның әр түрлі бөлімшелерінің қызметкерлері де қатыстырылуы мүмкін (мысалы, операциялар, АТ/телекоммуникация, аудит, кадр бөлімі және маркетинг).

Топ мүшелері ұйым ішінде олардың есімдері және олардың алмастыратын адамдардың есімдері, сондай-ақ олармен байланысты нақты деректер қолжетімді болуға тиіс. Мысалы, АҚ-нің оқыс оқиғалары менеджментінің жүйесі құжаттамасында

процедуралар және есеп берулер нысандары бойынша, бірақ саясаттағы емес кез келген құжаттарды қоса алғанда қажетті бөліктерді нақты көрсетуге тиіс.

АҚОЖТ-ның басшысы:

- оқыс оқиғаға қатысты шара қабылдау туралы шешімді дереу қабылдау өкілеттілігі болуы;

- әдетте, қарапайым операциядан оқшаулануға тиіс жоғары басшыны хабардар ету үшін жеке желі болуы;

- АҚОЖТ-ның барлық мүшелері үшін білім мен шеберліктің қажетті деңгейін, сондай-ақ осы деңгейді қолдауды қамтамасыз етуі;

- топтың неғұрлым құзырлы мүшесіне әрбір оқыс оқиғаны зерттеуді тапсыруға тиіс.

7.5.3 Ұйымның басқа бөлімшелерімен өзара іс-әрекет

АҚОЖТ-ның басшысының және оның тобының мүшесінің өкілеттілік деңгейі АҚ-ның оқыс оқиғасына барабар қажетті іс-әрекетті қабылдауға мүмкіндік беруге тиіс.

Бірақ, қаржыға және беделге қатысты ұйымға жағымсыз әсер етуі мүмкін іс-әрекеттер жоғары басшымен келісуге тиіс. Сондықтан АҚ-нің оқыс оқиғалары менеджменті саясатын қамтамасыз ету жүйесінде қандай орган, АҚОЖТ-ның басшысы АҚ-нің маңызды оқыс оқиғалары туралы хабарлайтыны нақтылануға тиіс.

Бұқаралық ақпарат құралдарымен хабарлау процедуралары және осы хабарлауға жауапкершілік жоғары басшымен келісілуі, құжатталуы және мыналар:

- бұқаралық ақпарат құралдарымен жұмысты ұйымдастырушы өкіл;
- АҚОЖТ-мен ұйым бөлімшелерінің өзара әрекет әдісі анықталуға тиіс.

7.5.4 Тараптық тұлғалармен және ұйымдармен қарым-қатынас

АҚОЖТ-ы және тиісті тараптық тұлғалар және ұйымдар арасындағы қарым-қатынасты белгілеу қажет.

Бөгде адамдарға және ұйымдарға мыналар жатады:

- шарт бойынша жұмыс істейтін бөгде көмекші қызметкерлер, мысалы, КТЖЖБ;
- бөгде ұйымдардың АҚОЖТ-ы, сондай-ақ КТЖЖБ;
- құқық қолдану ұйымдары;
- апаттық қызмет (мысалы, өрт сөндіру бригадасы/бөлімшесі);
- тиісті мемлекеттік ұйымдар;
- заң қызметкерлері;
- қоғаммен және (немесе) бұқаралық ақпарат құралдарымен байланыс жөніндегі арнайы адам;
- бизнес бойынша серіктестер;
- тұтынушылар;
- қоғамдық.

7.6 Ақпараттық қауіпсіздіктің жауап қайтаруын техникалық және басқа да қолдау

АҚ-нің оқыс оқиғаларына тез арада және тиімді жауап қайтару барлық қажетті техникалық және басқа да құралдар қолдау тапқанда, дайындалғанда және тесттелгенде жеңіл жүзеге асырылады.

Осындай іс-шаралар мыналарды қамтиды:

- ұйым активтерінің бөліктерін (активтердің жаңартылған тізбесі болуы) және олардың ұйым қызметімен байланысы бойынша ақпаратқа қолжетімдігін;

- ұйым қызметінің үздіксіздігін қамтамасыз етудің құжатталған стратегиясына және тиісті жоспарға қолжетімдікті;

- ақпарат берудің құжатталған және жарияланған процестерін;

- АҚ-нің оқиғалары/оқыс оқиғаларының электронды деректер базасын және деректер базасын тез арада толтыру және жаңарту үшін техникалық құралдарды, оның ақпаратының талдауын пайдалануды және жауап қайтару процестерін жеңілдетуді (қолдан жасалған жазба кейде қажет етілетінін және ұйым пайдалану жалпыға бірдей қабылданған);

- АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасы үшін ұйым қызметінің үздіксіздігін қамтамасыз ету бойынша барабар шараларды.

Деректер базасын тез арада толтыру, жаңарту, ақпарат және деректер базасы мазмұнын талдау және АҚ-нің оқыс оқиғаларына жауап қайтару процестерін жеңілдету үшін пайдаланылатын техникалық құралдар мыналарға әсер етуге тиіс:

- АҚ-нің оқиғалары және оқыс оқиғалары туралы есептерді дереу алуға;

- бұрын жұмыс істеген қызметкерлерге (тиісті бөгде адам) осыған сәйкес келетін құралмен (мысалы, электронды пошта, факс, телефон және т.б. арқылы), яғни деректердің сенімді нақты базасын сұрата отырып (барлық уақытта жеңіл қолжетімді болуы және қағаз және басқа да көшірмелері болуға тиіс) қауіпсіз (қажет болғанда) әдіспен ақпарат беру құралымен таныстыруға;

- бағаланған қауіп-қатерге сәйкес абай болуды, Интернет арқылы немесе жүйеге, сервиске және (немесе) желіге рұқсатсыз кіру уақытында іске асырылатын электронды байланыстың басқа адаммен тыңдалуынан қорғауды сақтауға;

- бағаланған қауіп-қатерге сәйкес абай болуды, Интернет арқылы немесе жүйеге, сервиске және (немесе) желіге рұқсатсыз кіру уақытында жүзеге асырылатын электронды байланыстың басқа адаммен тыңдалуынан қорғауды сақтауға;

- ақпараттық жүйе, сервис және (немесе) желі туралы барлық деректерді және барлық өңделетін деректерді жинау процесіне;

- криптографиялық бақылау жүйенің, сервистің және (немесе) желінің қандай бөлігі өзгергенін анықтауға әсер етуі үшін бағаланған қауіп-қатерге сәйкес келсе және деректер өзгерген болса, криптографиялық бақылаудың тұтастығын пайдалануға;

- жиналған ақпаратты мұрағаттауды және қорғауды жеңілдетуге (мысалы, тіркеу журналындағы жазбалардағы цифрлік қолдарды және CD немесе DVD ROM құрылғыларында оқылуға арналған тасымалдағыштардағы дербес режімді сақтау алдындағы басқа да куәліктерді қолдана отырып);

- АҚ-нің оқыс оқиғасын дамытуды көрсететін баспаларды (мысалы, тіркеу журналын), оқыс оқиғаға рұқсат ету және ақпараттың сақталуын қамтамасыз ететін процесті;

- мыналардың:

резервтеудің тиімді процедураларының, нақты және сенімді резервтік көшірмелердің, резервтік көшірмелерді тестілеудің, зиян тасымалдағыш бағдарламаларды бақылаудың;

жүйелік және қолданбалы бағдарламалық қамтамасыз етумен ақпараттың шығыс тасымалдағышының;

ұйымның үздіксіз қызметін қамтамасыз етудің тиісті жоспарымен келісілген жүйелер және қосымшалар үшін сенімді және жаңартылған түзетулердің («патчея») көмегімен ақпараттық жүйенің, сервистің және (немесе) желі жұмысының штаттық режімін қалыпқа келтіруге.

Рұқсат кірген ақпараттық жүйе, сервис және (немесе) желі дұрыс жұмыс істемеуі мүмкін. Сондықтан АҚ-нің оқыс оқиғасына жауап қайтару үшін қажет техникалық құрылғының (бағдарламалық немесе аппараттық қамтамасыз ету) жұмысы ұйымда пайдаланылатын жүйелерге, сервистерге және (немесе) желіге негізделуге тиіс. Мүмкіндігіне қарай оқыс оқиғаларға жауап қайтарудың техникалық құралдары толық автоматтанған болуға тиіс.

Барлық техникалық құралдар мұқият таңдап алынуға, дұрыс енгізілуге және тұрақты тесттелуге (алынған резервтік көшірмелерді тестілеуді қоса алғанда) тиіс.

Осы бөлімде сипатталған техникалық құралдар АҚ-нің оқыс оқиғаларын анықтау және тиісті адамдарды автоматты хабарлау және рұқсатсыз басып кіру үшін тікелей пайдаланылатын техникалық құралдарды қамтымайды. Осы техникалық құралдар [1] және [2] сипатталған.

7.7 Хабарлауды қамтамасыз ету және оқыту

АҚ-нің оқыс оқиғалары менеджменті – бұл техникалық құралдарды ғана емес, сонымен қатар қызметкерлерді қамтитын процесс, бұл процесті ұйымда жұмыс тиісті жолмен оқытылған және ақпарат қауіпсіздігі мәселелерімен хабарланған адамдар қолдауға тиіс.

Ұйымның барлық қызметкерлерінің хабарлануы және қатысуы АҚ-нің оқыс оқиғаларының менеджментіне құрылымдық тәсілдің жетістігін қамтамасыз ету үшін өте маңызды. Сондықтан, АҚ-нің оқыс оқиғалары менеджментінің қызметі АҚ-нің мәселелерінде оқытудың және хабарлауды қамтамасыз етудің жалпы бағдарламасының бір бөлігі белсенді қолдауға тиіс. Хабарлауды қамтамасыз ету бағдарламасына тиісті материал бөгде ұйымдарды және жаңа қызметкерлерін, тұтынушыларын және мердігерлерді қоса алғанда, барлық қызметкерлер үшін қолжетімді болуға тиіс. АҚОЖТ мүшелері үшін, ал қажет болғанда АҚ-не жауапты қызметкерлер және арнайы әкімдер үшін пайдалануды қамтамасыз етудің топтарына арналған оқытудың арнайы бағдарламасы болуға тиіс. Оқыс оқиғалар менеджментіне қатысатын әр топ үшін АҚ-нің оқыс оқиғалары менеджментінің жүйесімен олардың өзара іс-әрекетінің типіне, жиілігіне және маңыздылығына байланысты дайындықтың әр түрлі деңгейлері талап етілуі мүмкін.

Хабарлауға оқыту жөніндегі нұсқау мыналарды қамтуға тиіс:

- АҚ-нің оқыс оқиғалары және оқиғалары менеджменті бойынша жұмыс технологиясын және оның іс-әрекеті саласын қоса ала отырып, АҚ-нің оқыс оқиғалары менеджментінің жүйесі жұмысының негізін;
- АҚ-нің оқыс оқиғалары және оқиғалары туралы хабарлау әдісін;
- көздердің құпиялығын қамтамасыз ету бойынша қорғау шараларын (қажет болғанда);
- жүйенің сервис деңгейі туралы келісімді;
- нәтижелері туралы хабарлау – көздер қандай жағдайларда хабарланатын болады.
- ақпаратты таратпау туралы келісіммен жасалатын кез келген шектеулер;
- АҚ-нің оқыс оқиғалары менеджментін ұйымдастырудың өкілеттілігі және оның хабарлау желісін;
- АҚ-нің оқыс оқиғалары менеджментінің жүйесінен кім және қалай есеп алатынын.

Кейбір жағдайларда АҚ-нің оқыс оқиғалары менеджменті туралы хабарлануды қамтамасыз етудің нақты деректерін басқа оқыту бағдарламасына (мысалы, қызметкерлерді болжау бағдарламасына немесе АҚ-нің мәселелеріндегі хабарлануды қамтамасыз етудің жалпы корпоративтік бағдарламасына) арнайы қосқан жөн. Бұл хабарланудың қамтамасыз етуіне тәсіл қызметкерлердің белгілі бір тобымен байланысты бағалы ақпаратты ұсынуы мүмкін және оқыту бағдарламасының тиімділігін және нәтижелігін жақсартуы мүмкін.

АҚ-нің оқыс оқиғалары менеджментінің жүйесін пайдалануға енгізгенге дейін барлық жұмыс істеп жүрген қызметкерлер АҚ-нің оқиғалары туралы анықтау және хабарлау процедураларымен танысуға тиіс, ал арнайы іріктелген қызметкерлер кейінгі процестерге қатысты жақсы хабарлануға тиіс. Содан кейін хабарлануды қамтамасыз ету бойынша тұрақты нұсқау және даярлық курстары жүргізіледі. Дайындық пайдалануды қамтамасыз ету тобының және АҚОЖТ-ның мүшелерінің, сондай-ақ АҚ-не жауапты

қызметкерлердің және арнайы әкімдіктердің арнайы жаттығуларымен және тестілеумен қоса жүруге тиіс.

8 «Пайдалану» кезеңі

8.1 Кіріспе

Пайдалану процесінде АҚ-нің оқыс оқиғалары менеджменті АҚ-нің оқыс оқиғаларынан алынған сабақтардың нәтижесінде сәйкестендірілген кез келген жетілдіру жүргізілетін «Жетілдіру» кезеңі болатын «Пайдалану» және «Талдау» кезеңдерінен тұрады. Бұл кезеңдер және олармен байланысты процестер 4.2 бөлімінде келтірілген. Осы бөлімде «Пайдалану» кезеңі, 9-бөлімде «Талдау» кезеңі, ал 10-бөлімде «Жетілдіру» кезеңі көзделеді. Бұл үш кезең және оған сәйкесті процестер 2-суретте берілген.

8.2 Түйінді процестерге шолу

«Пайдалану» кезеңіндегі түйінді процестер:

а) АҚ-нің оқиғаларын анықтау және ұйым қызметкерінің, қызметкерлер/клиенттің бірі немесе автоматты түрде (мысалы, желіаралық экранның дабыл сигналы) ол туралы хабарлауы;

б) АҚ-нің оқиғалары туралы ақпарат жинау және оқиға АҚ-нің оқыс оқиғасы болып табылады ма немесе дабылдың жалған сигналы ма екендігін анықтау мақсатында ұйымның пайдалануды қамтамасыз ету тобының қызметкерлері* бастапқы бағалау жүргізуі;

в) оқиға АҚ-нің оқыс оқиғасы болып табылатынын растау және рас болған жағдайда дереу жауап қайтаруға бастамалық ету мақсатында АҚОЖТ-на екінші бағалау жүргізу, сондай-ақ құқықтық сараптау қажеттігі және ақпарат беру бойынша іс-әрекеті;

г) оқыс оқиға бақылауда екендігін анықтау мақсатында жүргізілетін АҚОЖТ–ын талдау:

1) оң жағдайда одан әрі қажетті жауап қайтаруға бастамалық жасалады және оқыс оқиғаның салдарын талдау процесінде пайдалану үшін барлық ақпараттың дайындығын қамтамасыз етеді,

2) теріс жауап кезінде тиісті қызметкерлерді қатыстыру арқылы дағдарысқа қарсы іс-әрекетке бастамалық етеді, мысалы, басшының және ұйымның үздіксіз қызметін қамтамасыз ету тобы;

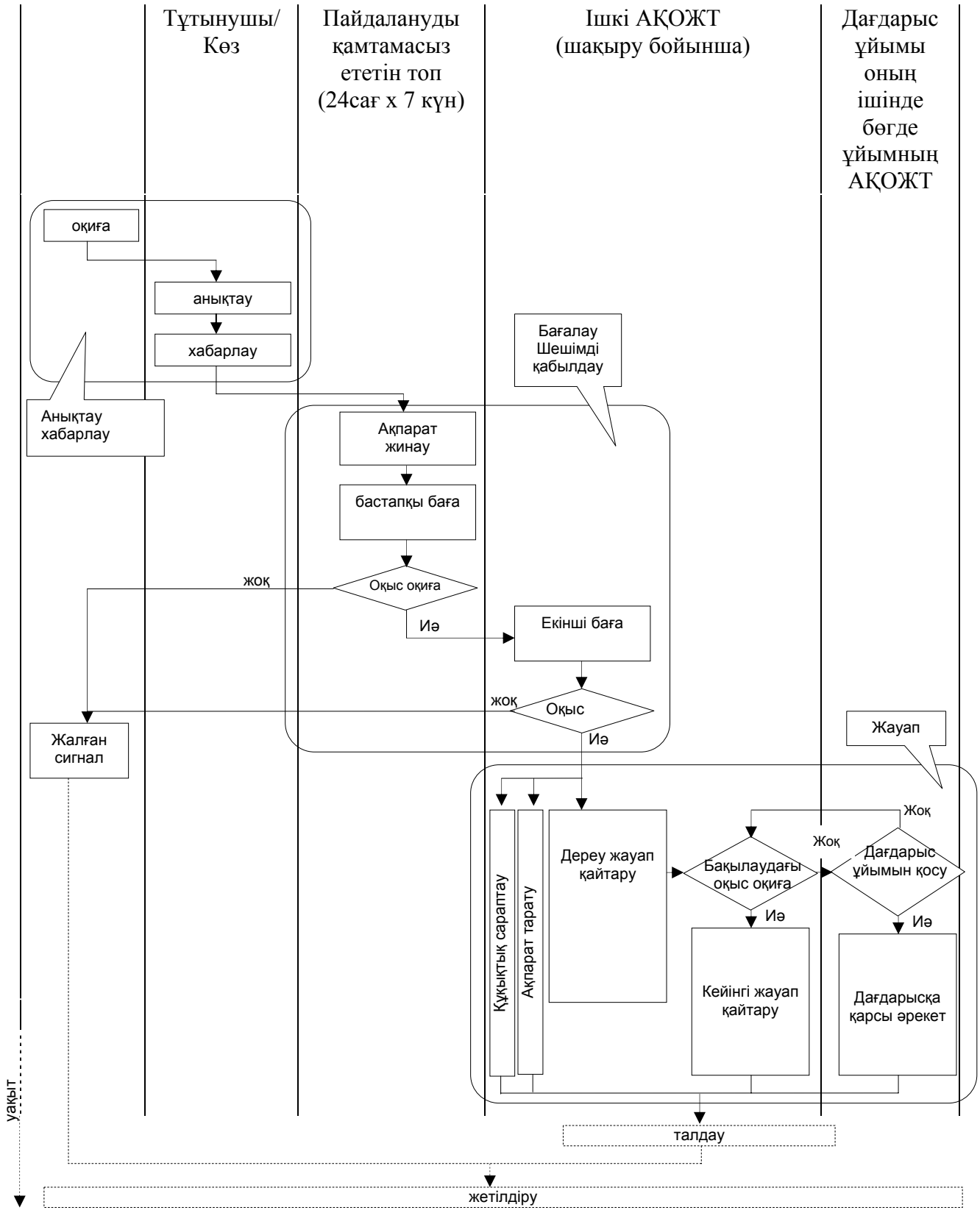
д) талап бойынша барлық кезең ішінде жүргізілетін шешімдерді одан әрі бағалау және (немесе) қабылдау әрекетінің аясын кеңейту;

е) барлық қатысты адамдары, әсіресе АҚОЖТ мүшелері одан әрі талдау үшін барлық іс-әрекетті тиісті тіркеуді қамтамасыз етуі;

ж) сот қудалауы немесе ұйым ішінде тәртіптік талқылау үшін оларды қажет ету жағдайларына осы куәліктерді қорғаныш сақтаудың тұрақты мониторингін және электронды түрде куәліктерді қорғаныш сақтауды және жинауды қамтамасыз ету;

и) АҚ-нің оқыс оқиғаларын бақылауды, АҚ-нің оқиғалар/оқыс оқиғалар деректерінің базасы тұрақты түрде іс-әрекетке сәйкес келуі үшін оқыс оқиғалар бойынша есеп беруді жаңартуды қоса алғанда өзгерістерді бақылаудың режімін қолдаудың процедураларын қолдауы болып табылады.

АҚ-нің оқиғаларына немесе оқыс оқиғаларына қатысты жиналған барлық ақпарат ГРИБ-пен басқарылатын АҚ-нің оқиғаларының/оқыс оқиғаларының деректер базасында сақталуға тиіс. Әрбір процесс сайын хабарланатын ақпарат шешімдерді бағалау және қабылдау үшін, сондай-ақ қабылданатын іс-әрекет үшін неғұрлым төзімді негізді қамтамасыз ететіндей кез келген уақытта неғұрлым толық болуға тиіс.



2-сурет – АҚ-нің оқиғаларын және оқыс оқиғаларын өңдеу операцияларының салдарларының блок-схемасы («Пайдалану» кезеңі)

АҚ-нің оқиғасын анықтағаннан және ол туралы хабарлағаннан кейін кейінгі процестердің мақсаттары мыналар болып табылады:

а) шешімдерді бағалаумен және қабылдаумен қатар қызметкерлердің тиісті лауазымдық сатысы арқылы оқыс оқиғалар менеджментімен байланысты қызметке, сондай-ақ қауіпсіздікті қамтамасыз етумен байланысты да, байланысты емес те қызметкерлерді қатыстыра отырып, іс-әрекетке жауапкершілікті бөлу;

б) жасалған хабарламаны талдауды және түзетуді, шығынды бағалауды және тиісті қызметкерлерді хабардар етуді қоса алғанда, әрбір хабарланған адамның формальды процедураларын (әрбір адамның іс-әрекеті оқыс оқиғаның типіне және қауіптілігіне байланысты) қамтамасыз ету;

в) АҚ-нің оқиғаларын мұқият құжаттау үшін, ал кейіннен, егер оқиға АҚ-нің оқыс оқиғасына жататын болса, онда АҚ-нің оқыс оқиғасына қатысты одан әрі әрекет ету үшін ұсынымдарды пайдалану және АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасын жаңарту.

Мыналар бойынша:

а) АҚ-нің оқиғалары туралы анықтау және хабарлау – 8.3 бөлімінде, шешімдерді бағалау және қабылдау (АҚ-нің оқыс оқиғасы болып саналады ма) – 8.4 бөлімінде, АҚ-нің оқыс оқиғасына жауап қайтару – 8.5 бөлімінде ұсынымдар келтірілген және мыналарды қамтиды:

- тез арада жауап қайтару,
- АҚ-нің оқыс оқиғасы бақылауға алынғанын анықтау мақсатында талдау,
- кейінгі жауап қайтарулар,
- дағдарысқа қарсы іс-әрекеттер,
- құқықтық сараптау,
- ақпарат беру,
- АҚ-нің оқыс оқиғалары менеджменті саласын кеңейту мәселелері бойынша түсініктер беру,
- іс-әрекетті тіркеу.

8.3 Ақпараттық қауіпсіздік оқиғалары туралы анықтау және хабарлау

АҚ-нің оқиғасы тікелей адамның алаңдатушылық тудыратын және техникалық, физикалық немесе процедуралық сипатқа ие қандай да бір нәрсені байқаған адамдардың анықтауы болуы мүмкін. Анықтау, мысалы, от/түтін детекторымен немесе бұрын анықталған орынға дабыл сигналдарын беру арқылы күзет сигнализациясының көмегімен жүзеге асырыла алады (белгілі бір іс-әрекеттегі адам жүзеге асыруы үшін). АҚ-нің техникалық оқиғасы автоматты түрде анықталуы мүмкін, мысалы, бұл аудит жазбасын талдау құрылғыларынан, желіаралық экрандардан, рұқсатсыз басып кіруді анықтау жүйелерінен, вирусқа қарсы бағдарламалардан, әр жағдайда осы құрылғылардың алдын ала орнатылған параметрлерінен болатын дабыл сигналы болуы мүмкін.

АҚ-нің оқиғасын анықтау себебіне қарамастан қандай да бір қалыпты емес жағдайға тікелей көңіл аударған немесе автоматты құралмен хабарланған адам анықтау және хабарлау процесіне бастама жасауға жауапты.

Бұл адам ұйымның тұрақты немесе шарт бойынша жұмыс істеп жүрген кез келген қызметкерлері бола алады.

Бұл өкіл бәрінен бұрын пайдалануды қамтамасыз ету тобының және менеджменттің көңілін аудару мақсатында АҚ-нің оқыс оқиғалары менеджментінің жүйесімен анықталған АҚ-нің оқиғасы туралы есеп беру нысанын пайдалануы және процедураларды бақылауға тиіс. Сонымен қатар, барлық қызметкерлер есеп беру нысанын қоса алғанда, АҚ-нің мүмкін оқиғалары туралы хабарлау мәселесіне қатысты ұсынымдармен танысуы, оларға рұқсаты болуы және АҚ-нің оқиғаларының әрбір жағдайы туралы хабарлау қажет

қызметкерлерді білуі маңызды. Барлық қызметкерлер АҚ-нің оқыс оқиғалары менеджментінің жүйесін түсінуге мүмкіндік беретін есеп беру нысаны туралы хабардар болуы қажет.

АҚ-нің нақты оқиғасын өңдеу оның нені білдіретініне, сондай-ақ осы оқиғадан туындайтын салдарлар мен іс-әрекеттерге байланысты. Оқиғаны өңдеу тәсілі туралы шешім қабылдау көптеген адамдар үшін олардың құзыретінің шегінен шығады. Сондықтан, АҚ-нің оқиғасы туралы хабарланған қызметкер оған сол сәтте қолжетімді мүмкіндігінше көп ақпарат болатындай есеп беру нысанын толтыруға тиіс. Қажет болғанда ол өзінің басшылығымен байланысады. Мүмкіндігінше бұл нысан электронды түрде болғаны дұрыс, себебі оны пайдалануды қамтамасыз етудің тиісті тобына (мүмкіндігінше аптасына жеті күн тәулігіне 24 сағат жұмыс істейтін), ал хабарлама көшірмесін АҚОЖТ-ның басшысына қауіпсіз беруге болады. АҚ-нің оқиғасы туралы хабарламаның есеп беру нысанының үлгісі А қосымшасында берілген.

Есеп беру нысанын толтыру кезінде мазмұнының нақтылығы ғана емес, сонымен қатар уақтылы толтырылуы маңызды екендігін ескеру қажет. Мазмұнын нақтылау себебіне байланысты АҚ-нің оқиғасы туралы есеп беру нысанын ұсынуды кешіктірмеу қажет. Егер хабарлайтын қызметкер деректерде есеп беру нысанындағы қандай да бір сызыққа сенімді болмаса, онда ол сызыққа белгі қойылуы, ақысы кейіннен жіберілуге тиіс. Сондай-ақ кейбір электронды хабарлау механизмдерінің өзі (мысалы, электронды пошта) рұқсатсыз кірудің мақсаты болып табылатынын мойындау керек.

Проблемалар болған жағдайда және санкцияланбаған адамдар есеп беру нысанын оқу және жүйеге рұқсатсыз кіру жағдайларын қоса алғанда, электронды хабарлау механизмдерімен өкілеттілік бойынша белгіленген проблемалардың болғаны туралы пікірді жүзеге асыру кезінде байланыстың балама құралдары пайдаланылуға тиіс. Байланыстың балама құралдары қолма-қол беру, телефон, мәтін хабарламасы бола алады. Осындай балама құралдар АҚ-нің оқиғасы АҚ-нің оқыс оқиғасы санатына ауысатын, әсіресе АҚ-нің осындай оқыс оқиғасы маңызды болып есептелуі мүмкін зерттеудің бастапқы сатысында пайдаланылуға тиіс.

Пайдалануды қамтамасыз ету тобының көп жағдайлары оны одан әрі өңдеу мақсатында АҚ-нің оқиғасы туралы хабарлауға тиіс, АҚ-нің оқиғасы жергілікті басшылықтың көмегімен орында өңделуі мүмкін жағдайлар болуы мүмкіндігін ескеру керек. АҚ-нің оқиғасын жалған дабыл ретінде дереу тануға немесе ұтымды рұқсат етуге болады. Бұл жағдайларда АҚ-нің оқиғасы-оқыс оқиғаларының деректер базасында оны тіркеу мақсатында жергілікті басшыға, пайдалануды қамтамасыз ету тобына, сондай-ақ және АҚОЖТ-нда есеп беру нысанын толтыру және жіберу қажет. Бұл жағдайда АҚ-нің оқиғасының жабылуы туралы хабарлаушы адам АҚ-нің оқыс оқиғалары туралы есеп беру нысанын толтыру үшін қажет етілетін ақпаратты беруі мүмкін. Бұл жағдайда АҚ-нің оқыс оқиғалары туралы есеп беру нысаны толтырылуға және инстанциясы бойынша жіберілуге тиіс.

8.4 Оқиғалар/оқыс оқиғалар бойынша шешімдерді бағалау және қабылдау

8.4.1 Бастапқы баға және алдын ала шешім

АҚ-нің оқыс оқиғалары менеджментінің жүйесін пайдалануды қамтамасыз ету тобында қабылдаушы адам толтырылған есеп беру нысанын алғанын растауға, оны АҚ-нің оқиғалары/оқыс оқиғалары деректерінің базасына енгізуге, есеп берудің осы нысанына талдау жасауға тиіс. Бұдан әрі лауазымды тұлға АҚ-нің оқиғалары туралы кез келген нақтылауды алуға және оқиға туралы хабарлаған адамның да, кез келген басқа көздің де қолжетімдігі саналатын, қажет етілетін қосымша ақпаратты жинауға ниет етуге тиіс. Содан кейін пайдалануды қамтамасыз ету тобының өкілі осы оқиға АҚ-нің оқыс оқиғасы санатына сәйкес келетінін, сәйкес келмейтінін немесе жалған болып табылатынын

анықтау үшін бағалау жүргізуге тиіс. Егер АҚ-нің оқиғасы жалған деп анықталса, есеп беру нысанын толтыруы және деректер базасындағы жазбалар және одан әрі талдау үшін АҚОЖТ-на беруі, сондай-ақ оқиға туралы хабарлаған адам және оның жергілікті басшысы үшін көшірме жасауға тиіс.

Осы кезеңде жиналған ақпарат және басқа да куәліктер тәртіптік немесе сот талқылауы үшін кейіннен қажет болуы мүмкін. Ақпаратты жинау және бағалау тапсырмасын орындаушы адам немесе адамдар куәліктерді жинау және сақтау бойынша талаптарды білуге тиіс.

Іс-әрекетті орындау күніне (күндеріне) және уақытқа қосымша мынадай толық құжаттау қажет:

- іс-шаралар өткізу (пайдаланылған құралдарды қоса алғанда) және олардың мақсаттары;
- оқиғалардың болуы куәліктерін сақтау орны;
- куәліктерді мұрағаттау әдісі (егер ол мүмкін болса);
- куәліктерді верификациялау әдісі (егер ол мүмкін болса);
- материалдарды сақтау бөліктері және оларға одан әрі қолжетімділік.

Егер АҚ-нің оқиғасы АҚ-нің мүмкін оқыс оқиғасы ретінде анықталса, ал пайдалануды қамтамасыз ету тобының қызметкері құзырлықтың тиісті деңгейіне ие болса, онда одан әрі бағалау жүргізіледі. Нәтижесінде түзету әрекеті қажет етілуі мүмкін, мысалы, қосымша «апаттық» қорғау шараларын сәйкестендіру және оларды іске асыруда тиісті адамнан көмек сұрау. АҚ-нің оқиғасы АҚ-нің оқыс оқиғасы ретінде анықталуы мүмкін (ұйымда қабылданған маңыздылық шкаласы бойынша), бұл жағдайда АҚОЖТ-ның басшысын тікелей хабардар ету қажет. АҚОЖТ-ның басшысын және жоғары басшыны бір мезетте хабардар етумен қатар ұйым қызметінің үздіксіздігін қамтамасыз ету басшысын хабарлау ретінде «дағдарыс жағдайын» хабарлау қажет етілуі мүмкін.

Бірақ тиісті іс-әрекеттерді одан әрі бағалау және орындау үшін АҚОЖТ-нда тікелей АҚ-нің оқыс оқиғасын беру жағдайы неғұрлым шындыққа жанасады.

Келесі қадам қандай болса да пайдалануды қамтамасыз ету тобының қызметкері мүмкіндігіне қарай есеп беру нысанын неғұрлым егжей-тегжейлі толтыруға тиіс. АҚ-нің оқыс оқиғасы бойынша есеп беру нысанының үлгісі А қосымшасында келтірілген. Есеп беру сипаттау түріндегі ақпаратты және мыналарды қаншалықты сипаттау мүмкіндігін қамтуға тиіс:

- АҚ-нің оқиғасы нені білдіретінін;
- оның себебі неде, оны кім жасағанын;
- ол неге әсер ететінін және әсер етуі мүмкіндігін;
- ұйымның қызметіне АҚ-нің оқыс оқиғасының шынайы немесе әлеуетті әсерін;
- АҚ-нің оқыс оқиғасының мүмкін маңыздылығын немесе маңызды еместігін көрсетуді (ұйым қабылдаған маңыздылық шкаласы бойынша);
- АҚ-нің оқыс оқиғасы осы уақытқа дейін қалай өңделгенін.

Ақпаратты санкцияланбаған ашу, ақпаратты санкцияланбаған түрлендіру, бар ақпараттан бас тарту, ақпаратқа және (немесе) сервиске қолжетімдіктің болмауы, ақпаратты және (немесе) сервисті жою нәтижесінде оқыс оқиғаның ұйым қызметіне әлеуетті немесе нақты жағымсыз әсерін қарау кезінде бірінші кезекте төменде санамаланған салдардың қайсысы АҚ-нің оқыс оқиғасы болатынын анықтау қажет. АҚ-нің салдардарының мысалдары мыналар болып табылады:

- операциялардың шығынын/үзілуін қаржыландыру;
- коммерциялық және экономикалық мүдделердің шығыны;
- дербес деректерден тұратын ақпараттың шығыны;
- құқықтық және нормативтік міндеттердің бұзылуы;
- менеджмент және басқа да операциялар бойынша жұмыс істемеу;

- ұйымның беделінің болмауы.

АҚ-нің оқыс оқиғасы санатына жататын санаттар үшін оларды АҚ-нің оқыс оқиғалары бойынша есеп беруге енгізу үшін әлеуетті немесе нақты әсерлерді санаттау бойынша тиісті ұсынымдар пайдаланылуға тиіс. Ұсынымдар мысалы В қосымшасында келтірілген.

Егер АҚ-нің оқыс оқиғасы рұқсат етілген болса, онда есеп беру қабылданған қорғау шараларының нақты деректерін және алынған сабақтарды қамтуға тиіс (мысалы, АҚ-нің осыған ұқсас оқыс оқиғаларының қайта туындауының алдын алу үшін қабылдануы тиіс қорғау шаралары).

Мүмкіндігінше неғұрлым егжей-тегжейлі есеп беру нысанын толтырғаннан кейін АҚ-нің оқыс оқиғаларының және оқиғаларының деректер базасына енгізу және кейіннен талдау үшін АҚОЖТ-на ұсынылуға тиіс.

Егер тексеру аптадан артық жүргізілсе, онда аралық есеп беру жасалуға тиіс.

АҚ-нің оқыс оқиғалары менеджментінің жүйесі құжатындағы нұсқауды негізге ала отырып, АҚ-нің оқыс оқиғасын бағалаған пайдалануды қамтамасыз ету тобының қызметкері:

- оқыс оқиға туралы материалды қашан және кімге жіберу;
- пайдалануды қамтамасыз ету тобы орындайтын барлық іс-әрекеттерді жүзеге асыру кезінде өзгерістерді бақылаудың құжатталған процедураларын орындау қажеттігі туралы хабарлануға тиіс.

Ақпараттық жүйеге рұқсатсыз кіруді және АҚ-нің оқыс оқиғалары туралы есеп беру нысанын санкцияланбаған адамдардың есептеуін қоса алғанда, электронды хабарлау (мысалы, электронды пошта) механизмінің іске қосылмауы бойынша белгіленген проблемалары бар екендігі туралы проблемалар немесе пікірлер болған кезде байланыстың балама құралы пайдаланылуға тиіс. Балама байланыс мыналар болуы мүмкін: телефон, мәтін хабарлама, сондай-ақ курьер. Сондай-ақ балама құралдар АҚ-нің оқиғасы шынайы болғанда АҚ-нің оқыс оқиғасы санатына, әсіресе «маңызды» саналуы мүмкін АҚ-нің осындай оқыс оқиғасына ауыстырылатын зерттеудің бастапқы кездегі сатыларында пайдаланылуға тиіс.

8.4.2 Ақпараттық қауіпсіздік оқыс оқиғасын қайта бағалау және растау

Ақпараттық қауіпсіздіктің оқыс оқиғасын қайта бағалау және растау немесе АҚ-нің оқиғасын АҚ-нің оқыс оқиғасына жатқызуға болатын не болмайтынына қандай да бір басқа шешім АҚОЖТ-ның міндетіне енуге тиіс. АҚОЖТ-ның есеп беруді қабылданатын қызметкері:

а) пайдалануды қамтамасыз ету тобы мүмкіндігінше неғұрлым егжей-тегжейлі толтырған есеп беру нысанын алғанын растауы;

б)осы нысанды АҚ-нің оқиғасының/оқыс оқиғасының деректер базасына енгізуі;

в) пайдалануды қамтамасыз ету тобына нақтылауға көңіл аударуы;

г) есеп беру нысанының мазмұнына талдау жасауы;

д) пайдалануды қамтамасыз ету тобынан, есеп беру нысанын толтырған адамнан немесе қандай да бір басқа да көздерден АҚ-нің оқиғасы (егер бар болса) туралы қосымша қажетті ақпаратты жинауға тиіс.

Егер АҚ-нің оқыс оқиғасының барабарлығына немесе алынған ақпараттың толықтығына қатысты қандай да бір белгісіздік әлі де бар болса, онда АҚОЖТ-ның қызметкері АҚ-нің оқыс оқиғасының шынайылығын немесе жалғандығын анықтау үшін қайта бағалау жүргізуге тиіс. Егер АҚ-нің оқыс оқиғасы «жалған» ретінде анықталса, АҚ-нің оқиғасы туралы есепті толтыру, оны АҚ-нің оқиғалары/оқыс оқиғалары деректерінің базасына қосу және АҚОЖТ-ның басшысына беру қажет. Есеп беру көшірмелері

пайдалануды қамтамасыз ету тобына, оқиға туралы хабарлаған адамға және оның жергілікті басшысына беру қажет.

Егер АҚ-нің оқыс оқиғасы «шынайы» ретінде анықталса, онда АҚОЖТ-ның қызметкері қажет болғанда әріптестерді қатыстыра отырып, одан әр бағалау жүргізуге тиіс. Бағалау мақсаты:

а) АҚ-нің оқыс оқиғасы нені білдіретінін, оның себебі не болғанын, оны кім немесе не жасағанын, неге әсер етті немесе әсер етуі мүмкін, АҚ-нің оқыс оқиғасының ұйым қызметіне әсерін немесе әлеуетті әсерін, оқыс оқиғаның мүмкін маңыздығын/маңызды еместігін көрсетуді (ұйымда қабылданған оқыс оқиғалардың маңыздылығы шкаласы бойынша);

б) кейбір ақпараттық жүйеге, сервиске және (немесе) желіге бұзушының алдын ала ойлаған техникалық рұқсатсыз кірулерін, мысалы:

1) жүйеге, сервиске және (немесе) желіге бұзушының кіру ауқымын және оның білетін бақылау деңгейін;

2) бұзушы қолжетімдік алған ақпарат көшірмеленгені, өзгергені немесе жойылғаны туралы деректерді;

3) қандай бағдарламалық қамтамасыз ету көшірмелерді, өзгерді немесе бұзушы бұзғаны туралы,

4) бұзушының аппараттық бөлімнің, сервистің және (немесе) желінің кез келген ақпараттық жүйесіне және (немесе) физикалық орналасқан жеріне алдын ала ойластырған жеке рұқсатсыз кірулеріне қатысты, мысалы:

- келтірілген физикалық шығындардың (қолжетімдіктің физикалық қорғанышы болмаған жағдайда) тікелей және жанама салдарларының масштабы,

- бұзушының жанама іс-әрекетімен жасалған АҚ-нің оқыс оқиғаларына қатысты тікелей және жанама салдарлар (мысалы, физикалық қолжетімдік өрттің себебінен болды ма, ақпараттық жүйенің осалдығы бағдарламалық қамтамасыз етудің, байланыс желісінің дұрыс жұмыс істеуінен немесе оператордың қателігінен болды ма),

в) АҚ-нің оқыс оқиғасын өңдеудің осы уақытқа дейін пайдаланылатын тәсілін барынша дереу растау болып табылады.

Ақпаратты санкцияланбаған ашу, ақпаратты санкцияланбаған түрлендіру, бар ақпараттан бас тарту, ақпаратқа және (немесе) сервиске қолжетімдіктің болмауы, ақпаратты және (немесе) сервисті жою нәтижесінде оқыс оқиғаның ұйым қызметіне әлеуетті немесе шынайы жағымсыз әсерін талдау кезінде осы оқыс оқиға нәтижесінде қандай салдарлар болғанын растау қажет.

АҚ-нің салдардарының мысалдары мыналар болып табылады:

- операциялардың шығынын/үзілуін қаржыландыру;
- коммерциялық және экономикалық мүдделердің шығыны;
- дербес деректерден тұратын ақпараттың шығыны;
- құқықтық және нормативтік міндеттердің бұзылуы;
- менеджмент және басқа да операциялар бойынша жұмыс істемеу;
- ұйымның беделінің болмауы.

Сол және басқа да санаттарға әлеуетті немесе нақты әсерлерді жатқызу үшін АҚ-нің оқыс оқиғасы санатына жататын АҚ-нің оқыс оқиғалары бойынша есеп беруге енгізілетін тиісті ұсынымдарды пайдалану қажет. Ұсынымдар үлгісі Б қосымшасында берілген.

8.5 Оқыс оқиғаларға жауап қайтару

8.5.1 Тез арада жауап қайтару

8.5.1.1Шолу

Оқыс оқиғаларды растағаннан кейін көп жағдайда АҚОЖТ-ның мүшесі АҚ-нің оқыс оқиғасына қатысты тез арада жауап қайтару бойынша іс-әрекетті, АҚ-нің оқыс оқиғасы

туралы есеп беру нысанындағы нақты деректерді тіркеуді, АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына енгізуді және АҚ-нің оқыс оқиғасына қажет етілетін іс-әрекеттер туралы ұйым қызметкерлеріне хабарлауды орындайды. Осы іс-әрекеттердің нәтижесі апаттық қорғау шараларын қабылдау (мысалы, АТ-бөлімшесінің тиісті басшысының және (немесе) жоғары басшының алдын ала келісімі бойынша рұқсатсыз кірген жүйені және (немесе) желіні ажырату және (немесе) қосымша тұрақты қорғаныш шараларын анықтау және осы шараларды қабылдау туралы ұйым қызметкерлеріне хабарлау мүмкін. Егер апаттық қорғаныш шаралар қабылданбаған болса, онда ұйымда қабылданған бағалау шкаласы бойынша АҚ-нің оқыс оқиғасының маңыздылығын анықтау қажет және егер АҚ-нің оқыс оқиғасы жеткілікті «маңызды» болса, онда ол туралы тиісті жоғары басшыға тікелей хабарлау қажет. Егер «дағдарыс жағдайын» хабарлау қажет болса, ұйым қызметінің үздіксіздігін қамтамасыз етуге жауапты басшы ұйым қызметінің үздіксіздігін қамтамасыз ету жоспарын белсендіру мүмкіндігі турлы хабарлануы, және АҚОЖТ-ның басшысына және жоғары басшыға хабарлауы қажет.

8.5.1.2 Жауап қайтару бойынша үлгілік іс-әрекеттер

Ақпараттық жүйеге, сервиске және (немесе) желіге алдын ала ойластырылған рұқсатсыз кірулер жағдайында дереу жауап қайтару бойынша іс-әрекеттердің мысалы мынадай:

- сындарлы маңызды қосымшалардың дұрыс жұмыс істеуін қамтамасыз ету;
- егер бұзушы бақылауда екендігін білмеген жағдайда, ол туралы неғұрлым толық ақпарат жинау мақсаттарда Интернетке және бақа да желіге қосулы күйде қалуы мүмкін.

Бірақ жауап қайтару бойынша шешім қабылдау кезінде мынадай факторларды есепке алу қажет:

- бұзушы бақылауға алынғанын сезуі және рұқсатсыз кірген жүйеге, сервиске және (немесе) желіге және дерекке одан әрі шығын келтіретін әрекеттерді қабылдауы мүмкін;
- бұзушы өзін байқататын ақпаратты бұзуы мүмкін.

Тиісті шешім қабылдау кезінде рұқсатсыз кірген жүйені, сервисті және (немесе) желіні дереу және сенімді ажыратуға техникалық мүмкіндік болуы маңызды. Бірақ осыған құқығы жоқ осындай ажыратуларды болдырмау үшін қызметкерлер түпнұсқаландырудың иісті құралдарын қолдануы қажет.

Оқыс оқиғаның қайта туындауын болдырмау әдетте неғұрлым басымды міндет болып табылады. Кейбір жағдайларда бұзушы жоюлуы керек әлсіз орынды анықтағанын, ал бұзушының анықтағыны оның жұмсаған күшін ақтамайтынын есепке алу қажет. Бұл, егер бұзушы негізінен қасқүнем болып саналмаса және шығын келтірмеген болса, әділетті болады.

Алдын ала ойластырылған рұқсатсыз кірулерден басқа АҚ-нің басқа да оқыс оқиғаларына қатысты айтатын болсақ, онда олардың көздері сәйкестендірілуге тиіс. Қорғау шараларын енгізу уақытында АТ-ның тиісті басшысының және (немесе) жоғары басшының алдына ала келісімін алғаннан кейін олардың тиісті бөліктерін оқшаулау немесе ақпараттық жүйені, сервисті және (немесе) желіні ажырату талап етілуі мүмкін. Ол үшін егер осалдық орын ақпараттық жүйе, сервис үшін және (немесе) желі үшін маңызды немесе сындарлы маңызды болса, көп уақыт қажет етілуі мүмкін.

Жауап қайтару бойынша басқа да іс-әрекет бақылау әдісімен белсендірілуі мүмкін [4]. Бұл әрекет АҚ-нің оқыс оқиғалары менеджментінің жүйесі үшін құжатталған процедуралар негізінде жүзеге асырылуға тиіс.

АҚ-нің оқыс оқиғасы нәтижесінде зақымдануы мүмкін ақпарат ақпараттың өзгеруіне, өшірілуіне немесе түрленуіне резервтік жазбалар бойынша АҚОЖТ-ның мүшесі тексеруге тиіс. Қасқүнем бұзушы рұқсатсыз кіру ізін жасыру мақсатында қолдан жасауы мүмкін тіркеу журналдарының тұтастығын тексеру қажеттігі туындауы мүмкін.

8.5.1.3 Оқыс оқиғалар туралы ақпаратты жаңарту

Кейінгі іс-әрекеттеріне қарамастан АҚОЖТ-ның қызметкері барынша көп егжей-тегжейлеу арқылы АҚ-нің оқыс оқиғасы туралы есеп беруді жаңартуы, оны АҚОЖТ-ның басшысына және басқа да адамдарға (қажет болғанда) осы туралы хабарлай отырып, АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына қосуға тиіс.

Мынадай:

- АҚ-нің оқиғасы нені білдіретіні;
- оның себебі неде, оны кім жасағаны;
- ол неге әсер етеді және әсер етуі мүмкіндігі;
- ұйымның қызметіне АҚ-нің оқыс оқиғасының шынайы немесе әлеуетті әсері;
- АҚ-нің оқыс оқиғасының мүмкін маңыздылығын немесе маңызды еместігін көрсетудегі өзгерістері (ұйым қабылдаған маңыздылық шкаласы бойынша);
- АҚ-нің оқыс оқиғасы осы уақытқа дейін қалай өңделгені туралы ақпаратты жаңартады.

Егер АҚ-нің оқыс оқиғасы рұқсат етілген болса, онда есеп беру қабылданған қорғау шараларының нақты деректерін және алынған сабақтарды қамтуға тиіс (мысалы, АҚ-нің осыған ұқсас оқыс оқиғаларының қайта туындауының алдын алу үшін қабылдануға тиіс қорғау шаралары).

Жаңартылған есеп беруді АҚ-нің оқыс оқиғалары және оқиғалары деректерінің базасына енгізу және олардың талабы бойынша АҚОЖТ-ның басшысына және басқа да адамдарға хабарлау қажет.

АҚОЖТ-ы одан әрі сараптау жүргізу және айғақ ретінде сотта пайдалану мүмкіндігіне қатысты ақпаратты қауіпсіз сақтауды қамтамасыз етуге жауапты. Мысалы, АТ-на бағытталған АҚ-нің оқыс оқиғасы үшін АҚ-нің оқыс оқиғасын бастапқы анықтағаннан кейін барлық тұрақсыз деректер сот талқылауы жүргізілгенге дейін АТ-ның өрт жүйесі, сервис және (немесе) желі ажыратылғанға дейін жиналуға тиіс. Ақпарат жинауға арналғаны кез келген жұмыс істеп тұрған процесс туралы мәліметті қамтиды және жадыда, кэште және тіркеуде сақталады. Бұл ретте:

- АҚ-нің оқыс оқиғасының сипатына байланысты сот талқылауы жағдайына өрт жүйесін, сервисті және (немесе) желіні толық көшіріп қайталауды немесе журналдарды және маңызды файлдарды резервтік көшірмелеуді жүргізуі;
- көрші жүйелердің, сервистердің және (немесе) желілердің журналдарын жинау және талдау жасау, мысалы, маршрутизаторлар мен желіаралық экранды;
- барлық жиналған ақпаратты тасымалдағышта тек оқуға ғана сақтау;
- сот талқылауы жағдайына көшіріп қайталауды орындау кезінде барлық іс-әрекеттер қолданыстағы нормативтік заңнамаға сәйкес орындалғанын бекіту және растау үшін кемінде екі адамның қатысуын қамтамасыз ету;
- сот талқылауы жағдайына қайталау үшін пайдаланылатын сервистік командаларды сипаттаумен және спецификацияның шығыс тасымалдағыштарымен бірге көшіріп қайталау және сақтау қажет.

АҚОЖТ-ның мүшесі, егер ол мүмкін болса, АҚ-нің оқыс оқиғалары туралы ақпаратты жаңарту кезінде өрт құрылғыларына рұқсатсыз кіруді болдырмау мүдделігіндегі осы құрылғылардың (АТ-на қатысы бар және қатысы жоқ) қауіпсіз жұмыс жағдайына жауапты болып табылады.

8.5.1.4 Қосымша әрекет

АҚОЖТ-ның мүшесі АҚ-нің оқыс оқиғасының шынайылығын анықтау кезінде оның қосымша әрекеттері:

- құқықтық сараптауды жүргізу;

- қандай нысанда және кімге ақпарат беру бойынша дәлелдер және ұсыныстар туралы ақпаратты ұйым ішінде және одан тыс беруге жауапты адамға хабарлауға тиіс.

АҚ-нің оқыс оқиғалары туралы есеп беруді мүмкіндігінше егжей-тегжейлі толтыру мүмкіндігінен кейін есеп беру АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына енгізіледі және АҚОЖТ-ның басшысына беріледі.

Егер тексеру ұйым ішінде бұрын келісілген уақыттан асып кетсе, онда аралық есеп беру құрылады.

АҚ-нің оқыс оқиғалары менеджментінің жүйесі құжатындағы нұсқауды негізге ала отырып, АҚ-нің оқыс оқиғасын бағалаған АҚОЖТ-ның мүшесі:

- оқыс оқиға туралы материалды қашан және кімге жіберу;
- АҚОЖТ-ның кез келген қызметін жүзеге асыру кезінде өзгерістерді бақылаудың құжатталған процедураларын басшылыққа алуды білуге тиіс.

Жүйеге рұқсатсыз кіру жағдайы болуы мүмкін жағдайларды қоса алған қарапайым байланыс құралдарына қатысты (мысалы, электронды пошта) проблемалар бар болғанда немесе бар деп саналғанда, АҚ-нің оқыс оқиғасы деп қорытынды жасалса, онда бірінші кезекте АҚ-нің оқыс оқиғасы туралы жауапты адамға жеке, телефонмен немесе мәтін хабарламамен хабарлауы қажет.

Қажет болғанда АҚОЖТ-ның басшысы ұйымның АҚ-нің қауіпсіздігін қамтамасыз ету басшысымен және басқару ұйымының тиісті басшысымен (директорлар кеңесінің мүшесі) бірлесіп ұйымның ішінде де одан тыс ретінде АҚ-нің оқыс оқиғаларына қатыстырылған барлық бөлімдермен байланысуға тиіс (7.5.3 және 7.5.4 бөлімдерін қараңыз).

Байланысты жылдам және тиімді ұйымдастыру үшін АҚ-нің оқыс оқиғасы әсер етуі мүмкін жүйеден, сервистен немесе желіден толық қатысы жоқ ақпаратты берудің сенімді әдісін алдын ала белгілеуі қажет. Мұндай алдын алу шаралар негізгі басшылардың қайсы бірі болмаған жағдайға ұйымның өкілдерін немесе резервтік кеңесшілерді тағайындауды қамтиды.

8.5.2 Оқыс оқиғаның бақылануы

Тиісті құқықтық сараптау арқылы дереу жауап қайтаруды және ақпаратты беру бойынша іс-әрекетті АҚОЖТ-ның мүшесі бастамалық жасағаннан кейін АҚ-нің оқыс оқиғасы бақылауда екендігіне шұғыл көз жеткізу қажет. Қажет болғанда АҚОЖТ-ның мүшесі АҚОЖТ-ның әріптестерімен, басшыларымен және (немесе) ұйымның басқа да қызметкерлерімен кеңес ала алады.

Егер АҚ-нің оқыс оқиғасы бақылауда екендігі расталса, онда АҚОЖТ-ның мүшесі АҚ-нің оқыс оқиғасын жою және зақымданған ақпараттық жүйенің қалыпты жұмысын қалпына келтіру мақсатында ақпаратқа жауап қайтару, құқықтық сараптауды жүргізу және ақпарат беру бойынша басқа да одан әрі қажетті іс-әрекеттерге көшуге тиіс. (8.5.3, 8.5.5 және 8.5.6 бөлімдерін қараңыз).

Егер АҚ-нің оқыс оқиғасы бақылауда екендігі расталмаса, онда АҚОЖТ-ның мүшесі «дағдарысқа қарсы» әрекетке бастамалық етуге тиіс (8.5.4 бөлімін қараңыз).

8.5.3 Кейінгі жауап қайтарулар

АҚ-нің оқыс оқиғасы бақылауда екендігін және «дағдарысқа қарсы жағдай» объектісі болып саналмайтынын анықтап, АҚОЖТ-ның мүшесі осы оқыс оқиғаға қатысты одан әрі жауап қайтарудың қажеттігін және мүмкін тәсілдерін анықтауға тиіс. Жауап қайтару зақымданған ақпараттық жүйені (лерді), сервисті (терді) және (немесе) желіні (лерді) қалыпты жұмыс жағдайына қалпына келтіруді қамтуға тиіс. Содан кейін АҚОЖТ-ның мүшесі АҚ-нің оқыс оқиғасы туралы егжей-тегжейді есеп беру нысанына және АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына енгізуі, сондай-ақ тиісті іс-

әрекеттерді аяқтауға жауапты адамдарға ол туралы хабарлауға тиіс. Осы іс-әрекеттердің жетістікпен аяқталуының нақты деректерін АҚ-нің оқыс оқиғасы туралы есеп беру нысанына және АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына енгізу, содан кейін АҚ-нің оқыс оқиғасы жабылуы және тиісті қызметкерлер ол туралы хабардар болу керек.

Кейбір жауап қайтарулар АҚ-нің оқыс оқиғасының осыған ұқсас қайталануын болдырмау үшін жіберілуге тиіс. Мысалы, АҚ-нің оқыс оқиғасына («патчея») бағдарламасына енгізу болмағандықтан АТ-ның бағдарламалық қамтамасыз етуі немесе аппаратура бөлігі жұмыс істемеуі себеп болғаны анықталса, онда бұл жағдайда өнім берушімен дереу байланысу қажет. Егер АҚ-нің оқыс оқиғасының себебі АТ-ның белгілі осалдығы болса, онда ол АҚ-нің қорғанышын тиісті жаңарту жоюға тиіс. Сондай-ақ АҚ-нің оқыс оқиғасы анықтаған және АТ-ның конфигурациясымен байланысты кез келген проблемаларды шешу қажет. АҚ-нің осындай оқыс оқиғасының немесе оған ұқсас оқыс оқиғаның қайталану немесе туындау мүмкіндіктерін азайтудың басқа да шаралары жүйелік парольдарды өзгерту және пайдаланылмайтын сервистерді ажырату болуға тиіс.

АҚ-нің оқыс оқиғасына жауап қайтару бойынша қызметтің басқа да аясы АТ-ның жүйесінің, сервисінің және (немесе) желісінің мониторингін қамтуы мүмкін. АҚ-нің оқыс оқиғасын бағалау арқылы АҚ-нің оқыс оқиғаларының белгілері болуы мүмкін қарапайым емес немесе күдікті оқиғаларын анықтауда қоса әрекет ету үшін мониторингтің қосымша қорғау шараларын енгізу орынды болады. Мұндай мониторинг АҚ-нің оқыс оқиғасын кеңінен ашуға және беделін түсіретін АТ-ның басқа да жүйесін сәйкестендіруге көмектеседі.

АТ-мен байланысты және байланысты емес ретінде АҚ-нің оқыс оқиғаларына қолдану мүмкін бизнес-процесстің үздіксіздігін қамтамасыз етудің қолданыстағы жоспарында құжатталған арнайы жауап қайтаруларды белсендіру қажеттілігі туындауы мүмкін.

Арнайы жауап қайтарулар АТ-мен тікелей ғана емес, сонымен қатар байланыстың сөйлесу желісінің және физикалық құрылғылардың көмегі арқылы кейіннен қалпына келтіру және ұйымның түйінді функцияларын қолдаумен байланысты ұйым қызметінің барлық аспектілері үшін қарастырылуға тиіс.

Жауап қайтарудың тағы бір аясы зақымданған ақпараттық жүйені (лерді), сервисті (терді) және (немесе) желіні (лерді) қалыпты жұмыс жағдайына қалпына келтіру болып табылады. Зақымданған ақпараттық жүйені (лерді), сервисті (терді) және (немесе) желіні (лерді) қауіпсіз жұмыс жағдайына қалпына келтіру белгілі осалдар үшін «патчеяны» айтарлықтай қолданумен немесе беделіне нұсқан келтірілген элементтерді ажырату болуға тиіс. Содан кейін АҚОЖТ-ның мүшесі АҚ-нің оқыс оқиғасы туралы егжей-тегжейді есеп беру нысанына және АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына енгізуі, сондай-ақ тиісті іс-әрекеттерді аяқтауға жауапты адамдарға ол туралы хабарлауға тиіс. Осы іс-әрекеттердің жетістікпен аяқталуының нақты деректерін АҚ-нің оқыс оқиғасы туралы есеп беру нысанына және АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына енгізу, содан кейін АҚ-нің оқыс оқиғасы жабылуы және тиісті қызметкерлер ол туралы хабардар болуы керек. Егер АҚ-нің оқыс оқиғасының іс-әрекеті уақытында тіркеу журналдарын жою салдарынан АҚ-нің оқыс оқиғасы туралы ақпараттың барлық көлемі жоғалса, жүйенің, сервистің және (немесе) желінің толық қайта құрылуы талап етілуі мүмкін. Бұлар ұйым қызметі үздіксіздігінің тиісті жоспарының бір бөлігін белсендіруді талап етуі мүмкін.

Егер АТ-мен байланысты емес АҚ-нің оқыс оқиғасы, мысалы, өртпен, су алумен немесе жарылумен арандатылған болса, онда тиісті жоспарында құжатталған ұйым қызметінің үздіксіздігін қамтамасыз етуді қалпына келтіру бойынша әрекет орындалады.

8.5.4 «Дағдарысқа қарсы» әрекет

Егер АҚ-нің оқыс оқиғасы бақылауда болмаса және «дағдарысқа қарсы әрекет» режімінде өңделуге тиіс болса, онда алдын ала әзірленген жоспар (жоспарлар) пайдаланылуға тиіс.

Ақпараттық жүйенің қолжетімділігіне/бұзылуына және кей деңгейде тұтастығына әсер етуі мүмкін АҚ-нің оқыс оқиғаларының барлық мүмкін типтерін өңдеудің жақсы нұсқалары ұйым қызметінің үздіксіздігін қамтамасыз ету стратегиясында анықталуға тиіс.

Бұл нұсқалар ұйым қызметінің басымдықтарымен және бизнес-процестерді қалпына келтірудің қолданыстағы уақытша рамкаларымен және АТ-ның, қызметкерлердің және орналастырудың барынша қолжетімді уақытымен, сөйлесу байланысымен тікелей байланысты болуға тиіс. Жоспарда:

- ұйым қызметінің үздіксіздігін қамтамасыз етудің ескерту, растау шараларын және сыртқы өзгерістерге төзімділігін;
- ұйым қызметінің үздіксіздігін қамтамасыз ету жоспарының (жоспарларының) құрылымын және негізгі ережесін анықтауы қажет.

Ұйым қызметінің үздіксіздігін қамтамасыз ету жоспары (жоспарлар) және қанағаттанарлық деп танылған және тесттелген осы жоспарды (жоспарларды) белсендіруді қолдауға арналған қорғаныш шаралары олардың арналған неғұрлым көп «дағдарысқа қарсы» әрекеттерін енгізу үшін негіз болуға тиіс.

Мүмкін «Дағдарысқа қарсы» басқа да типтер мыналарды:

- өрт сөндіру құралдарын және көшіру процедураларын;
- су басуды болдырмау құралдарын және көшіру процедураларын;
- бомба жарылысын болдырмау құралдарын және көшірудің тиісті процедураларын;
- ақпараттық жүйедегі алдамшы фактілерді тексеру жөніндегі мамандардың жұмысы;
- техникалық рұқсатсыз кірулерді тексеру жөніндегі мамандардың жұмысын белсендіруді қамтиды (бірақ шектелмейді).

8.5.5 Құқықтық сараптау

Егер алдыңғы бағалау барысында АҚ-нің маңызды оқыс оқиғасының айғағы мақсатында құқықтық сараптауды, құқықтық сараптаудың қажеттілігі анықталса, АҚОЖТ-ы жүргізеді.

АҚ-нің нақты оқыс оқиғасына неғұрлым егжей-тегжейлі сараптау жүргізу мақсатында АҚ-нің оқыс оқиғалары менеджментінің бастапқы процесінде пайдаланылмайтын қолданатын құжатталған рәсімдерге және АҚ-ке негізделген құралдарды және тексеру әдістерін қолдану қажет. Мұндай сараптауды құрылымдық әдіспен жүргізеді және ішкі тәртіптік талқылаулар кезінде немесе сот процестерінің барысында айғақ ретінде пайдаланылуы мүмкін.

Құқықтық сараптау жүргізу үшін қызметтік үй-жай, сондай-ақ тиісті қызметкерлер қорғалған техникалық және бағдарламалық құралдар пайдаланылуы мүмкін (мысалы: аудит құралдары және әдістері, куәліктерді қалына келтіру құралдары). Құқықтық сараптаудың әрбір іс-әрекеті, тиісті фотосуреттерді беруді, аудит нәтижелерін талдау туралы есеп беруді құрды, деректерді қалпына келтіру журналдарын тексеруді қоса алғанда толық құжатталған болуға тиіс. Құқықтық сараптауды жүргізген адамның немесе адамдардың білігі біліктілік талаптарының нәтижелері сияқты құжатталуға тиіс. Құқықтық сараптаудың объективтілігін және логикалық сипатын көрсетуге қабілетті кез келген басқа ақпаратты да құжаттау қажет. АҚ-нің оқыс оқиғалары туралы, осы оқиғаларды құқықтық сараптаумен байланысты қызметтер туралы барлық жазбалар, және басқалар, сондай-ақ ақпаратқа тиісінше тасымалдауыштар нақты қорғалған ортада сақталуы және жазбаларды түрлендіру мақсатында оларға авторланбаған адамдардың

қолжетімдігін болдырмау үшін тиісті рәсімдермен бақылануға тиіс. АТ-ны қолдануға негізделген құқықтық сараптау құралдары сот тәртібімен осы сәйкестікпен келіспеушілік мүмкіндіктерін жою мақсатында құқықтық нормаларға дәл сай болуға тиіс, сонымен қатар оларда технологиялардағы барлық ағымдық өзгерістер ескерілуге тиіс. ГИИБ-ның физикалық ортасында куәліктерді өңдеудің дауланбайтынына кепілдік беретін қажетті шарттарды құруы қажет. АҚ-нің оқыс оқиғаларына жауап қайтаруды қамтамасыз ету үшін кез келген уақытта қызметкерлер саны жеткілікті болуға тиіс.

Уақыт өте келе, алдамшылықты, ұрлықты және вандализмнің рұқсатсыз кіруін қоса алғанда АҚ-нің оқыс оқиғаларының көп салалы контексінде куәліктердің талдауына қойылатын талаптарды әзірлеу қажеттілігі туындайды. Кейіннен АҚОЖТ-ның қоса әрекет етуі үшін АТ-ға негізделген құралдардың көп саны және бір қарағанда өшірілген, шифр қойылған немесе зақымданған болып көрінетін ақпаратты қоса алғанда ақпараттық жүйедегі, сервистегі және (немесе) желідегі жасырын ақпаратты ашу үшін қосалқы процедураларды қажет етеді. Бұл құралдар АҚ-нің оқыс оқиғаларының белгілі типтеріне байланысты барлық аспектілерді есепке алуға тиіс (олар АҚОЖТ-ның процедураларында құжатталуға тиіс).

Қазіргі заманғы жағдайда құқықтық сараптауды тексеру көптеген серверлерді (файлды сервер, баспа сервері, байланыс), сондай-ақ жойылған қолжетімдіктің құралдарын қоса алғанда барлық операциялық ортаға таратылатын желілік құрылымы бар қиын ортаға жиі қосады. Мәтінді іздеу құралдарын, бейнелеуді қалыптастыруды бағдарламалық қамтамасыз етуді және құқықтық сараптауға арналған бағдарламалар пакеттерін қоса алғанда көптеген құрал-саймандық құралдар бар. Құқықтық сараптаудың басты мақсаты қолжетімсіздіктің куәлігін сақтау, оларды соттағы кез келген келіспеушілікке қарсы тұруға тексеру және талдау жасау жұмыстарының барысында шығыс тасымалдарының тұтастығындағы күмәнді болдырмау үшін шығыс деректерінің нақты көшірмесіне құқықтық сараптау жүргізу болып табылады.

Құқықтық сараптаудың жалпы процесі қызметтің мына түрлерін:

- құқықтық сараптау жүргізу процесінде мақсатты жүйелердің, сервистердің және (немесе) желілердің қолжетімсіздігін болдырмаудан, өзгертуден немесе вирустардың кіруін қоса алғанда басқа да беделді төмендетуден қорғауды қамтамасыз етуді және олардың қалыпты жұмысына әсерінен немесе аз әсерінен қорғауды қамтамасыз етуді;
- айғақтарды жинаудың басымдықтарын белгілеуді, яғни олардың көбінен азына қарай өзгеруін қарау (маңызды деңгейде АҚ-нің оқыс оқиғасының сипатына байланысты);
- жойылған болып көрінетін, бірақ файлдар, қорғалған пароль немесе басқадай шифрланған файлдар болып табылатын қалыпты файлдарды, файлдарды қоса алғанда заттық жүйедегі, сервистегі және (немесе) желідегі барлық қажетті файлдарды сәйкестендіруді;
- өшірілген файлдардың және басқа да деректердің мүмкіндігінше көп санын қалпына келтіруді;
- IP-мекен-жайларды, хосттардың атауларын, желілік бағыттарды және Web-сайттар ақпаратын ашуды;
- операциялық жүйені бағдарламалық қамтамасыз етуді де қолданбалы бағдарламалық қамтамасыз етуді де пайдаланатын жасырын, уақытша қосымша жүктеп алу файлдардың және файлдардың ішіндегі мазмұнын алып тастауды;
- қорғалған немесе шифр қойылған файлдарды бағдарламалық қамтамасыз етудің ішіндегі мазмұнға қолжетімділікті (егер ол заңнамамен тыйым салынбаса);
- дискідегі арнайы есте сақтау аясында табылған барлық мүмкін маңызды деректерді (әдетте қолжетімсіз) талдауды;
- файлға қолжетімдік уақытын, оны құруды және өзгертуді талдауды;
- жүйені/сервисті/желіні және қосымшаларды тіркеу журналын талдауды;

- жүйедегі/сервистегі/желідегі тұтынушылардың және (немесе) қосымшалардың қызметін анықтауды;

- электронды пошталарды шығыс ақпараттың және оның мазмұнының болуына талдауды;

- «Троян атынан» тұратын файлдарды және жүйеде басында болмаған файлдарды анықтау мақсатында файлдардың тұтастығын тексеруді жүргізуді;

- мүмкіндігіне қарай мүлікке келтірілген шығынның нақты айғақтарын талдау, мысалы, саусақ іздерін, бейнетаспа нәтижелері, дабыл жүйесін тіркеу журналдарын, куәгерлерді рұқсаттамаларын және сұраулар бойынша қолжетімдігін тіркеу журналдары;

- өндірілген әлеуетті куәліктерді зақымдауды, жарамсыз етуді болдырмау және санкцияланбаған адамдардың құпия материалын қарауды болдырмау үшін оларды өңдеуді және сақтауды. Айғақтарды жинау барлық жағдайда осы айғақтарды ұсыну мүмкін істерді тыңдау немесе сот ісі ережелеріне сәйкес жүргізілуге тиіс;

- бас есеп беруге қосымшаға енгізілген тиісті файлдардың тізіміне енгізе отырып, куәліктерді келтірумен оларды орындау уақытының және қажетті іс-әрекеттерде АҚ-нің оқыс оқиғасының себептері туралы қорытындыларды алуды;

- кез келген тәртіптік немесе құқықтық іс-әрекеттерді (қажет болғанда) сараптамалық қолдауды қамтамасыз етуді қамтуға тиіс.

Жоғарыда көрсетілген іс-әрекеттерді орындау әдісі (тері) АҚОЖТ-ның процедуралары жұмысында құжатталуға тиіс.

АҚОЖТ-ы техникалық білімнің кеңейтілген саласындағы әртүрлі дағдыларын (құралдарды және бұзушы пайдалануы мүмкін әдістерді білуді қоса алғанда), талдау/зерттеу жүргізу әдісін (пайдаланылатын куәліктерді қорғауды есепке алумен), құқықтық және нормативтік ережелерді білуі, АҚ-нің оқыс оқиғаларымен байланысты тенденциялар туралы тұрақты хабардар болуға тиіс.

8.5.6 Ақпарат беру

АҚОЖТ-ы АҚ-нің оқыс оқиғасының шынайылығын растау кезінде көп жағдайларда баспасөзді қоса алғанда ұйымның ішінде де, одан тыс та нақты адамдарды ақпараттандыру қажеттілігі (АҚОЖТ-ы мен басшылықтың арасындағы қарапайым байланыс желілерінен тыс) туындайды. Бұл үшін бірнеше кезең қажет етіледі, мысалы: АҚ-нің оқыс оқиғасының шынайылығын және оның бақылануын растау, АҚ-нің оқыс оқиғасын «дағдарысқа қарсы іс-әрекет» объектісі ретінде анықтау, АҚ-нің оқыс оқиғасын талдауды аяқтау және АҚ-нің оқыс оқиғасы туралы қорытындыны қалыптастыру.

Осындай қызметті қоса әрекет ету үшін АҚ-нің нақты оқыс оқиғасы туындауы және осы ақпаратты баспасөзге және (немесе) бұқаралық ақпарат құралдарына ұсынған жағдайда оны тез арада бейімдеу мақсатында нақты ақпаратты алдын ала дайындаған орынды. Егер баспасөзге АҚ-нің оқыс оқиғасына қатысты толық ақпарат ұсынылса, онда ол ұйымның ақпаратын тарату саясатына сәйкес ұсынылуға тиіс. Қоғам арасында таралуға жататын ақпаратқа тиісті адамдар, мысалы, жоғары басшы, қоғаммен байланыс жөніндегі үйлестіруші және АҚ-нің қызметкерлері талдау жасауға тиіс.

8.5.7 Шешімдерді қабылдау аясын кеңейту

АҚ-нің оқыс оқиғасы туралы шешімге жоғары басшыны, ұйым ішіндегі басқа топты немесе тараптық ұйымның адамын/тобын қатыстыру қажет болғанда жағдайлар туындауы мүмкін. Әңгіме АҚ-нің оқыс оқиғасына жататын ұсынылатын іс-әрекеттерге немесе қажет етілетін іс-әрекеттерді анықтау мақсатында одан әрі бағалауға қатысты шешімдерді қабылдау туралы болуы мүмкін. Шешімдерді қабылдау аясын кеңейту кейінен 8.4 бөліміне сәйкес бағалау процесін қажет етуі немесе, егер проблема оны анықтаудың ерте сатысында белгілі болса, бағалау процесінің барысында болуы мүмкін. Шешімді қабылдау

аясын кеңейту туралы шешімді бір кездері қабылдауы қажет әлде кім үшін, яғни пайдалануды қамтамасыз ету тобы және АҚОЖТ-ның мүшелері үшін АҚ-нің оқыс оқиғаларының менеджменті жүйесінің құжаттамасында тиісті сипатталуы қажет.

8.5.8 Іс-қимылды тіркеу және өзгерістер

АҚ-нің оқыс оқиғалары менеджментіне және хабарлауға (ақпараттандыру) қатыстырылғандар өздерінің барлық іс-қимылдарын одан әрі талдау жағдайларына олардға тиісті жолмен тіркеулері қажет. Осы іс-қимылдары туралы ақпаратты АҚ-нің оқыс оқиғалары туралы есеп беру нысанына АҚ-нің оқыс оқиғаларының есеп берудің бірінші нысанынан талдауды аяқтауға дейінгі АҚ-нің оқыс оқиғасы іс-әрекетінің барлық уақыты ішінде үздіксіз жаңартылатын АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасына енгізіледі.

Бұл ақпарат қорғаныс құралдарын қолдану және резервтеудің тиісті режімін қамтамасыз ету арқылы мүмкіндігінше сақталуға тиіс. Одан басқа АҚ-нің оқыс оқиғасын бақылау, есеп беру нысанын және АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасын жаңарту өзгерістерді енгізуді бақылаудың формальды қабылданған жүйесіне сәйкес енгізілуге тиіс.

9 «Талдау» кезеңі

9.1 Кіріспе

АҚ-нің оқыс оқиғасы туралы шешімдерді қабылдаған соң, АҚ-нің оқыс оқиғалары менеджментінің жалпы қауіпсіздігін және жүйесін әлеуетті жақсартуды және алынған сабақтарды анықтау мақсатында құқықтық сараптауды және талдауды одан әрі жүргізу қажет.

9.2 Одан әрі құқықтық сараптау

Кейде АҚ-нің оқыс оқиғасын жапқан соң куәліктерді анықтау мақсатында құқықтық сараптауды жүргізудің қажеттілігі бұрынғыша сақталуы мүмкін. Ол 8.5.5-ке сәйкес құралдардың және процедуралардың жиынтығын пайдаланумен АҚОЖТ-ы жүргізуге тиіс.

9.3 Алынған сабақтар

АҚ-нің оқыс оқиғасы аяқталған соң оның өңделуінен алынған сабақтарды тез арада сәйкестендіруі және мынадай:

- АҚ-нің қорғаныш шараларына қойылатын жаңа немесе өзгерген талаптары жағынан қаралуы мүмкін тиісті іс-әрекеттерді қабылдауы мүмкін. Бұл техникалық немесе техникалық емес (физикалықты қоса алғанда) қорғаныш шаралары болуы мүмкін. Талаптардың алынған сабақтарына байланысты қауіпсіздік мәселелерінде хабарланумен қамтамасыз ету (тұтынушылар, сондай-ақ басқа да қызметкерлер үшін) қауіпсіздік бойынша нұсқауларды және (немесе) стандарттарды шығаруды;
- АҚ-нің оқыс оқиғалары менеджментінің жүйесіндегі және оның процестеріндегі, есеп беру нысандарындағы және АҚ-нің оқиғаларының/оқыс оқиғаларының деректер базасындағы өзгерістерді қамтамасыз ету мақсатында материалдарды дереу жаңартуды және нұсқау жүргізуді қамтиды;

Одан басқа АҚ-нің оқыс оқиғасы бойынша сабақтармен танысу кезінде АҚ-нің жеке оқыс оқиғасы шеңберінде ғана алынған тәжірибелерді қарау емес, сонымен қатар АҚ-нің оқыс оқиғасын жою тәсілдерінің қорғау шараларындағы немесе өзгерістеріндегі қажеттіліктерді анықтау мүддесінде пайдаланылуы мүмкін АҚ-нің оқыс оқиғаларына алғышарттардың туындауы тенденцияларының (заңдылығын) болуын тексеру қажет.

Сондай-ақ АҚ-нің тестілеу жүргізу, әсіресе АҚ-нің оқыс оқиғасының АТ-не бағытталғаннан кейінгі осалдықтарды бағалау орынды.

Сондықтан алдағы уақытта оқыс оқиғалардың туындауы мүмкіндігін төмендету үшін ескерту шараларын қабылдауы мүмкін:

- тенденцияларды/үлгілерді;
- проблемалық салаларды;
- қызметтердің саласын анықтау үшін АҚ-нің оқиғалары/оқыс оқиғаларының деректер базаларын тұрақты талдау қажет.

АҚ-нің оқыс оқиғасын өңдеу процесінде алынатын маңызды ақпарат АҚ-нің оқыс оқиғаларын ертерек сәйкестендіруге айтарлықтай мүмкіндік беруі мүмкін тенденцияларды (заңдылықты) талдауға бағытталуға және АҚ-нің қандай оқыс оқиғалары алдағы тәжірибе және құжаттар негізінде туындау мүмкіндігі туралы ескертуді қамтуға тиіс. Мемлекеттік және коммерциялық КТЖЖБ-нан өнім берушілерден алынған АҚ-нің оқыс оқиғалары және оларға тиісті осалдықтар туралы ақпаратты пайдалану қажет.

Қауіпсіздікті тесттеу және АҚ-нің оқыс оқиғасынан кейінгі ақпараттық жүйенің, сервистің және (немесе) желінің осалдықтарын бағалау АҚ-нің осы оқыс оқиғасымен зақымданған тек ақпараттық жүйесімен, сервисімен және (немесе) желісімен шектелмеуге тиіс. Қауіпсіздікті тесттеуді және осалдықтарды бағалауды олармен байланысты кез келген ақпараттық жүйеге, сервиске және (немесе) желіге тарату қажет. Осалдықтарды егжей-тегжейлі бағалау АҚ-нің оқыс оқиғасы барысында басқа да ақпараттық жүйелерде, сервистерде және (немесе) желілерде осалдықтардың болуын анықтау және жаңа осалдықтардың туындау мүмкіндігін болдырмау үшін пайдаланылады.

Осалдықтарды бағалау тұрақты жүргізілуге тиістігін және АҚ-нің оқыс оқиғасынан кейін жүргізілетін осалдықтарды қайта бағалау бағалаудың үздіксіз процесін алмастыратын емес, оның бір бөлігі болуға тиістігін атап айту маңызды.

АҚ қамтамасыз ету мәселелері жөніндегі ұйым басшысының әрбір жиналысында және (немесе) АҚ-нің жалпы ұйымдастыру саясаты жөніндегі мәселелерге қатысты басқа да жиналыстарда оны талдау үшін АҚ-нің оқыс оқиғаларының қорытынды талдауын жариялау қажет.

9.4 Қауіпсіздікті жақсартуды анықтау

АҚ-нің оқыс оқиғасының рұқсатынан кейін талдау процесінде жаңа немесе өзгертілген қорғау шаралары қажеттілік ретінде анықталуы мүмкін. Ұсынымдар және қорғау шараларына қойылатын олардың тиісті талаптары оларды дереу енгізу қаржылық немесе пайдалану себептері бойынша мүмкін болмауы мүмкін, бұл жағдайда олар ұйымның неғұрлым ұзақ мерзімді мақсаттарында көзделуге тиіс. Мысалы, қаржылық түсінік бойынша неғұрлым желіаралық экранға ауысуды қысқа уақытта жүзеге асыру мүмкін емес, одан басқа осы мәселені шешу ұйымның АҚ-нің ұзақ мерзімді мақсатын енгізу қажет (10.3 бөлімін қараңыз).

9.5 Жүйені жақсартуды анықтау

Ақпарат рұқсатынан кейін АҚОЖТ-ның басшысы немесе оның орнына тағайындалған адам АҚ-нің оқыс оқиғасына жауап қайтару нәтижелігінің дәрежесін бағалау және анықтау мақсатында барлық оқиғаларға талдау жасауға тиіс. Осыған ұқсас талдау АҚ-нің оқыс оқиғалары менеджменті жүйесінің жетістікпен қатыстырылған элементтерін анықтауға және кез келген жетілдіруде нақты деректерді анықтауға арналған.

Оқыс оқиғаға жауап қайтарғаннан кейін жүргізілген талдаудың маңызды аспектісі АҚ-нің оқыс оқиғалары менеджментінің жүйесіне ақпараттың және алынған білімнің кері қайтуы болып табылады. Егер АҚ-нің оқыс оқиғасы айтарлықтай маңызды болса, онда

оқыс оқиға рұқсатынан кейін ол туралы ақпаратты білетін барлық мүдделі тараптар жиналыс жүргізуі қажет. Осы жиналыста мынадай:

- АҚ-нің оқыс оқиғалары менеджменті жүйесінде қабылданған процедуралар қажетінше жұмыс істеді ме;
- оқыс оқиғаларды анықтауға мүмкіндік беретін процедуралар немесе әдістер бар ма;
- жауап қайтару процесінде пайдаланылатын процедуралар немесе құралдар анықталды ма;
- оқыс оқиғаны сәйкестендіруден кейін ақпараттық жүйені қалпына келтіруге көмектесетін процедуралар қабылданды ма;
- анықтау, хабарлау және жауап қайтару процесстерінде тиімді барлық қатыстырылған тараптардың оқыс оқиғасы туралы ақпарат берілді ме – осындай мәселелер қаралуға тиіс.

Хабарлау нәтижелері құжатталуы және осы нәтижелер бойынша нақты келісілген іс-әрекеттер жүзеге асырылуға тиіс (10.4 бөлімін қараңыз).

10 «Жетілдіру» кезеңі

10.1 Кіріспе

«Жетілдіру» кезеңі «Талдау» кезеңінің ұсынымдарын, яғни АҚ-нің менеджменті нәтижелерін және қауіп-қатерлерін талдауын, АҚ-нің оқыс оқиғалары менеджментінің қауіпсіздігін және жүйесін жақсарту бойынша ұсынымдарды қамтиды. Осы ұсынымдардың әрқайсысы төменде қаралады.

10.2 Қауіпсіздік және қауіп-қатерлер менеджментін талдауды жетілдіру

АҚ-нің оқыс оқиғасының маңыздылығына және оның әсері деңгейіне байланысты АҚ-нің менеджментінің және АҚ-нің қауіп-қатерлерінің талдау нәтижелерін бағалау кезінде жаңа қауіптерді және осалдықты есепке алуға тура келеді. АҚ-нің қауіп-қатерлерін жаңартылған талдауды және АҚ-нің менеджментін талдауды аяқтау нәтижесінде қолданыстағыларға өзгерістер енгізу немесе жаңа қорғау шараларын қолдану қажеттігі туындайды.

10.3 Қауіпсіздікті жетілдіруді жүзеге асыру

«Талдау» кезеңі процесінде жасалған ұсынымдарды (9.4 бөлімі) және бірнеше оқыс оқиғаларды талдауды басшылыққа ала отырып, АҚ жаңартылған және (немесе) жаңа қорғау шараларын енгізу процестеріне бастамалық жасайды. 9.3-ке сәйкес бұл қауіпсіздік (тұтынушылар және басқа да қызметкерлер үшін) қауіпсіздік бойынша нұсқауларды және (немесе) стандарттарды шығару мәселелерінде хабарланумен қамтамасыз ету мақсатында нұсқау жүргізу үшін материалды тез арада жаңарту қажеттілігін қамту мүмкін (физикалықты қоса алғанда) қорғау шаралары болуы мүмкін.

Ұйымның ақпараттық жүйелері, сервистері және желілері, сонымен қатар жүйелердің/сервистердің/желілердің сенімділігін үздіксіз арттыру процесін қамтамасыз ету және осалдықтарды анықтау мақсатында тұрақты талдауға жатуға тиіс.

Процедуралардың және құжаматтамалардың қауіпсіздігіне байланысты талдау оқыс оқиғадан кейін тез арада жүргізілуі, бірақ кейіннен қажет етілетін неғұрлым мүмкін АҚ-нің оқыс оқиғасынан кейін АҚ-нің оқыс оқиғасы менеджментінің процесінде анықталған кез келген проблемаларды және жиналған ақпаратты есепке ала отырып, АҚ-нің қамтамасыз ету процедураларын және саясатын жаңарту қажет. Ұйымның АҚ-нің басшысымен бірге АҚОЖТ-ы ұзақ мерзімді мақсаты АҚ-нің қамтамасыз ету процедураларының және саясатының осы жаңартылған нұсқаларын ұйымға тарату болып табылады.

10.4 Жүйені жақсартуды жүзеге асыру

Жақсартуға арналған АҚ-нің оқыс оқиғалары менеджменті жүйесінің саласы (9.5-бөлімді қараңыз) талдау жасалған болуы, ал негізделген өзгерістер жүйе құжаттамасының жаңартылған нұсқасына енгізілуге тиіс. АҚ-нің оқыс оқиғалары менеджменті жүйесінің есеп беру нысандарындағы, процедураларындағы және процесстеріндегі өзгерістер мұқият тексерілуге және практикада қолдану алдында тесттелуге тиіс.

10.5 Басқа да жетілдірулер

«Талдау» деген кезеңде басқа да жақсартулар орнатылған болуы мүмкін, мысалы, АҚ-нің саясаттарындағы, стандарттарындағы және процедураларындағы өзгерістер, сондай-ақ аппараттық және бағдарламалық қамтамасыз ету конфигурацияларындағы өзгерістер.

А қосымша
(ақпараттық)

Ақпараттық қауіпсіздік оқиғалары және оқыс оқиғалары туралы есептер нысанының үлгісі

Ақпараттық қауіпсіздік оқиғалары және оқыс оқиғалары туралы есептер

А.1 Толтыру бойынша ұсынымдар

Осы нысанды тағайындау (АҚ-нің оқиғалары және оқыс оқиғалары туралы есептер нысаны) АҚ-нің оқиғасы туралы, содан кейін, егер ол АҚ-нің оқыс оқиғасы ретінде анықталса, онда белгілі бір адамдар үшін АҚ-нің оқыс оқиғасы туралы ақпаратты қамтамасыз ету болып табылады.

Егер АҚ-нің оқиғасы дамып жатса немесе болған болса, әсіресе ұйымның меншіктігін немесе беделін айтарлықтай жоғалтуға немесе шығынға әкеп соқтыруы мүмкіндігіне күдік болса, онда ұйымның АҚ-нің оқыс оқиғалары менеджментінің жүйесінде сипатталған рәсімдерге сәйкес АҚ-нің оқиғалары туралы есептер нысанын тез арада толтыру және тапсыру қажет.

Ұсынылған ақпарат осы оқиға АҚ-нің оқыс оқиғасы ретінде санатталуға тиістігін және (оң жауап болған жағдайда) жоғалту мен шығынды болдырмау немесе шектеу үшін қажет қандай түзету шаралар қабылдаған дұрыстығын анықтайтын бағалаудың тиісті процесіне бастамалық жасау үшін пайдаланылатын болады. Бағалау процесі барлық сипат бойынша қысқа мерзімді болып табылса, онда осы сәтте есеп беру нысанының барлық сызығын толтыру міндетті емес.

Егер қызметкер есеп берудің толтырылған нысанын толық/біртіндеп талдайтын пайдалануды қамтамасыз ету тобының мүшесі болса, онда ол осы оқиғаны АҚ-нің оқыс оқиғасы санатына жатқызуға болатын, болмайтынына шешім қабылдауға тиіс. Бұл ретте қызметкер оң шешіммен АҚ-нің оқыс оқиғасы туралы неғұрлым көп ақпаратты есеп берудің нысанына енгізуі және АҚ-нің оқиғасы және оқыс оқиғасы туралы есеп берулердің нысандарын АҚОЖТ-ға беруге тиіс. АҚ-нің оқиғасы АҚ-нің оқыс оқиғасы санатына жататынына қарамастан, АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасы жаңартылуға тиіс.

Егер қызметкер пайдалануды қамтамасыз ету тобының мүшесі берген АҚ-нің оқиғалары және оқыс оқиғалары туралы есеп берулердің нысандарын талдайтын АҚОЖТ-ның қызметкері болса, зерттеу барысы бойынша жаңартылуы және тиісінше АҚ-нің оқиғалары/оқыс оқиғаларының деректер базасы жаңартылуға тиіс.

Нысандарды толтыру кезінде мынадай ұсынымдар сақтау керек:

- мүмкіндігінше есептер нысаны электронды түрде* толтырылуға және берілуге тиіс. Егер проблемалар болса немесе жүйеге рұқсатсыз кіру және есептер нысандары санкцияланбаған адамдар оқуы мүмкін жағдайларды қоса алғанда (мысалы, электронды пошта) электронды хабарлау механизмінің өкілеттігі бойынша қабылданған проблемалар бар деп есептелінсе, байланыстың балама құралдары пайдаланылуға тиіс. Байланыстың балама құралдары телефон немесе мәтін хабарламасы, сондай-ақ курьерлерді пайдалану болуы мүмкін.*

- қызметкер сенімді болған фактілерге негізделген ақпаратты ұсыну қажет, барлық нысандарды толтыру үшін ойдан шығару қажет емес. Егер қызметкер растай алмайтын

* Егер мүмкін болса, онда есептер нысандары болуға тиіс, мысалы, АҚ оқыс оқиғаларының электронды деректер базасындағы қауіпсіз web-бетте. Қазіргі кезде қағаз технологиясына негізделген жүйе өте баяу жұмыс істейтін және пайдалануда айтарлықтай тиімді емес болып табылады.

басқа да ақпаратты енгізуді дұрыс деп есептесе, ол ақпараттың расталмағанын және оның дұрыстығына сену себебін көрсетуі қажет;

- қызметкермен қалай байланысуға болатыны егжей-тегжейлі көрсетілуі қажет. Ұсынылған есепке қатысты одан әрі ақпарат алу үшін онымен байланыс жасау қажеттілігі дереу немесе бірнеше уақыт өткен соң туындауы мүмкін.

Егер қызметкер кейіннен оның ұсынған қандай да бір ақпараты нақты еместігін анықтаған болса, онда есеп берулерге түзету енгізу және оны қайта ұсыну қажет.

А.2 Ақпараттық қауіпсіздіктің оқиғалары туралы есептер нысаны

Ақпараттық қауіпсіздіктің оқиғалары туралы есеп

Оқиға күні

Оқиға нөмірі*

Оқиғалардың және (немесе оқыс оқиғалардың тиісті сәйкестендіру нөмірі (егер қажет етілсе):

Хабарлайтын адам туралы ақпарат

Тегі	_____	Мекенжай	_____
Ұйым	_____		_____
Телефон	_____	Электрондық пошта	_____

АҚ-нің оқиғасын сипаттау

Оқиғаны сипаттау:

Не болды

Қалай болды

Неден болды

Зақымданған құрауыштар

Ұйымға жағымсыз әсері

Кез келген сәйкестендірілген осалдықтар

АҚ-нің оқиғасының нақты дерегі

Оқиғаның болған күні және уақыты

Оқиғаны анықтаған күні және уақыты

Оқиға туралы хабарлаған күні және уақыты

Оқиға аяқталды ма? (шаршымен белгілеңіз)

Иә □ Жоқ □

Егер «иә», онда оқиғаның ұзақтығын күнмен/сағатпен/минутпен нақтылау

* Оқиғаның нөмірін ұйымның АҚОЖТ-ның басшысы белгілейді.

А.2 Ақпараттық қауіпсіздіктің оқыс оқиғасы туралы есеп *(жалғасы)*

Оқиғаның күні

Оқыс оқиғаның нөмірі*

Оқиғалардың және (немесе) оқыс оқиғалардың тиісті сәйкестендірілген нөмірі (егер қажет етілсе):

Пайдалануды қамтамасыз ету тобының қызметкері туралы ақпарат

Тегі _____ Мекен-жайы _____

Телефон _____ Электрондық пошта _____

АҚОЖТ-ның қызметкерлі туралы ақпарат

Тегі _____ Мекен-жайы _____

Телефон _____ Электрондық пошта _____

АҚ-нің оқыс оқиғасын сипаттау

Оқиғаны қосымша сипаттау:

Не болды

Қалай болды

Неден болды

Зақымданған компоненттер

Ұйымға жағымсыз әсер ету

Кез келген сәйкестендірілген осалдықтар

АҚ-нің оқыс оқиғасы туралы егжей-тегжейлер

Оқыс оқиғаның туындаған күні және уақыты

Оқыс оқиғаны анықтаған күн және уақыт

Оқыс оқиға туралы хабарлаған күн және уақыт

Оқиға аяқталады ма? (шаршымен белгілеңіз) Иә □ Жоқ □

Егер «Иә», онда оқиғаның ұзақтығын күнмен/сағатпен/минутпен нақтылау. Егер «Жоқ», онда оның ұзақтығын нақтылау

* Оқыс оқиғалардың нөмірін ұйымның АҚОЖТ-ның басшысы белгілейді және тиісті оқиғалардың нөміріне жалғасады.

А.2 Ақпарттық қауіпсіздіктің оқыс оқиғасы туралы есеп *(жалғасы)*

АҚ-нің оқыс оқиғасының типі

(Шаршылардың біріне белгі қою, содан кейін төмендегі тиісті сызықты толтыру

Ұзақ □ Ниет □ Болжалды □

(ішінен біреуін) Ниет □ (қауіптің типі көрсетілсін)

Ұрлау (TH) □ Сипаттық /логикалық рұқсатсыз кіру (HA) □

Алдауыш (FR) □ Ресурстарды дұрыс пайдаланбау (MI) □

Іріткі салу әрекеті/физикалық шығын (SA) □ Басқа шығын (OD) □

Зиянды тасымал бағдарламасы (MC) □

Анықтау:

(ішінен біреуін) кездейсоқ □ (қауіптің типі көрсетілсін)

Аппаратураның жұмыс істемеуі (HF) □ Басқа да табиғи оқиғалар (NE) □

Жұмыс істемеу ПО (SF) □ Анықтау:

Байланыс жүйесінің жұмыс істемеуі (CF) □ Маңызды сервистерді жоғалту (LE) □

Өрт (HE) □ Кадрмен жеткіліксіз қамтамасыз етілу (SS) □

Су басу (FL) □ Басқа да жағдайлар (OA) □

Анықтау:

(ішінен біреуін) Қателік □ (қауіптердің типі көрсетілсін)

Операциялық қателік (OE) □ Тұтынушының қателігі (UE) □

Аппараттық құралдарды пайдаланудағы қателік (HE) □ Жобалау қателігі (DE) □

Пайдаланудағы қателік ПҚ (SE) □ Басқа да жағдайлар (болжалмаған қателіктерді қоса алғанда) (OA) □

Анықтау:

Белгісіз □ (Егер АҚ-нің оқыс оқиғасының типі белгіленбеген болса, (болжалған, кездейсоқ, қателік) белгіленбеген болса, онда «белгісіз» деген шаршыға белгі қою қажет және мүмкіндігінше жоғарыда келтірілгендерді, қысқартуларды пайдалана отырып, қауіптердің типін көрсету қажет)

Анықтау:

А.2 Ақпараттық қауіпсіздіктің оқыс оқиғасы туралы есеп *(жалғасы)*

Зақымданған активтер

Зақымданған активтер (болған кезде)	(АҚ-нің оқыс оқиғаларымен зақымданған немесе сериялық, лицензия нөмірлерін және нұсқалардың нөмірін қоса алғанда, оларға байланысты (қажет етілген жерде) активтерді сипаттау күні
	Ақпарат/деректер _____
	Аппараттық құралдар _____
	Бағдарламалық қамтамасыз ету _____
	Байланыс құралдары _____
	Құжаттама _____

Оқыс оқиғаның ұйым қызметіне жағымсыз әсер етуі/әсер

Төменде көрсетілген бұзушылықтар үшін тиісті шаршыларға белгі қойылсын, содан кейін «маңыздылық» деген бағанда мынадай қысқартуларды пайдалана отырып, 1 10 шкаласы бойынша ұйымның қызметіне жағымсыз әсер ету деңгейі көрсетілсін:

(FD) — операцияның қаржылық шығыны/үзілуі, (CE) — коммерциялық және экономикалық мүдделер, (PI) — дербес деректерден тұратын ақпарат, (LR) — құқықтық және нормативтік міндеттер (бұл осыған ұқсас түпнұсқамен салыстыруға қажет), (MO) — менеджмент және операция, (LG) — беделді жоғалту (В қосымшасындағы мысалды қараңыз.). «Көрсеткіш» деген бағандағы код әрпін жазып алу, егер нақты ұстаулар белгіде болса – олар «құны» деген бағанда көрсетілсін.

		Маңыздылығы	Көрсеткіш	Ұстап қалу
Құпиялықтың бұзылуы (яғни санкцияланбаған ашу)	□			
Тұтастығының бұзылуы (яғни санкцияланбаған түрлену бар)	□			
Қолжетімдіктің бұзылуы (яғни қолжетімділік)	□			
Бас тартудың бұзылуы	□			
Жою	□			
(«Маңыздылық» үшін жалпы 1 10 шкаласы бойынша және «құны» үшін ақшалай АҚ-нің оқыс оқиғасынан кейін қалыпқа келтіруге арналған жалпы шығыстарды көрсетуге болатын орын)		Маңыздылығы	Көрсеткіш	Ұстап қалу

АҚ-нің оқыс оқиғасынан кейін қалыпқа келтіруге арналған жалпы шығыстар

А.2 Ақпараттық қауіпсіздіктің оқыс оқиғасы туралы есеп *(жалғасы)*

Оқыс оқиға рұқсаты

АҚ-нің оқыс оқиғасын тексеру күні _____
Оқыс оқиғаға тексеру жүргізген адамның (дардың) тегі _____
АҚ-нің оқыс оқиғасының аяқталған күні _____
әсер етудің аяқталған күні _____
АҚ-нің оқыс оқиғасын тексеру аяқталған күн _____
Тексеру туралы есепті сақтау орны _____

Оқыс оқиғаға қатысы бар адам/бұзушылар

(ішінен біреуін)
Адам (PE) □
Ұйымдастырылған топ (GR) □
Ресми құрылтайланған ұйым/мекеме (OI) □
Кездейсоқтық (AC) □
Бұзушының болмауы (NP) □
Мысалы, табиғи факторлар, жабдықтың жұмыс істемеуі, адами фактор

Бұзушының сипатты

(ішінен біреуін)
Нақты немесе болжалды дәлел
Криминалдық/қаржылық пайда(CG) □
саясат/терроризм (PT) □
сауық/хакерлік (PH) □
орын (RE) □
Басқа да мотивтер (OM)

Анықтау:

АҚ-нің оқыс оқиғасы рұқсаты үшін пайдаланылатын іс-әрекеттер
(мысалы, «ешбір іс-әрекет», «қолдағы құралдармен», «ішкі тексеріс», «..... қатыстыру арқылы сыртқы тексеріс»)

Оқыс оқиға рұқсаты үшін жоспарланған іс-әрекеттер
(жоғары келтірілген мүмкін іс-әрекеттерді қоса алғанда)

Басқа да іс-әрекеттер
(мысалы, бұрынғыша тексеру қажет етіледі, бірақ басқа қызметкерлердің тексеруімен)

А.2 Ақпараттық қауіпсіздік оқиғасы туралы есеп *(жалғасы)*

Қорытынды

(оқыс оқиға маңызды не маңызды еместігін шаршылардың біріне белгілеу және осы қорытындының қысқа мазмұнын қоса беру (басқа да кез келген қорытындыны көрсету)

Маңызды □ Маңызды емес □

_____

Хабарландырылған адамдар/субъектілер

(есеп берудің бұл бөлігі АҚ саласында міндет жүктелген және талап етілетін іс-әрекеттерді жасайтын тиісті адам толтырады. әдетте бұл адам ұйымның АҚ-нің басшысы болып табылады)

АҚ қызметінің басшысы □

Жергілікті басшы (қандай бөлімнен екендігін нақтылау) □

АҚОЖТ-ның басшысы □

Ақпараттық жүйенің басшысы □

Есеп берудің авторы □

Полиция □

Есеп беру авторының басшысы □

Басқа да адамдар □ (мысалы, анықтамалық қызмет, кадр бөлімі, қызмет басшысы, ішкі аудит қызметі, бөгде КСБР, регулятивті орган)

Анықтау:

Қатыстырылған адамдар

Бастамашы	Талдаушы	Талдаушы
Қолы _____	Қолы _____	Қолы _____
Тегі _____	Тегі _____	Тегі _____
Лауазымы _____	Лауазымы _____	Лауазымы _____
Күні _____	Күні _____	Күні _____

Талдаушы	Талдаушы	Талдаушы
Қолы _____	Қолы _____	Қолы _____
Тегі _____	Тегі _____	Тегі _____
Лауазымы _____	Лауазымы _____	Лауазымы _____
Күні _____	Күні _____	Күні _____

Б қосымшасы
(Ақпараттық)

Ақпараттық қауіпсіздіктердің оқыс оқиғаларын бағалау жөніндегі жалпы ұсынымдардың үлгісі

Б.1 Кіріспе

Осы қосымшада АҚ-нің оқыс оқиғаларының қолайсыз салдарын бағалау және санаттау жөніндегі мысалға келтірілген ұсыным ұсынылған. Мұнда әрбір ұсынымның 1-ден 10-ға дейінгі шкаласы бар (1 – төмен, 10 – жоғары) (Практикада басқа да шкалалар пайдаланылады, мысалы, 1-ден 5-ке дейінгі градацияда. Әрбір ұйым өзінің шарттарына неғұрлым сәйкес келетін шкаланы пайдалануға тиіс).

Ұсыныммен танысу алдында мынадай түсініктемелермен танысуы қажет:

- төменде келтірілген ұсынымдардың кейбіреулерінде АҚ-нің оқыс оқиғасының әрбір градациясы үшін (1-ден 10-ға дейінгі) және сәйкесінше басқа шкалалар үшін (мысалы, 1-ден 5-ке дейінгі градациямен) келтірілген жағымсыз салдарлар үшін «Жазба жоқ» деген ескерту қамтылады. Бірақ кейбір градацияларда (1-ден 10-ға дейінгі шкала бойынша) АҚ-нің нақты оқыс оқиғалары үшін АҚ-нің оқыс оқиғасы салдары туралы жазбаларда үлкен айырмашылық болмағандықтан, неғұрлым төмен градацияда жазба жазу орынды емес деп есептелінеді және бұл жағдайда «Жазба жоқ» деген ескертпе жасалады. Осыған ұқсас жоғарыда баяндалғанға байланысты, АҚ-нің оқыс оқиғасының неғұрлым жоғары градациялары кезінде олар үшін қолайсыз салдарлар жоғары градация үшін көрсетілген маңызды жағымсыз салдарлар болуы мүмкін емес деп есептелінеді және тиісінше осы градациялар үшін «Жазба жоқ» деген ескертпе болады. (Сондықтан, шкалалардың градациясын және «Жазба жоқ» деген белгілеуді алып тастау дұрыс емес);
- келтірілген ұсынымдар үшін айырмашылық шамасында келтірілген қаржы көрсеткіштерін қолдану біршама қарапайым емес сияқты көрінеді. Осы ұсынымдарды пайдалану алдында ұйымға неғұрлым сәйкес келетін валюталар курсының ауысып тұруын нормалаумен толықтырылуға тиіс.

Сондықтан, ақпараттық санкцияланбай ашылуы, ақпараттың санкцияланбаған өзгерістері, пайдаланылған ақпараттың жұмыс істемеуі, ақпаратқа және (немесе) сервиске қолжетімсіздік, ақпаратты және (немесе) сервисті жою болып табылатын ұйымдар қызметі үшін АҚ-нің оқыс оқиғасының жағымсыз салдарын тексеру үшін санамаланатын ұсынымдарды пайдалану кезінде бірінші кезекте төменде көрсетілген санаттардың қайсысы сәйкесті болатынын анықтау қажет. АҚ-нің оқыс оқиғасы туралы есеп беру нысанына енгізу мақсатында бизнес-процесске («маңыздылық») нақты жағымсыз әсер етуді анықтау үшін санаттау бойынша ұсыным қабылдау қажет.

Б.2 Операциялардың барысының қаржылық шығындары/бұзушылық

Берілген ақпаратты санкцияланбай ашудың, түрлендірудің және ойды бұрмалаудың сондай-ақ осындай ақпараттың қолжетімсіздігі және жойылуы салдары қаржылық шығынға әкелуі мүмкін, мысалы, акцияға баға төмендеу, осы салдарларға қатысты әрекет етпеу немесе кештетіп әрекет ету себептерінен алдауыш немесе байланыстың бұзылуы нәтижесінде.

Кез келген ақпараттың қолжетімсіздігі немесе жойылуы салдарынан бизнес-процесс бұзылуы мүмкін. АҚ-нің осындай оқыс оқиғаларынан кейін жағдайды жөндеуге және (немесе) бизнес-процессті қалпына келтіруге уақыт және күш талап етіледі. Бұл салдарлар кейбір жағдайларда маңызды болуға және назарға алынуға тиіс. Салдарларды есептеу үшін қалпына келтіру уақыты қызметкерлердің жұмыс уақыты бірліктерінде есептелуге және жұмыс уақытының құны қайта есептелуге (қаржылық шығын) тиіс. Бұл қаржылық

шығындар ұйым ішінде қабылданған тиісті градация/деңгей бойынша 1 адамның айына орташа жұмыс істеу құнына қарап, есептелуге тиіс. Мынадай ұсынымдарды басшылыққа алу ұсынылады:

1) x_1 немесе одан аз қаржылық шығындардағы/шығыстардағы нәтиже;
2) x_1 және x_2 арасындағы қаржылық шығындардағы/шығыстардағы нәтиже;
3) $x_2 + 1$ и x_3 арасындағы қаржылық шығындардағы/шығыстардағы нәтиже;
4) $x_3 + 1$ и x_4 арасындағы қаржылық шығындардағы/шығыстардағы нәтиже;
5) $x_4 + 1$ и x_5 арасындағы қаржылық шығындардағы/шығыстардағы нәтиже;
6) $x_5 + 1$ и x_6 арасындағы қаржылық шығындардағы/шығыстардағы нәтиже;
7) $x_6 + 1$ и x_7 арасындағы қаржылық шығындардағы/шығыстардағы нәтиже;
8) $x_7 + 1$ и x_8 арасындағы қаржылық шығындардағы/шығыстардағы нәтиже;
9) x_8 астам қаржылық шығындардағы/шығыстардағы нәтиже;
10) ұйым жұмысты аяқтайды.

Б.3 Коммерциялық және экономикалық мүдделер

Коммерциялық және экономикалық ақпарат қорғауды қажет етеді және оның беделін түсіретін әсерлер бойынша немесе бәсекелестер үшін оның маңыздығы есебімен бағаланады. Мүдделерді білдіретін ақпаратты қорғауды қамтамасыз ету бойынша мынадай ұсынымдарды басшылыққа алған дұрыс:

1) бәсекелестік үшін, бірақ коммерциялық маңызы (құндылығы) жоқ;
2) y_1 немесе одан төменге (коммерциялық айналым) тең ақпарат құндылығының параметрі мәні кезіндегі бәсекелестік үшін;
3) $У_1$+ 1 және $У_2$ (айналым) диапазонындағы немесе жалақының қаржылық шығыны немесе жоғалуы болып табылатын немесе заңсыз пайдаларды жеңілдететін немесе үшінші бір тараптың беретін ақпаратының дұрыстығын растау бойынша міндеттерді бұзатын ақпарат құндылығының параметрі мәні кезіндегі бәсекелестік үшін;
4) $У_1$+ 1 және $У3$ (тауар айналым) диапазонындағы ақпарат құндылығының параметрі мәні кезіндегі бәсекелестік үшін;
5) $У_3$ + 1 и $У_4$(тауар айналым) диапазонындағы ақпарат құндылығының параметрі мәні кезіндегі бәсекелестік үшін;
6) $У_4$ + 1 (айналым) астам диапазонындағы ақпарат құндылығының параметрі мәні кезіндегі бәсекелестік үшін; сондай-ақ мына жағдайларды:
7) жазба жоқ*;
8) жазба жоқ;
9) коммерциялық мүдделерге елеулі әсер етуі болуы немесе ұйымның қаржылық жағдайын бұзу мүмкін;
10) жазба жоқ

[1] «Жазба жоқ» деген термин АҚ-нің оқыс оқиғасы салдарының осы градациясы үшін тиісті жазба жоқ дегенді білдіреді.

Б.4 Дербес деректерден тұратын ақпарат

Жеке адамдардың дербес деректерінен тұратын ақпаратты ақтау және өңдеу орындарында адамгершілік және этикалық деп саналады, ал кейбір жағдайларда жақсы жағдайда заңды тұлғаға қолайсыздық, ал кейбір міндеттемелер кезінде кері жағдайда ашылған ақпаратқа дербес деректерді қорғау бөлігінде заңнама талаптарына сәйкес адамды сотпен қудалауға соқтыруы мүмкін санкцияланбаған ашудан болатын осы ақпаратты қажетті заңды қорғау болып есептелінеді. Тең дәрежелерде дербес деректерден тұратын ақпарат барлық жағдайда дұрыс болуы, себебі қолайсыз деректердің туындауына әкеп соқтыратын оның санкцияланбаған өзгерістері оның санкцияланбаған ашуының салдары болуы мүмкін. Дербес деректерден тұратын ақпаратты қолжетімді ету немесе жою маңызды, өйткені бұл АҚ-нің оқыс оқиғасы уақытында заңды тұлғалардың дұрыс шешім қабылдауына немесе олардың әрекетсіздігіне әкеп соқтыруы мүмкін, бұның санкцияланбаған ашу немесе түрлендіру сияқты әсері болуы мүмкін. Дербес деректерден тұратын ақпараттың шығынын болдыру градациясы бойынша мынадай ұсынымдарды басшылыққа алу қажет:

1) нақты адамға маңызды емес шығын (қолайсыздық) әкелу (залал тигізу), бірақ құқықтық немесе нормативтік талаптарды бұзу емес;

2) нақты адамға маңызды емес шығын (қолайсыздық) әкелу (залал тигізу) (ызасын келтіру, көңіл күйін бұзу), бірақ құқықтық немесе нормативтік талаптарды бұзу емес;

3) құқықтық, нормативтік немесе этикалық талаптарды бұзу, сондай-ақ нақты адамға немесе адамдар тобына маңызды емес қолайсыздық тудыратын ақпаратты қорғаудың бұзылуына қатысты ниеттерді жариялау;

4) құқықтық, нормативтік немесе этикалық талаптарды бұзу, сондай-ақ нақты адамға маңызды қолайсыздық немесе адамдар тобына маңызды емес қолайсыздық тудыратын ақпаратты қорғаудың бұзылуына қатысты ниеттерді жариялау;

5) құқықтық, нормативтік немесе этикалық талаптарды бұзу, сондай-ақ нақты адамға маңызды проблемалар тудыратын ақпаратты қорғаудың бұзылуына қатысты ниеттерді жариялау;

6) құқықтық, нормативтік немесе этикалық талаптарды бұзу, сондай-ақ адамдар тобы үшін маңызды проблемалар тудыратын ақпаратты қорғаудың бұзылуына қатысты ниеттерді жариялау;

7) жазба жоқ;

8) жазба жоқ:

9) жазба жоқ;

10) жазба жоқ.

Б.5 Құқықтық және нормативтік міндеттер

Ұйымның сақтайтын және өңдейтін деректері құқықтық және нормативтік міндеттерге бағынуы немесе ұйым қызметінің осы міндеттемелерге сәйкестігін қамтамасыз ету мақсатында сақталуы және өңделуі мүмкін. Ниеттелген немесе ниеттелмеген осындай міндеттемелерді сақтамау осы ұйымда жұмыс істейтін адамдарға құқықтық немесе әкімшілік шаралар қабылдауға әкеп соқтыруы мүмкін. Осы шараларды қабылдау нәтижесі айыппұл салу және (немесе) түрмеге жабу болуы мүмкін.

Мынадай ұсынымдарды басшылыққа алу ұсынылады:

1) жазба жоқ;

2) жазба жоқ;

3) z_1 немесе одан аз қаржылық шығынға/айыппұлға әкеп соқтыратын құқық қолдану, азаматтық талап арыз немесе қылмыстық іс туралы ескерту;

4) $z_1 + 1$ және z_2 арасындағы қаржылық шығынға/айыппұлға әкеп соқтыратын құқық қолдану, азаматтық талап арыз немесе қылмыстық іс туралы ескерту;

5) $z_2 + 1$ и z_3 арасындағы қаржылық шығынға/айыппұлға немесе екі жылға дейін түрме жабуға әкеп соқтыратын құқық қолдану, азаматтық талап арыз немесе қылмыстық іс туралы ескерту;

6) $z_3 +$ және z_4 арасындағы қаржылық шығынға/айыппұлға немесе екі жылдан он жылға дейін түрме жабуға әкеп соқтыратын құқық қолдану, азаматтық талап арыз немесе қылмыстық іс туралы ескерту;

7) қаржылық шығынға/айыппұлға немесе он жылға дейін түрме жабуға әкеп соқтыратын құқық қолдану, азаматтық талап арыз немесе қылмыстық іс туралы ескерту;

8) жазба жоқ;

9) жазба жоқ;

10) жазба жоқ.

Б.6 Менеджмент және операция

Ақпарат ұйымның тиімді жұмысына шығын әкелуге мүмкіндік жасайтын оның осындай беделді түсіруі болуы мүмкін. Мысалы, келешекте саясатқа өзгеріс енгізуге қатысты ақпарат ашылса, осындай қоғамдық жауап қайтаруды арандату осы саясатты іске асырылуына мүмкіндік бермеуі мүмкін. Берілген ақпаратты түрлендіру, мағынасын өзгерту немесе қаржылық аспектілерге немесе компьютерлік бағдарламалық қамтамасыз етуге қатысты ақпараттың қолжетімдігі ұйымның жұмысы үшін маңызды салдар болуы мүмкін. Одан басқа АҚ-нің қамтамасыз ету бойынша міндеттердің бас тартуы ұйымның жұмысы үшін жағымсыз салдар болуы мүмкін. Салдарларды бағалау бойынша мынадай ұсынымдарды басшылыққа алу ұсынылады:

1) ұйымның бір бөлімшесінің тиімді емес жұмысы;

2) жазба жоқ;

3) ұйымды және оның жұмысын тиімді басқару бойынша функцияның (қызметтің) бұзылуы;

4) жазба жоқ;

5) ұйым саясатын тиімді әзірлеу немесе функциялау үшін кедергілер жасау;

6) басқа ұйымдармен коммерциялық немесе саяси келісімге келулер кезінде ұйымға шығын келтіру;

7) ұйым басты саясатын тиімді әзірлеу немесе функциялау үшін кедергілер жасау, қандай да бір тәсілмен маңызды операцияларды ажырату немесе маңызды тоқтату;

8) жазба жоқ;

9) жазба жоқ;

10) жазба жоқ.

Б.7 Беделді жоғалту

Ақпараттың санкцияланбай ашылуы, АҚ қамтамасыз ету бойынша міндеттемелерден бас тарту немесе ақпаратты түрлендіру, сондай-ақ ақпараттың қолжетімсіздігі ұйымның одан әрі беделін жоғалтуына, сенімді жоғалтуына және басқа да жағымсыз салдарларға әкеп соқтыратын ұйымның беделін жоғалтуы мүмкін.

Ұйымның беделін бағалау бойынша мынадай ұсынымдарды басшылыққа алу ұсынылады:

1) жазба жоқ;

2) ұйым ішінде қанағаттанбаушылықты болдыру;

3) жергілікті/өңірлік масштабтағы қажет етілмеген салдарларға әкеп соқтыратын акционерлермен, тұтынушылармен, өнім берушілермен, реттеуші органдармен, үкіметпен, өзге де ұйымдармен немесе қоғамдастықпен арақатынасына жағымсыз әсер;

4) жазба жоқ;

5) ұлттық масштабтағы қажет етілмеген салдарларға әкеп соқтыратын акционерлермен, тұтынушылармен, өнім берушілермен, реттеуші органдармен, үкіметпен, өзге де ұйымдармен немесе қоғамдастықпен арақатынасына жағымсыз әсер;

6) жазба жоқ;

7) қажет етілмеген салдарларға әкеп соқтыратын акционерлермен, тұтынушылармен, өнім берушілермен, реттеуші органдармен, үкіметпен, өзге де ұйымдармен немесе қоғамдастықпен арақатынасына маңызды жағымсыз әсер;

8) жазба жоқ;

9) жазба жоқ;

10) жазба жоқ.

Библиография

[1] ҚР СТ ИСО/МЭК 13335-2-1998 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологияларды қорғауды басқару. 1-бөлім. Ақпараттық және коммуникациялық технологияларды қорғауды басқаруға арналған жалпы ұғымдар мен модельдер.

[2] ҚР СТ ИСО/МЭК ТО 15947-2002 Ақпараттық технология. Ақпаратты қорғауды басқару жөніндегі ереженің жиынтығын қорғауды қамтамасыз ету әдістері

[3] ҚР СТ ИСО/МЭК ТО 18043-2002 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Рұқсатсыз кіру және анықтау жүйесін таңдау, өрістету және пайдалану жөніндегі ұсыныс.

[4] ҚР СТ ИСО 9000-2005 Қазақстан Республикасының Мемлекеттік техникалық реттеу жүйесі. Сапа менеджменті жүйесінің стандарттар жинағы.

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: ақпараттық қауіпсіздіктің оқыс оқиғаларының менеджменті, ақпараттық қауіпсіздіктің оқыс оқиғасына жауап қайтару тобы, ақпараттық қауіпсіздік оқиғасы, ақпараттық қауіпсіздік менеджментінің жүйесі

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Управление нарушениями безопасности информации

СТ РК ИСО/МЭК ТО 18044-2009

ISO/IEC TR 18044:2004 Information technology. Security techniques.Information security incident management, IDT

Издание официальное

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

Астана

Предисловие

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

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

3 Настоящий стандарт идентичен международному стандарту ISO/IEC TR 18044:2004 Information technology - Security techniques-Information security incident management (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности).

Перевод с английского языка (en)

Степень соответствия - идентичная (IDT)

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

5 ВВЕДЕН ВПЕРВЫЕ

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

Содержание

Введение

Типовые политики информационной безопасности или защитные меры информационной безопасности (ИБ) не могут полностью гарантировать защиту информации, информационных систем, сервисов или сетей. Поэтому внедрение защитных мер не обеспечивает полной защиты, следовательно, инциденты информационной безопасности возможны. Инциденты информационной безопасности могут оказывать прямое или косвенное негативное воздействие на функционирование организации. Кроме того, будут неизбежно выявляться новые, ранее не идентифицированные угрозы. Недостаточная подготовка конкретной организации к обработке таких инцидентов делает практическую реакцию на инциденты малоэффективной, и это потенциально увеличивает степень негативного воздействия на функционирование организации. Таким образом, для любой организации, серьезно относящейся к информационной безопасности, важно применять структурный и плановый подход к:

- обнаружению, оповещению об инцидентах информационной безопасности, их оценке;
- реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после негативных воздействий (например, в областях поддержки и планирования непрерывности рабочего процесса);
- извлечению уроков из инцидентов информационной безопасности, введению превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

Положения настоящего стандарта содержат представление о менеджменте инцидентов информационной безопасности в организации с учетом сложившейся практики на международном уровне.

Настоящий стандарт предназначен для использования организациями всех сфер деятельности при обеспечении информационной безопасности в процессе менеджмента инцидентов. Его положения могут использоваться совместно с другими стандартами, в том числе стандартами, содержащими требования к системе менеджмента информационной безопасности и системе менеджмента качества организации

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Управление нарушениями безопасности информации

Information technology. Security techniques.Information security incident management

Дата введения 2010-07-01

1 Область применения

Настоящий стандарт устанавливает порядок управления нарушениями безопасности информации, содержит рекомендации по менеджменту инцидентов информационной безопасности в организациях для руководителей подразделений по обеспечению информационной безопасности (далее - ИБ) при применении информационных технологий (далее - ИТ), информационных систем, сервисов и сетей.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные нормативные документы:

СТ РК ИСО/МЭК 13335-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных технологий. Часть 1. Общие понятия и модели для управления защитой информационных и коммуникационных технологий.

СТ РК ИСО/МЭК 17799-2006 Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации.

ПРИМЕЧАНИЕ При пользовании настоящим Стандартом целесообразно проверить действие ссылочных стандартов классификаторов по ежегодно издаваемому информационному указателю «Нормативные документы по стандартизации» по состоянию на текущий год и соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим Стандартом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применяются термины по СТ РК ИСО/МЭК 13335-1, СТ РК ИСО/МЭК 17799, а также следующие термины с соответствующими определениями:

3.1 **Планирование непрерывности деятельности** (business continuity planning): Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность деятельности организации и поддерживающих ее элементов.

Издание официальное

ПРИМЕЧАНИЕ Данный процесс должен также обеспечивать восстановление деятельности с учетом заданных очередностей и интервалов времени и дальнейшее восстановление всех функций организации в рабочее состояние. Ключевые элементы этого процесса должны обеспечивать применение и тестирование необходимых планов и средств и включение в них информации, бизнес-процессов, информационных систем и сервисов, речевой связи и передачи данных, персонала и физических устройств.

3.2 **Событие информационной безопасности** (information security event): Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

3.3 **Инцидент информационной безопасности** (information security incident): Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации операций и создания угрозы ИБ.

ПРИМЕЧАНИЕ Примеры инцидентов ИБ приведены в разделе 6.

3.4 **Группа реагирования на инциденты информационной безопасности (ГРИИБ)** (Information Security Incident Response Team (ISIRT)): Группа обученных и пользующихся доверием членов организации.

3.5 **Информационная безопасность (ИБ)**: Комплекс правовых, организационных и технических мероприятий, направленных на сохранение, предотвращение неправомерного доступа к электронным информационным ресурсам, информационным системам, включая незаконные действия по получению, копированию, распространению, искажению, уничтожению или блокированию информации.

ПРИМЕЧАНИЕ Данная группа обрабатывает инциденты ИБ во время их жизненного цикла и иногда может дополняться внешними экспертами, например, из общепризнанной группы реагирования на компьютерные инциденты или компьютерной группы быстрого реагирования (КГБР).

3.6 **Информационная технология (ИТ):** Совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу и распространение информации.

4 Общие положения

4.1 Цели

В качестве основы общей стратегии ИБ организации необходимо использовать структурный подход к менеджменту инцидентов ИБ. Целями такого подхода являются обеспечение условий для:

- определения инцидентов организации, связанных с ИБ* и их эффективной обработкой,
- оценки идентифицированных инцидентов ИБ и реагирования на них наиболее целесообразным и результативным способом;
- минимизации воздействий инцидентов ИБ на организацию и ее деятельность с

* События ИБ могут быть результатом случайных или преднамеренных попыток компрометации защитных мер ИБ, но в большинстве случаев событие ИБ само по себе не означает, что попытка в действительности была успешной и, следовательно, каким-то образом повлияла на конфиденциальность, целостность и (или) доступность, то есть не все события ИБ будут отнесены к категории инцидентов ИБ.

помощью соответствующих защитных мер, являющихся частью процесса реагирования на инцидент, иногда наряду с применением соответствующих элементов плана (-ов) обеспечения непрерывности деятельности организации;

- извлечения уроков по превращению инцидентов ИБ и их менеджмента с целью повышения шансов по их недопущению в будущем, улучшения внедрения и использования защитных мер ИБ, улучшения общей системы менеджмента инцидентов ИБ.

4.2 Этапы

Для достижения целей в соответствии с Разделом 4.1 менеджмент инцидентов ИБ подразделяют на четыре отдельных этапа:

1) планирование и подготовка;
2) использование;
3) анализ;
4) улучшение.

ПРИМЕЧАНИЕ Этапы менеджмента инцидентов ИБ аналогичны процессам модели PDCA, используемой в стандартах серии [4].

Основное содержание этих этапов показано на Рисунке 1.

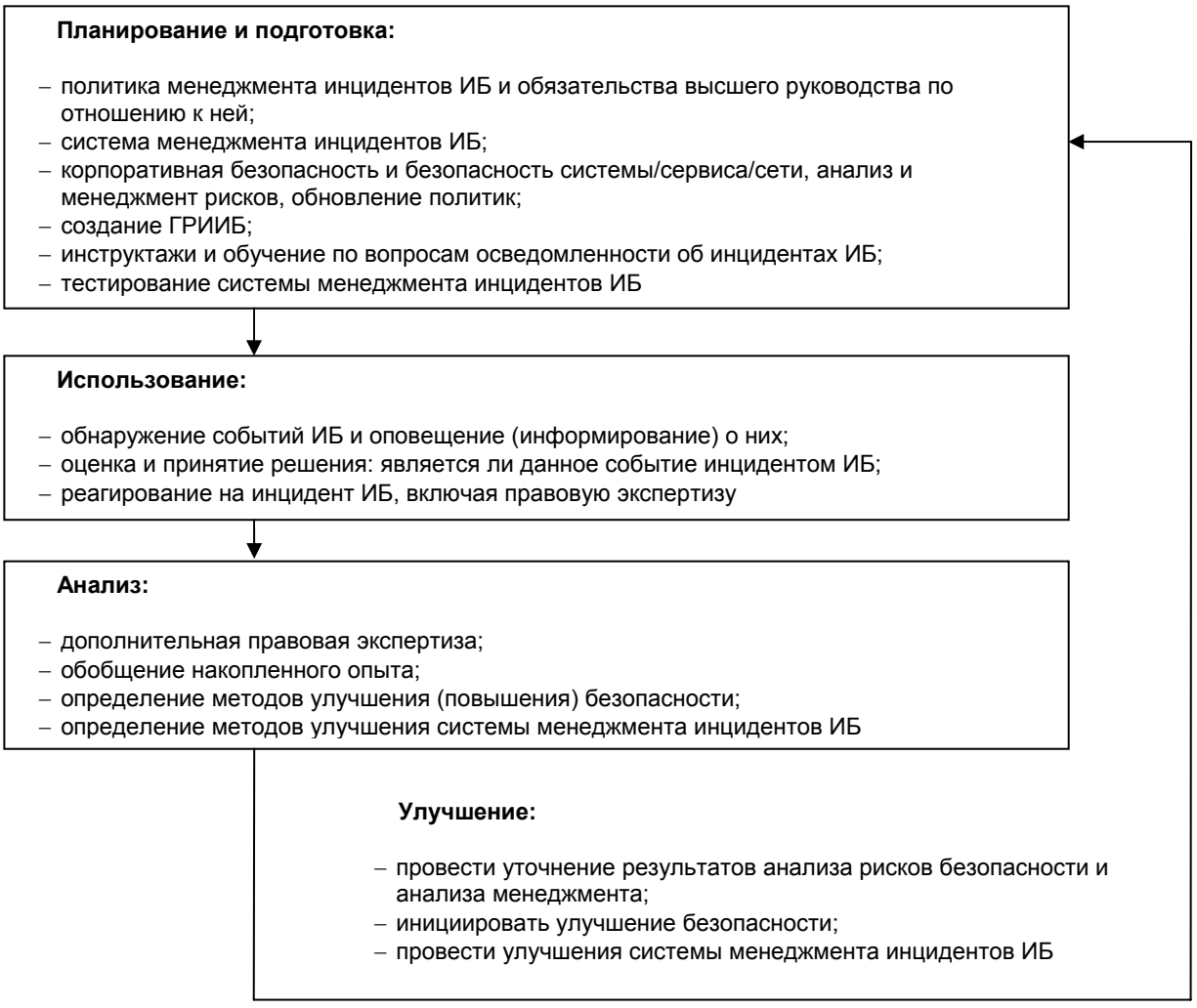


Рисунок 1 — Этапы менеджмента инцидентов ИБ

4.2.1 Планирование и подготовка

Эффективный менеджмент инцидентов ИБ нуждается в надлежащем планировании и подготовке. Для обеспечения эффективности реакции на инциденты ИБ необходимо:

- разработать и документировать политики менеджмента инцидентов ИБ, а также получить очевидную поддержку этой политики заинтересованными сторонами и, в особенности, высшего руководства;

- разработать и в полном объеме документировать систему менеджмента инцидентов ИБ для поддержки политики менеджмента инцидентов ИБ. Формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты ИБ, а также градации шкалы* серьезности инцидентов должны быть отражены в документации на конкретную систему. (В некоторых организациях такая система может называться «Планом реагирования на инциденты ИБ»);

- обновить политики менеджмента ИБ и рисков на всех уровнях, то есть на корпоративном и для каждой системы, сервиса и сети отдельно с учетом системы менеджмента инцидентов ИБ;

- создать в организации соответствующее структурное подразделение менеджмента инцидентов ИБ, то есть ГРИИБ, с заданными обязанностями и ответственностью персонала, способного адекватно реагировать на все известные типы инцидентов ИБ. В большинстве организаций ГРИИБ является группой, состоящей из специалистов по конкретным направлениям деятельности, например, при отражении атак вредоносной программы привлекают специалиста по инцидентам подобного типа;

- ознакомить весь персонал организации посредством инструктажей и (или) иными способами с существованием системы менеджмента инцидентов ИБ, ее преимуществами и с надлежащими способами сообщения о событиях ИБ. Необходимо проводить соответствующее обучение персонала, ответственного за управление системой менеджмента инцидентов ИБ, лиц, принимающих решения по определению того, являются ли события инцидентами, и лиц, исследующих инциденты;

- тщательно тестировать систему менеджмента инцидентов ИБ. Этап «Планирование и подготовка» — в соответствии с разделом 7.

4.2.2 Использование системы менеджмента инцидентов информационной безопасности

При использовании системы менеджмента инцидентов ИБ необходимо осуществить следующие процессы:

- обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);

- сбор информации, связанной с событиями ИБ, и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;

- реагирование на инциденты ИБ:

- немедленно, в реальном или почти реальном масштабе времени;

- если инциденты ИБ находятся под контролем, выполнить менее срочные действия (например, способствующие полному восстановлению после катастрофы);

- если инциденты ИБ не находятся под контролем, то выполнить «антикризисные» действия (например, вызвать пожарную команду/подразделение или инициировать выполнение плана непрерывности деятельности организации);

---

* Необходимо иметь определенную шкалу серьезности инцидентов с соответствующей классификацией. Эта шкала может состоять, например, из двух положений: «значительные» и «незначительные». Выбор градаций шкалы должен основываться на фактических или предполагаемых негативных воздействиях на операции.

- сообщить о наличии инцидентов ИБ и любые относящиеся к ним подробности персоналу своей организации, а также персоналу сторонних организаций (что может включить в себя, по мере необходимости, распространение подробностей инцидента с целью дальнейшей оценки и (или) принятия решений);
- правовую экспертизу;
- надлежащую регистрацию всех действий и решений для последующего анализа;
- разрешение проблемы инцидентов.

Этап «Использование» — в соответствии с Разделом 8.

4.2.3 Анализ

После разрешения/закрытия инцидентов ИБ необходимо предпринять следующие действия по анализу состояния ИБ:

- провести дополнительную правовую экспертизу (при необходимости);
- изучить уроки, извлеченные из инцидентов ИБ;
- определить улучшения для внедрения защитных мер ИБ, полученные из уроков, извлеченных из одного или нескольких инцидентов ИБ;
- определить улучшения для системы менеджмента инцидентов ИБ в целом, учитывая уроки, извлеченные из результатов анализа качества предпринимаемого подхода (например, из анализа результативности процессов, процедур, форм отчета и (или) организации).

Этап «Анализ» — в соответствии с Разделом 9.

4.2.4 Улучшение

Процессы менеджмента инцидентов ИБ являются итеративными, с постоянным внесением улучшений с течением времени в ряд элементов ИБ. Эти улучшения предлагаются на основе данных об инцидентах ИБ и реагировании на них, а также данных о динамике тенденций. Этап «Улучшение» включает в себя:

- пересмотр имеющихся результатов анализа рисков ИБ и анализ менеджмента организации;
- улучшение системы менеджмента инцидентов ИБ и ее документации;
- инициирование улучшений в области безопасности, включая внедрение новых и (или) обновленных защитных мер ИБ.

Этап «Улучшение» — в соответствии с Разделом 10.

5 Преимущества структурного подхода и ключевые вопросы менеджмента инцидентов информационной безопасности

В данном разделе представлена информация:

- о преимуществах, получаемых от качественной системы менеджмента инцидентов ИБ;
- о ключевых вопросах, которые необходимо рассмотреть с целью убеждения в этих преимуществах высшего корпоративного руководства и персонала, предоставляющего отчеты в систему и получающего от нее информацию.

5.1 Преимущества

Любая организация, использующая структурный подход к менеджменту инцидентов ИБ, может извлечь из него значительные преимущества, которые можно объединить в следующие группы:

- улучшение ИБ;
- снижение негативных воздействий на деятельность организации, например, прерывание деятельности организации и финансовые убытки как последствия инцидентов ИБ;

- усиление внимания к вопросам предотвращения инцидентов;
- усиление внимания к установлению приоритетов и сбору доказательств;
- вклад в обоснование бюджета и ресурсов;
- обновление результатов менеджмента и анализа рисков на более высоком уровне;
- предоставление материала для программ повышения осведомленности и обучения в области ИБ;
- предоставление входных данных для анализа политики ИБ и соответствующей документации. Каждое из этих преимуществ рассматривается ниже.

5.1.1 Улучшение безопасности

Структурный процесс обнаружения, оповещения, оценки и менеджмента инцидентов и событий ИБ позволяет быстро идентифицировать любое событие или инцидент ИБ и реагировать на них, тем самым улучшая общую безопасность за счет быстрого определения и реализации правильного решения, а также обеспечивая средства предотвращения подобных инцидентов ИБ в будущем.

5.1.2 Снижение негативных воздействий на деятельность организации

Структурный подход к менеджменту инцидентов ИБ может способствовать снижению уровня негативных воздействий, связанных с инцидентами ИБ, на деятельность организации. Последствия этих воздействий могут включать в себя немедленные финансовые убытки, а также долговременные потери, возникающие от ущерба, нанесенного репутации и кредитоспособности организации.

5.1.3 Усиление внимания к предотвращению инцидентов

Использование структурного подхода к менеджменту инцидентов ИБ может способствовать усилению внимания к предотвращению инцидентов внутри организации. Анализ данных, связанных с инцидентами, позволяет определить модели и тенденции появления инцидентов, тем самым способствуя усилению внимания к предотвращению инцидентов и, следовательно, определению соответствующих действий по предотвращению возникновения инцидентов.

5.1.4 Усиление внимания к системе установления приоритетов и свидетельств

Структурный подход к менеджменту инцидентов ИБ создает прочную основу для системы установления приоритетов при проведении расследований инцидентов ИБ.

При отсутствии четких процедур существует риск того, что расследования проводятся в непостоянном режиме, когда реагирование на инциденты осуществляется по мере их появления или как реакция на распоряжение соответствующего руководителя. Это может помешать проведению расследования в последовательности, соответствующей идеальному установлению приоритетов там, где оно действительно необходимо.

Четкие процедуры расследования инцидентов могут обеспечить правильность и правовую допустимость сбора данных, и их обработки. Это имеет большое значение в случае инициирования судебного преследования или дисциплинарного разбирательства. Однако следует признать вероятность того, что действия, необходимые для восстановления после инцидента ИБ, могут подвергнуть риску целостность собранных свидетельств.

5.1.5 Бюджет и ресурсы

Хорошо продуманный структурный подход к менеджменту инцидентов ИБ способствует обоснованию и упрощению распределения бюджетов и ресурсов внутри подразделений организации. Кроме того, выгоды получает и сама система менеджмента

инцидентов ИБ. Такие выгоды связаны со следующими условиями:

- использованием менее квалифицированного персонала для идентификации и фильтрации ложных сигналов тревоги;
- применением навыков квалифицированного персонала в самом необходимом направлении;
- привлечением квалифицированного персонала только для тех процессов, где требуются его навыки, и только на той стадии процесса, где его содействие необходимо.

Кроме того, структурный подход к менеджменту инцидентов ИБ может включать в себя процедуру приостановки «отметки времени» с целью возможности выполнения «количественных» оценок обработки инцидентов ИБ в организации. Это делает возможным, например, предоставление информации о времени разрешения инцидентов с различными приоритетами на различных платформах. При наличии слабых мест в процессе менеджмента инцидентов ИБ эти слабые места также должны быть идентифицируемыми.

5.1.6 Менеджмент и анализ рисков ИБ

Использование структурного подхода к менеджменту инцидентов ИБ способствует:

- сбору более качественных данных для идентификации и определения характеристик различных типов угроз и связанных с ними уязвимостей;
- предоставлению данных о частоте возникновения идентифицированных типов угроз.

Полученные данные о негативных последствиях инцидентов ИБ для деятельности организации будут полезны для анализа этих последствий. Данные о частоте возникновения различных типов угроз намного повысят качество оценки угроз. Аналогично, данные об уязвимостях намного повысят качество будущих оценок уязвимостей.

Вышеупомянутые данные значительно улучшат результаты анализа менеджмента и анализа рисков ИБ.

5.1.7 Осведомленность в вопросах ИБ

Структурный подход к менеджменту инцидентов ИБ предоставляет узконаправленную информацию о программах обеспечения осведомленности в вопросах ИБ. Эта информация является источником реальных примеров, на которых можно показать, что инциденты ИБ действительно происходят именно в данной организации, а не где-либо еще. Таким образом, можно продемонстрировать выгоды быстрого получения информации о решениях. Более того, подобная осведомленность в вопросах ИБ позволяет снизить вероятность ошибки, возникновения паники и (или) растерянности у людей в случае появления инцидента ИБ.

5.1.8 Входные данные для анализа политики ИБ

Информация, предоставляемая системой менеджмента инцидентов ИБ, может обеспечить ценные входные данные для анализа результативности и последующего улучшения политик ИБ (и другой документации, связанной с ИБ). Это относится к политикам и другой документации, как на уровне организации, так и для отдельных систем, сервисов и сетей.

5.2 Ключевые вопросы

Наличие обратной связи, по которой поступает информация о том, как осуществляется менеджмент инцидентов ИБ, помогает сохранять нацеленность действий персонала на борьбу с реальными рисками для систем, сервисов и сетей организации. Эта

важная обратная связь не может быть эффективно реализована через процесс реагирования на инциденты ИБ, поскольку инциденты ИБ происходят нерегулярно. Обратная связь может быть более результативной при наличии структурированной, хорошо продуманной системы менеджмента инцидентов ИБ, применяющей общую структуру для всех подразделений организации. Данная общая структура должна непрерывно обеспечивать получение от системы как можно более полных результатов и представлять собой надежную основу для быстрого определения возможных условий возникновения инцидента ИБ до его появления, а также выдавать соответствующие сигналы оповещения.

Менеджмент и аудит системы менеджмента ИБ обеспечивают основу доверия, необходимого для расширения совместной работы с персоналом и снижения недоверия в отношении сохранения анонимности, безопасности и доступности полезных результатов. Например, руководство и персонал организации должны быть уверены в том, что сигналы оповещения дадут своевременную, точную и полную информацию относительно ожидаемого инцидента.

При внедрении систем менеджмента инцидентов ИБ организациям следует избегать таких потенциальных проблем, как отсутствие положительных результатов и беспокойства по поводу вопросов, связанных с проблемами неприкосновенности персональных данных. Необходимо убедить заинтересованные стороны в том, что для предотвращения появления вышеупомянутых проблем были предприняты определенные шаги.

Таким образом, для построения оптимальной системы менеджмента инцидентов ИБ нужно рассмотреть ряд ключевых вопросов, включая:

- обязательства руководства;
- осведомленность;
- правовые и нормативные аспекты;
- эксплуатационную эффективность и качество;
- анонимность;
- конфиденциальность;
- независимость деятельности ГРИИБ;
- типологию.

Каждый из этих вопросов будет рассмотрен ниже.

5.2.1 Обязательства руководства

Для принятия структурного подхода к менеджменту инцидентов ИБ жизненно необходима постоянная поддержка со стороны руководства. Персонал организации должен распознавать инциденты ИБ и знать свои действия при их возникновении, а также осознавать большие преимущества структурного подхода для организации. Однако этого может быть недостаточно при отсутствии поддержки со стороны руководства. Необходимо донести до руководства, что организация должна выполнять обязательства по обеспечению ресурсами и поддержке способности реагирования на инциденты.

5.2.2 Осведомленность

Другой важной проблемой принятия структурного подхода к менеджменту инцидентов ИБ является осведомленность. Несмотря на потребность в пользователях для участия в работе организации, вряд ли можно рассчитывать на их эффективное участие в работе организации при отсутствии осведомленности о том, какую выгоду они и их подразделение получат от участия в структурном подходе к управлению инцидентами информационной безопасности.

Любая система менеджмента инцидентов ИБ должна сопровождаться документом с

определением программы обеспечения осведомленности, включающим в себя:

- преимущества структурного подхода к менеджменту инцидентов ИБ как для организации, так и для ее персонала;
- информацию об инцидентах, хранящуюся в базе данных событий и (или) инцидентов ИБ, и выходные данные из нее;
- стратегию и механизмы для программы обеспечения осведомленности, которая в зависимости от типа организации может быть отдельной программой или частью более широкой программы осведомленности в вопросах ИБ.

5.2.3 Правовые и нормативные аспекты

В политике менеджмента инцидентов ИБ и соответствующей системе необходимо учитывать следующие правовые и нормативные аспекты менеджмента инцидентов ИБ.

1) Обеспечение адекватной защиты персональных данных и неприкосновенность персональной информации.

В странах, где существует специальное законодательство, защищающее конфиденциальность и целостность данных, оно часто ограничено контролем за персональными данными. Поскольку инциденты ИБ обычно возникают в результате деятельности персонала или посторонних лиц, то может потребоваться соответствующая регистрация информации личного характера и управление ею. Следовательно, при структурном подходе к менеджменту инцидентов ИБ следует учитывать необходимость в соответствующей защите персональных данных, а также следующие условия:

- лица, имеющие доступ к персональным данным, не должны лично знать тех людей, информация о которых изучается;
- лица с доступом к личным данным должны подписать соглашение об их неразглашении до того, как получат доступ к ним;
- персональные данные должны использоваться исключительно для тех целей, для которых они были получены, то есть для расследования инцидентов ИБ.

2) Соответствующее хранение записей.

Некоторые законы других стран требуют от компаний ведения соответствующих записей своей деятельности для анализа в процессе ежегодного аудита организации. Такие же требования существуют для различных организаций. В некоторых странах от организаций требуется составление отчетов или создание архивов для различных органов (например, в случае совершения серьезного преступления или проникновения в правительственную систему, содержащую конфиденциальную информацию).

3) Наличие защитных мер для обеспечения выполнения коммерческих договорных обязательств.

При наличии обязывающих требований по предоставлению услуг по менеджменту инцидентов ИБ (например, требования ко времени реагирования) организация должна предусматривать обеспечение соответствующей ИБ в целях обеспечения выполнения этих обязательств при любых обстоятельствах (в связи с этим в случае заключения организацией контракта со сторонней организацией (см. Раздел 7.5.4), например, КГБР, необходимо включение всех необходимых требований, наряду с временем реагирования, в контракт со сторонней организацией).

4) Правовые вопросы, связанные с политиками и процедурами.

Необходима проверка политик и процедур, связанных с системой менеджмента инцидентов ИБ, на предмет наличия правовых и нормативных проблем, например, имеются ли уведомления о дисциплинарных взысканиях и (или) судебном преследовании сотрудников, виновных в создании инцидентов, так как в некоторых странах увольнение сотрудников является довольно сложным процессом.

5) Проверка на законность непризнания ответственности.

Все заявления об ограничении ответственности за действия, предпринятые группой менеджмента инцидентов ИБ или внешним вспомогательным персоналом, должны быть проверены на законность.

6) Включение в контракты со сторонним персоналом всех необходимых аспектов.

Контракты со сторонним вспомогательным персоналом, например, КГБР, должны тщательно проверяться на предмет внесения в контракт ответственности за нарушение обязательств по неразглашению, доступности услуг и последствия неправильных консультаций.

7) Соглашения о неразглашении конфиденциальной информации.

От членов группы менеджмента инцидентов ИБ может потребоваться подписание соглашения о неразглашении конфиденциальной информации как при устройстве на работу, так и при увольнении. В некоторых странах такие соглашения могут не иметь юридической силы. Данный аспект необходимо подвергать проверке.

8) Исполнение требований правоприменяющих органов.

Необходимо обеспечить ясность в вопросах, связанных с возможностью того, что правоприменяющие органы на законном основании могут затребовать информацию от системы менеджмента инцидентов ИБ. В некоторых случаях может потребоваться ясность о минимальном уровне, определяемом законом, на котором инциденты необходимо документировать, и о сроке хранения этой документации.

9) Ясность в вопросах ответственности.

Необходимо уточнить вопросы потенциальной ответственности и необходимые соответствующие защитные меры. Ниже приведены примеры событий, имеющих отношение к возложению ответственности:

- если инцидент ИБ может повлиять на деятельность другой организации (например, раскрытие совместно используемой информации), которая вовремя не оповещается и в результате несет ущерб;
- если в продукции обнаружена новая уязвимость без уведомления об этом поставщика, что привело к возникновению серьезного связанного с этой уязвимостью инцидента, в результате которого значительно пострадали одна или несколько организаций;
- если в какой-либо стране, где от организаций требуется информирование или создание архивов для правоохранительных органов в отношении всех случаев, которые могут быть связаны с тяжким преступлением или проникновением в правительственную систему, содержащую информацию ограниченного доступа или элементы критически важной национальной инфраструктуры, соответствующие требования не выполнены;
- если информация раскрыта и появилось указание на причастность некоторого лица или организации к атаке на информационные ресурсы организации. Этот факт может нанести ущерб репутации и деятельности конкретных лиц или организации;
- если раскрыта информация, что в определенном элементе программного обеспечения произошел сбой, но впоследствии эта информация оказалась ложной.

10) Специальные нормативные требования.

Об инцидентах ИБ следует информировать соответствующий контрольный орган, если это предусмотрено специальными и нормативными требованиями, например, как это предусмотрено в атомной промышленности.

11) Судебные преследования или внутренние дисциплинарные разбирательства.

Для успешного судебного преследования или проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников, независимо от того, были ли эти атаки техническими или физическими, необходимо применять соответствующие меры защиты ИБ, включая доказуемо защищенные от внесения изменений журналы аудита. Для обеспечения успешного судебного преследования или

проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников, независимо от того, были ли эти атаки техническими или физическими, необходимо собрать свидетельства для судов или других административных органов. Необходимо показать, что:

- документация не подвергалась искажениям и является полной;
- копии электронного свидетельства доказуемо идентичны оригиналам;
- все системы ИТ, от которых были получены свидетельства, во время регистрации работали в штатном режиме.

12) Правовые аспекты, связанные с методами мониторинга

Последствия использования методов мониторинга должны быть рассмотрены в контексте национального законодательства. Законность различных методов может меняться в зависимости от страны. Например, в некоторых странах необходимо информировать людей о ведении мониторинга, в том числе методами наблюдения. Необходимо учесть несколько факторов, определяющих, кто (что) подвергается мониторингу, каким образом они (оно) подвергаются мониторингу и когда проводится мониторинг. Необходимо также отметить, что мониторинг/наблюдение в контексте систем обнаружения вторжений (СОВ) специально рассматривается в [3].

13) Подготовка правил пользования информационными ресурсами и ознакомление с ними.

Порядок использования информационных систем и ресурсов в организации должен быть определен, документирован и доведен до сведения всего предполагаемого персонала (например, персонал необходимо проинформировать о допустимой политике использования и потребовать письменное подтверждение понимания и принятия ими этой политики при устройстве на работу в организацию или получении доступа к информационным системам).

5.2.4 Эффективность эксплуатации и качество

Эффективность эксплуатации и качество структурного подхода к менеджменту инцидентов ИБ зависит от ряда факторов, включающих в себя обязательность уведомления об инцидентах, качество уведомления, простоту использования, быстродействие и обучение. Некоторые из этих факторов связаны с обеспечением осведомленности пользователей о важности менеджмента инцидентов ИБ и их мотивированностью сообщать об инцидентах. Что касается быстродействия, то время, используемое на сообщение об инциденте ИБ, — не единственный фактор, важно также учитывать время, необходимое для обработки данных и распространения обработанной информации (особенно в случае с сигналами аварийности).

Для минимизации задержек соответствующие программы обеспечения осведомленности и обучения пользователей должны дополняться поддержкой по «горячей линии», которая обеспечивается персоналом, осуществляющим менеджмент инцидентов ИБ.

5.2.5 Анонимность

Вопрос обеспечения анонимности является основополагающим для успеха менеджмента инцидентов ИБ. Пользователи должны быть уверены, что информация об инцидентах ИБ, которую они сообщают, полностью защищена, а при необходимости обезличена, с тем, чтобы ее невозможно было связать с их организацией или ее подразделением без их согласия.

Система менеджмента инцидентов ИБ должна учитывать ситуации, когда важно обеспечить анонимность лица или организации, сообщающих о потенциальных инцидентах ИБ при особых обстоятельствах. У каждой организации должны быть

положения, в которых четко разъяснялись бы важность сохранения анонимности или ее отсутствия для лиц и организаций, сообщающих о потенциальном инциденте ИБ. ГРИИБ может потребоваться дополнительная информация, не сообщенная изначально информирующим об инциденте лицом или организацией. Более того, важная информация об инциденте ИБ может быть получена от первого обнаружившего его лица.

5.2.6 Конфиденциальность

В системе менеджмента инцидентов ИБ может содержаться конфиденциальная информация, и лицам, занимающимся инцидентами, может потребоваться доступ к ней. Поэтому во время обработки необходимо обеспечивать анонимность этой информации, или персонал должен подписать соглашение о конфиденциальности (неразглашении) при получении доступа к ней. Если события ИБ регистрируют через общую систему менеджмента проблем, то конфиденциальные подробности, возможно, придется опустить.

Кроме того, система менеджмента инцидентов ИБ должна обеспечивать контроль за передачей сообщений об инцидентах сторонними организациями, включая СМИ, партнеров по бизнесу, потребителей, регулирующие организации и общественность.

5.2.7 Независимость деятельности группы реагирования на инциденты информационной безопасности

Группа менеджмента инцидентов ИБ должна быть способна эффективно удовлетворять функциональные, финансовые, правовые и политические потребности конкретной организации и быть в состоянии соблюдать осторожность при управлении инцидентами ИБ. Деятельность группы менеджмента инцидентов ИБ должна также подвергаться независимому аудиту с целью проверки эффективности ее функционирования. Эффективным способом реализации независимости контроля является отделение цепочки сообщений о реагировании на инцидент ИБ от общего оперативного руководства и возложение на вышестоящего руководителя непосредственных обязанностей по управлению реагированием на инциденты. Финансирование работы группы, во избежание чрезмерного влияния на нее со стороны, также должно быть отдельным.

5.2.8 Типология

Общая типология, отражающая структуру подхода к менеджменту инцидентов ИБ, является одним из ключевых факторов обеспечения последовательных надежных результатов. Типология*, наряду с общепринятыми метриками и стандартной структурой баз данных, обеспечивает возможность сравнивать результаты, улучшать предупреждающую информацию и получать более точное представление об угрозах для информационных систем и их уязвимостях.

6 Примеры инцидентов информационной безопасности и их причин

Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. Инциденты ИБ, о которых не было

* Определение общей типологии не является целью настоящего стандарта. Рекомендуется обращение к другим источникам за этой информацией.

сообщено, но которые были определены как инциденты, расследовать невозможно и защитных мер для предотвращения повторного появления этих инцидентов применить нельзя.

Ниже приведены некоторые примеры инцидентов ИБ и их причин, которые даются только с целью разъяснения. Важно заметить, что эти примеры не являются исчерпывающими.

6.1 Отказ в обслуживании

Отказ в обслуживании является обширной категорией инцидентов ИБ, имеющих одну общую черту. Подобные инциденты ИБ приводят к неспособности систем, сервисов или сетей продолжать функционирование с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

Существует два основных типа инцидентов ИБ, связанных с отказом в обслуживании, создаваемых техническими средствами: уничтожение ресурсов и истощение ресурсов.

Некоторыми типичными примерами таких преднамеренных технических инцидентов ИБ «отказ в обслуживании» являются:

- зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;
- передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;
- одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы (то есть замедление их работы, блокирование или разрушение).

Одни технические инциденты ИБ «отказ в обслуживании» могут возникать случайно, например, в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного программного обеспечения, а другие - преднамеренно. Одни технические инциденты ИБ «отказ в обслуживании» инициируются намеренно с целью разрушения системы, сервиса и снижения производительности сети, тогда как другие — всего лишь побочными продуктами иной вредоносной деятельностью. Например, некоторые наиболее распространенные методы скрытого сканирования и идентификации могут приводить к полному разрушению старых или ошибочно сконфигурированных систем или сервисов при их сканировании. Следует заметить, что многие преднамеренные технические инциденты типа «отказ в обслуживании» часто инициируются анонимно (то есть источник атаки неизвестен), поскольку злоумышленник обычно не получает информации об атакуемой сети или системе.

Инциденты ИБ «отказ в обслуживании», создаваемые нетехническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться, например, следующими факторами:

- нарушениями систем физической защиты, приводящими к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;
- случайным нанесением ущерба аппаратуре и (или) ее местоположению от огня или воды/наводнения;
- экстремальными условиями окружающей среды, например, высокой температурой (вследствие выхода из строя системы кондиционирования воздуха);
- неправильным функционированием или перегрузкой системы;
- неконтролируемыми изменениями в системе;
- неправильным функционированием программного или аппаратного обеспечения.

6.2 Сбор информации

Инциденты ИБ «сбор информации» подразумевают действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки. Подобные инциденты ИБ предполагают проведение разведки с целью определения:

- наличия цели, получения представления об окружающей ее сетевой топологии и о том, с кем обычно эта цель связана обменом информации;
- потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

- сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);
- отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;
- зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;
- сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов (например, электронная почта, протокол FTP, сеть) и версий программного обеспечения этих сервисов;
- сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов (горизонтальное сканирование).

В некоторых случаях технический сбор информации расширяется и переходит в несанкционированный доступ, если, например, злоумышленник при поиске уязвимости пытается получить несанкционированный доступ. Обычно это осуществляется автоматизированными средствами взлома, которые не только производят поиск уязвимости, но и автоматически пытаются использовать уязвимые системы, сервисы и (или) сети.

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят к:

- прямому или косвенному раскрытию или модификации информации;
- хищению интеллектуальной собственности, хранимой в электронной форме;
- нарушению учетности, например, при регистрации учетных записей;
- неправильному использованию информационных систем (например, с нарушением закона или политики организации).

Инциденты могут вызываться, например, следующими факторами:

- нарушениями физической защиты безопасности, приводящими к несанкционированному доступу к информации и хищению устройств, хранения данных, содержащих значимые данные, например, ключи шифрования;
- неудачно и (или) неправильно конфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

6.3 Несанкционированный доступ

Несанкционированный доступ, как тип инцидента, включает в себя инциденты, не вошедшие в первые два типа. Главным образом этот тип инцидентов состоит из несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети. Некоторые примеры несанкционированного доступа с

помощью технических средств включают в себя:

- попытки извлечь файлы с паролями;
- атаки переполнения буфера с целью получения привилегированного (например, на уровне системного администратора) доступа к сети;
- использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;
- попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя или администратора.

Инциденты несанкционированного доступа, создаваемые нетехническими средствами, которые приводят к прямому или косвенному раскрытию или модификации информации, нарушениям учетности или неправильному использованию информационных систем, могут вызываться следующими факторами:

- разрушением устройств физической защиты с последующим несанкционированным доступом к информации;
- неудачной и (или) неправильной конфигурацией операционной системы вследствие неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения, приводящих к результатам, подобным тем, которые описаны в последнем абзаце Раздела 6.2.

7 Этап «Планирование и подготовка»

Этап «Планирование и подготовка» менеджмента инцидентов ИБ включает в себя:

- документирование политики обработки сообщений о событиях и инцидентах ИБ и системе, соответствующей этой политике (включая родственные процедуры);
- создание подходящей структуры менеджмента инцидентов ИБ в организации и подбор соответствующего персонала;
- создание программы обучения и проведения инструктажа с целью обеспечения осведомленности о менеджменте инцидентов.

После завершения этого этапа организация должна быть полностью готова к надлежащей обработке инцидентов ИБ.

7.1 Общее представление о менеджменте инцидентов информационной безопасности

Для результативного и эффективного ввода менеджмента инцидентов ИБ в эксплуатацию после необходимого планирования следует выполнить ряд подготовительных действий. Эти подготовительные действия включают в себя:

- формулирование и разработку политики менеджмента инцидентов ИБ, а также утверждение этой политики высшим руководством организации (см. Раздел 7.2);
- разработку и документирование подробной системы менеджмента инцидентов ИБ (см. Раздел 7.3). Документация системы менеджмента инцидентов ИБ должна содержать следующие элементы:
- шкалу серьезности для классификации инцидентов ИБ. Как указано в Разделе 4.2.1, такая шкала может состоять, например, из двух положений: «значительные» и «незначительные». В любом случае положение шкалы основано на фактическом или предполагаемом ущербе для операций организации;
- формы докладов[*] о событиях[**] и инцидентах[***] ИБ (примеры форм приведены в

[*] Если возможно, эти формы должны быть представлены в электронном виде (например, на защищенной веб-странице) и связаны с базой данных, хранящей электронную информацию о событиях/инцидентах ИБ. В настоящее время бумажная технология требовала бы слишком много времени и

Приложении А), соответствующие документированные процедуры и действия, связанные со ссылками на нормальные процедуры использования данных и системы, сервисов и (или) сетевого резервирования, планами обеспечения непрерывности деятельности организации;

- операционные процедуры для ГРИИБ с документированными обязанностями и распределением функций среди назначенных ответственных лиц[****] для осуществления различных видов деятельности, например, таких как:

- отключение атакованной системы, сервиса и (или) сети при определенных обстоятельствах по согласованию с соответствующим руководством ИТ и (или) организации и в соответствии с предварительным соглашением;

- оставление атакованной системы, сервиса и (или) сети в работающем состоянии и подсоединенной к сети;

- ведение мониторинга потока входящих, выходящих или находящихся в атакованной системе, сервисе и (или) сети данных;

- активация нормальных дублирующих процедур и действий по планированию непрерывности деятельности согласно политике безопасности системы, сервиса и (или) сети;

- ведение мониторинга и организация защищенного хранения свидетельств в электронном виде на случай их востребования для судебного разбирательства или дисциплинарного расследования внутри организации;

- передача подробностей об инциденте ИБ сотрудникам своей организации и сторонним лицам или организациям;

- тестирование функционирования системы менеджмента инцидентов ИБ, ее процессов и процедур (см. Раздел 7.3.5);

- обновление политик менеджмента и анализа рисков ИБ, корпоративной политики ИБ, специальных политик ИБ для систем, сервисов и (или) сетей для включения ссылок на менеджмент инцидентов ИБ и обеспечение регулярного пересмотра этих политик в контексте выходных данных системы менеджмента инцидентов ИБ (см. Раздел 7.4);

- создание ГРИИБ с соответствующей программой обучения ее персонала (см. Раздел 7.5);

- технические и другие средства поддержки системы менеджмента инцидентов безопасности ИБ (и деятельности ГРИИБ) (см. Раздел 7.6);

- проектирование и разработка программы обеспечения осведомленности о менеджменте инцидентов ИБ (см. Раздел 7.7), ознакомление с этой программой всего персонала организации (и повторное проведение ознакомления в дальнейшем в случае кадровых изменений).

В следующих подразделах приведено описание каждого вида этой деятельности, включая содержание каждого требуемого документа.

была бы неэффективной.

[**] Форму заполняет лицо, принимающее сообщение (то есть не член группы менеджмента инцидентов ИБ).

[***] Эта форма используется персоналом менеджмента инцидентов ИБ для пополнения первоначальной информацией о событии ИБ текущего ведения записей оценок инцидента и пр. до полного разрешения инцидента. На каждой стадии в базу данных событий/инцидентов ИБ включаются обновления. Запись в базе данных, содержащая «заполненную» форму или сведения о событиях/инцидентах ИБ, далее используется в деятельности по разрешению инцидента.

[****] В небольших организациях одно и то же лицо может выполнять несколько функций.

7.2 Политика менеджмента инцидентов информационной безопасности

7.2.1 Назначение политики

Политика менеджмента инцидентов ИБ предназначена для всего персонала, имеющего авторизованный доступ к информационным системам организации и местам их расположения.

7.2.2 Лица, связанные с политикой менеджмента инцидентов информационной безопасности

Политика менеджмента инцидентов ИБ утверждается старшим должностным лицом организации с документально подтвержденными полномочиями, полученными от высшего руководства. Политика должна быть доступна для каждого сотрудника и подрядчика и доведена через инструктаж и обучение с целью обеспечения их осведомленности в области ИБ (см. Раздел 7.7).

7.2.3 Содержание политики менеджмента инцидентов информационной безопасности

Политика менеджмента инцидентов ИБ должна включать в себя следующие вопросы:

- значимость менеджмента инцидентов ИБ для организации, а также обязательства высшего руководства относительно поддержки менеджмента и его системы;
- общее представление об обнаружении событий ИБ, оповещении о них и сборе соответствующей информации, а также о путях использования этой информации для определения инцидентов ИБ. Это общее представление должно содержать перечень возможных событий ИБ, а также информацию о том, как сообщать о ней, что, где и кому сообщать, а также как обращаться с совершенно новыми событиями ИБ;
- общее представление об оценке инцидентов ИБ, включая перечень ответственных лиц, необходимые для выполнения действия, уведомления об инцидентах и дальнейшие действия ответственных лиц;
- краткое изложение действий после подтверждения того, что событие ИБ является инцидентом ИБ. Эти действия представляют:
- немедленное реагирование;
- правовую экспертизу;
- передачу информации соответствующему персоналу или сторонним организациям;
- проверку, находится ли инцидент ИБ под контролем;
- дальнейшее реагирование;
- объявление «кризисной ситуации»;
- определение критериев усиления реагирования на инциденты ИБ;
- определение ответственного за инцидент лица;
- ссылку на необходимость правильной регистрации всех действий для дальнейшего и непрерывного мониторинга с целью обеспечения защищенного хранения свидетельств в электронном виде на случай их востребования для судебного разбирательства или дисциплинарного расследования внутри организации;
- действия, следующие за разрешением инцидента ИБ, включая извлечение урока из инцидента и улучшение процесса, следующего за инцидентами ИБ;
- подробности места хранения документации о системе, включая процедуры хранения;
- общее представление о деятельности ГРИИБ, включающее в себя следующие вопросы:
- организационную структуру ГРИИБ и весь основной персонал группы, включая лиц, ответственных за:
- краткое информирование высшего руководства об инцидентах;

- проведение расследований и другие действия персонала группы после объявления «кризисной ситуации»;

- связь со сторонними организациями (при необходимости);

- положение о менеджменте ИБ, область деятельности ГРИИБ и полномочия, в рамках которых она будет ее осуществлять. Это положение должно включать в себя, как минимум, формулировку целевого назначения, определение области деятельности ГРИИБ и подробности об учредителе ГРИИБ и его полномочиях;

- формулировку целей ГРИИБ применительно к основной деятельности группы персонала. Для выполнения своих функций персонал должен участвовать в оценке инцидентов ИБ, реагировании на них и управлении ими, а также в их успешном разрешении. Для целей и назначения ГРИИБ требуется четкое и однозначное определение;

- определение сферы деятельности ГРИИБ. Обычно в сферу деятельности ГРИИБ организации входят все информационные системы, сервисы и сети организации. В некоторых случаях для организации может потребоваться сужение сферы действия ГРИИБ. При этом необходимо четко документировать, что входит и что не входит в сферу ее деятельности;

- личность учредителя ГРИИБ — старшего должностного лица (член правления, старший руководитель), который санкционирует действия ГРИИБ и устанавливает уровни полномочий, переданных ГРИИБ. Осведомленность об этом поможет всему персоналу организации понять предпосылки создания и структуру ГРИИБ, что является крайне важной информацией для формирования доверия к ГРИИБ. Перед обнародованием подробностей о создании и структуре ГРИИБ необходимо проверить законность этого действия. В некоторых обстоятельствах раскрытие полномочий группы персонала может послужить причиной предъявления ей претензий по нарушению обязательств;

- общее представление о программе обеспечения осведомленности и обучения менеджменту инцидентов ИБ;

- перечень нормативно-правовых аспектов, предполагаемых к рассмотрению (см. Раздел 5.2.3).

7.3 Программа менеджмента инцидентов информационной безопасности

7.3.1 Назначение программы

Программа менеджмента инцидентов ИБ предназначена для создания подробной документации, описывающей процессы и процедуры обработки инцидентов ИБ и оповещения (информирования) об инцидентах ИБ. Программа менеджмента ИБ приводится в действие при обнаружении события ИБ. Она используется в качестве руководства при:

- реагировании на события ИБ;

- определении того, становятся ли события ИБ инцидентами ИБ;

- менеджменте инцидентов ИБ до их разрешения;

- идентификации полученных уроков при обработке инцидентов, а также необходимых улучшений системы и (или) безопасности в целом;

- реализации идентифицированных улучшений.

7.3.2 Лица, связанные с программой менеджмента инцидентов информационной безопасности

Программа менеджмента инцидентов ИБ предназначена для всего персонала организации, включая лиц, ответственных за:

- обнаружение и оповещение о событиях ИБ. Эти лица могут быть служащими, работающими на постоянной основе или по контракту;

- оценку и реагирование на события ИБ и инциденты ИБ, которые участвуют в извлечении уроков на этапе разрешения инцидентов ИБ и в улучшениях ИБ и самой программы менеджмента инцидентов ИБ. Этими лицами являются члены группы обеспечения эксплуатации (или подобной группы), ГРИИБ, руководство организации, персонал отделов по связям с общественностью и юристы.

Следует также учитывать пользователей третьей стороны, которые сообщают об инцидентах ИБ и связанных с ними уязвимостях, и, кроме того, государственные и коммерческие организации, предоставляющие информацию об инцидентах ИБ и уязвимостях.

7.3.3 Содержание программы менеджмента инцидентов информационной безопасности

В содержание программы менеджмента инцидентов ИБ должны быть включены:

а) обзор политики менеджмента инцидентов ИБ;

б) общее представление о программе менеджмента инцидентов ИБ в целом;

в) детальные процессы и процедуры[*], информация о соответствующих сервисных программах и шкалах, связанных с проведением оценок событий ИБ (включая, если потребуется, их детализацию), используя принятую шкалу серьезности событий/инцидентов, и определением их способности к изменению своей категории на категорию инцидентов ИБ:

1) для этапа «Планирование и подготовка»:

– с обнаружением и оповещением о появлении событий ИБ (человеком или автоматическими средствами),

– со сбором информации о событиях ИБ:

2) для этапа «Использование» (в случае подтверждения инцидентов ИБ):

– с оповещением сотрудников своей организации и сторонних лиц или организаций о наличии инцидентов ИБ или любых важных деталях, касающихся инцидентов,

– с осуществлением немедленного реагирования, которое может включать в себя активизацию процедур восстановления и (или) передачу сообщений соответствующему персоналу согласно анализу и принятым степеням шкалы серьезности инцидентов,

– с проведением правовой экспертизы (при необходимости) по степеням шкалы серьезности инцидентов ИБ и изменением этих степеней,

– с определением наличия контроля над инцидентами ИБ,

– с созданием дополнительных реагирований (если требуется), включая те, которые могут потребоваться гораздо позднее (например, при устранении последствий какого-либо бедствия),

– в случае отсутствия контроля над инцидентами ИБ с инициированием антикризисных действий (например, вызов пожарной команды или активизация плана обеспечения непрерывности деятельности организации), с детализацией дальнейшей оценки и (или), если потребуется, дальнейших решений, с проверкой правильности регистрации всей деятельности для дальнейшего анализа, с обновлением базы данных событий/инцидентов ИБ.

В программе менеджмента инцидентов ИБ предусматривается возможность как немедленного, так и более длительного реагирования на инциденты ИБ. Для всех инцидентов ИБ требуется своевременная оценка потенциальных негативных воздействий, как кратковременных, так и более длительных (например, крупномасштабное бедствие

[*] Организация может принимать решения о включении всех процедур в программу или подробном изложении в дополнительных документах всех или некоторых процедур.

может произойти через некоторое время после первого инцидента ИБ). Более того, некоторые виды реагирования могут потребоваться для совершенно непредвиденных инцидентов ИБ, когда возникнет необходимость в специальных защитных мерах. Даже в такой ситуации в документации программы должны содержаться общие рекомендации по действиям, которые могут стать необходимыми;

3) для этапа «Анализ»:

– с проведением, если потребуется, дальнейшей правовой экспертизы,

– с идентификацией и документированием опыта, извлеченного из инцидентов ИБ,

– с определением и анализом улучшений ИБ на основе полученного опыта,

– с анализом эффективности процессов и процедур реагирования на инциденты ИБ, оценкой инцидентов ИБ и восстановления после каждого из них, а также определением улучшений программы менеджмента инцидентов ИБ в целом (на основе полученного опыта),

– с обновлением базы данных событий/инцидентов ИБ;

4) для этапа «Улучшение» — уточнение на основе полученного опыта:

– результатов анализа и менеджмента рисков ИБ,

– программы менеджмента инцидентов ИБ (например, процессов и процедур, формы оповещения и (или) структуры организации),

– общей безопасности внедрения новых и (или) улучшенных защитных мер,

– с градацией шкалы серьезности событий/инцидентов (например, значительный, незначительный; существенный, экстренный, незначительный, неэкстренный) и соответствующих руководств,

– с руководством решения о необходимости интенсификации каждого процесса, для кого должна проводиться интенсификация и в соответствии с какими процедурами. Персонал, оценивающий событие или инцидент ИБ, должен знать, основываясь на руководствах из документации программы менеджмента инцидентов ИБ, когда при нормальных обстоятельствах необходимо переходить к интенсификации процессов и для кого. Кроме того, возможно возникновение непредвиденных обстоятельств, когда интенсификация процессов может стать необходимой. Например, незначительный инцидент ИБ может перейти в категорию «существенный» или в «кризисную ситуацию» в случае его неправильной обработки, или незначительный инцидент ИБ, не обработанный в течение недели, может стать «значительным» инцидентом ИБ. В руководстве должны определяться типы событий и инцидентов ИБ, типы интенсификации процессов и лица, которые могут ее проводить,

– с необходимыми процедурами для надлежащей регистрации всех действий в соответствующей форме и проведением анализа журнала регистрации назначенным персоналом,

– с процедурами и механизмами поддержания режима контроля изменений, который включает в себя прослеживание событий и инцидентов ИБ, обновление отчета об инцидентах ИБ и обновление самой программы,

– с процедурами правовой экспертизы,

– с процедурами и руководством по использованию систем обнаружения вторжений (СОВ), обеспечивающими соблюдение связанных с ними правовых и нормативных аспектов (см. Раздел 5.2.3). Руководство должно включать в себя рассмотрение преимуществ и недостатков действий по наблюдению за злоумышленником,

– со структурой организации программы,

– с компетенцией и обязанностями членов ГРИИБ в целом и ее отдельных членов, с важной информацией о контактах группы.

7.3.4 Процедуры

Перед тем как приступить к работе с программой менеджмента инцидентов ИБ, необходимо иметь в наличии документированные и проверенные процедуры. В документации по каждой процедуре должны указываться лица из группы эксплуатационной поддержки и (или) из ГРИИБ, ответственные за использование и менеджмент этой процедуры. Такие процедуры должны включать в себя процедуры сбора и защищенного хранения электронных свидетельств, которые должны непрерывно контролироваться на случай судебного разбирательства или дисциплинарного расследования внутри организации. Более того, должны существовать документированные процедуры, включающие в себя не только действия группы эксплуатационной поддержки и ГРИИБ, но и процедуры, задействованные в правовой экспертизе и «антикризисной» деятельности, если они не задействованы где-либо еще, например, в плане обеспечения непрерывности деятельности организации. Очевидно, что эти документированные процедуры должны полностью соответствовать документированной политике менеджмента инцидентов ИБ и другой документации программы менеджмента инцидентов ИБ.

Необходимо иметь в виду, что не все процедуры являются общедоступными. Например, нежелательно, чтобы весь персонал организации знал подробности о работе ГРИИБ при взаимодействии с ней. ГРИИБ должна обеспечивать наличие «общедоступного» руководства, включая информацию, полученную из результатов анализа инцидентов ИБ, которая находится в легкодоступной форме, например, в интранете организации. Нежелательно раскрывать некоторые детали программы менеджмента инцидентов ИБ, чтобы лицо, обладающее конфиденциальной информацией внутри организации (инсайдер), не могло помешать процессу расследования. Например, если банковский служащий, присваивающий денежные средства, осведомлен о некоторых деталях программы, то он может лучше скрывать свою деятельность от следствия или иным образом препятствовать обнаружению и расследованию инцидента ИБ и восстановлению после него.

Содержание рабочих процедур зависит от многих критериев, особенно связанных с характером уже известных потенциальных событий и инцидентов ИБ и типами задействованных активов информационных систем и их средой. Так, некая рабочая процедура может быть связана с определенным типом инцидентов или с типом продукции (например, межсетевые экраны, базы данных, операционные системы, приложения), или со специфической продукцией. В каждой рабочей процедуре должно быть четко определено, какие шаги необходимо предпринять и кем. Она должна отражать опыт, полученный как из внутренних, так и внешних источников (например, государственные или коммерческие КГБР, или аналогичные группы, а также поставщики).

Для обработки уже известных типов событий и инцидентов ИБ должны существовать рабочие процедуры. Необходимы также рабочие процедуры, которым надо следовать, если тип обнаруженного инцидента ИБ или события неизвестен. В этом случае рассматривают следующие аспекты:

- процесс оповещения для обработки таких «исключительных случаев»;
- указания, определяющие время для получения одобрения реагирования на инцидент со стороны руководства с целью избежания задержки реагирования;
- предварительно одобренное делегирование принятия решения без обычного процесса одобрения.

7.3.5 Тестирование программы

Для выявления потенциальных дефектов и проблем, которые могут возникнуть в процессе менеджмента событий и инцидентов ИБ, необходимо запланировать регулярные

проверки и тестирование процессов и процедур менеджмента инцидентов ИБ. Любые изменения, возникающие в результате анализа реагирований на инциденты ИБ, должны подвергаться строгой проверке и тестированию.

7.4 Политики менеджмента рисков и информационной безопасности

7.4.1 Назначение

Целями включения содержания менеджмента инцидентов ИБ в корпоративные политики менеджмента рисков и ИБ и специальные политики ИБ систем, сервисов и сетей являются:

- описание значимости менеджмента инцидентов ИБ, особенно системы оповещения и обработки инцидентов ИБ;
- указание обязанностей высшего руководства относительно надлежащей подготовки к инцидентам ИБ и реагированию на них, то есть относительно системы менеджмента инцидентов ИБ;
- обеспечение согласованности различных политик;
- обеспечение планового и систематического реагирования на инцидент ИБ для минимизации негативного воздействия инцидентов.

7.4.2 Содержание

Корпоративная политика менеджмента рисков и ИБ, а также специальные политики ИБ для систем, сервисов или сетей должны обновляться с целью обеспечения точного соответствия общей политике менеджмента инцидентов ИБ и соответствующей ей системе. В соответствующие разделы необходимо включать обязательства высшего руководства и описание:

- политики;
- процессов системы и соответствующей инфраструктуры;
- требований по обнаружению, оповещению, оценке и управлению инцидентами;
- четкого определения персонала, ответственного за авторизацию и (или) проведение определенных важных действий (например, перевод информационной системы в режим off-line или даже отключение системы).

Кроме того, корпоративная политика должна содержать требование о создании соответствующих механизмов анализа для обеспечения использования любой информации, полученной в результате процессов обнаружения, мониторинга и разрешения инцидентов ИБ, в качестве входных данных для обеспечения стабильной результативности корпоративных политик менеджмента рисков ИБ, а также специальных политик ИБ для систем, сервисов и сетей.

7.5 Создание группы реагирования на инциденты информационной безопасности

7.5.1 Назначение группы реагирования на инциденты информационной безопасности

Целью создания ГРИИБ является обеспечение организации соответствующим персоналом для оценки, реагирования на инциденты ИБ и извлечения уроков из них, а также необходимой координации, менеджмента, обратной связи и процесса передачи информации. Члены ГРИИБ могут участвовать в снижении физического и финансового ущерба, а также ущерба для репутации организации, связанного с инцидентами ИБ.

7.5.2 Члены группы реагирования на инциденты информационной безопасности и структура этой группы

Состав и количество персонала, а также структура ГРИИБ должны соответствовать

масштабу и структуре организации. ГРИИБ может представлять собой изолированную команду или отдел, персонал этой группы может выполнять и другие обязанности, а также привлекать сотрудников из различных подразделений организации. В соответствии с Разделами 4.2.1 и 7.1 во многих случаях ГРИИБ может быть действующей группой, возглавляемой старшим руководителем. Вышестоящему руководителю оказывают помощь специалисты по конкретным вопросам, например, по отражению атак вредоносных программ, которые привлекаются в зависимости от типа инцидента ИБ. В зависимости от численного состава организации сотрудники ГРИИБ могут также выполнять несколько функций внутри ГРИИБ. В ГРИИБ могут также привлекаться служащие из различных подразделений организации (например, операций, ИТ/телекоммуникаций, аудита, отдела кадров и маркетинга).

Члены группы должны быть доступны для контакта так, чтобы их имена и имена лиц, их замещающих, а также подробности о контакте с ними были доступными внутри организации. Например, в документации системы менеджмента инцидентов ИБ должны быть четко указаны необходимые детали, включая любые документы по процедурам и формы отчетов, но не в положениях политики.

Руководитель ГРИИБ должен:

- иметь делегированные полномочия немедленного принятия решения о том, какие меры предпринять относительно инцидента;
- как правило, иметь отдельную линию для оповещения высшего руководства, которая должна быть изолирована от обычных операций;
- обеспечивать необходимый уровень знаний и мастерства для всех членов ГРИИБ, а также поддержание этого уровня;
- поручать расследование каждого инцидента наиболее компетентному члену группы.

7.5.3 Взаимодействие с другими подразделениями организации

Уровень полномочий руководителя ГРИИБ и членов его группы должен позволять предпринимать необходимые действия, адекватные инциденту ИБ.

Однако действия, которые могут оказать неблагоприятное влияние на всю организацию в отношении финансов или репутации, должны согласовываться с высшим руководством. Поэтому важно уточнить, какой орган в системе обеспечения политики менеджмента инцидентов ИБ, руководитель ГРИИБ оповещает о серьезных инцидентах ИБ.

Процедуры общения со средствами массовой информации и ответственность за это общение также должны быть согласованы со старшим руководством, документированы и определять:

- представителя организации по работе со средствами массовой информации;
- метод взаимодействия подразделения организации с ГРИИБ.

7.5.4 Отношения со сторонними лицами и организациями

Необходимо установить отношения между ГРИИБ и соответствующими сторонними лицами и организациями.

К сторонним лицам и организациям могут относиться:

- сторонний вспомогательный персонал, работающий по контракту,например, КГБР;
- ГРИИБ сторонних организаций, а также КГБР;
- правоприменяющие организации;
- аварийные службы (например, пожарная бригада/отделение);
- соответствующие государственные организации;
- юридический персонал;

- официальные лица по связям с общественностью и (или) представителями средств массовой информации;
- партнеры по бизнесу;
- потребители;
- общественность.

7.6 Техническая и другая поддержка реагирования на инциденты информационной безопасности

Быстрое и эффективное реагирование на инциденты ИБ осуществляется гораздо легче, когда все необходимые технические и другие средства поддержки получены, подготовлены и протестированы. Эти мероприятия включают в себя:

- доступ к деталям активов организации (предпочтительно иметь обновленный перечень активов) и информацию по их связям с видами деятельности организации;
- доступ к документированной стратегии обеспечения непрерывности деятельности организации и соответствующим планам;
- документированные и опубликованные процессы передачи информации;
- использование электронной базы данных событий/инцидентов ИБ и технических средств, для быстрого пополнения и обновления базы данных, анализа ее информации и упрощения процессов реагирования (хотя общепризнано, что иногда сделанные вручную записи также оказываются востребованными и используются организацией);
- адекватные меры по обеспечению непрерывности деятельности организации для базы данных событий/инцидентов ИБ.

Технические средства, используемые для быстрого пополнения, обновления баз данных, анализа содержания информации и баз данных и облегчения процессов реагирования на инциденты ИБ, должны содействовать:

- быстрому получению отчетов о событиях и инцидентах ИБ;
- уведомлению ранее отобранного персонала (соответствующих сторонних лиц) подходящими для этого средствами (например, через электронную почту, факс, телефон и т. д.), то есть, запрашивая поддержку надежной контактной базы данных (которая должна быть всегда легкодоступной и должна включать в себя бумажные и другие копии) и средство передачи информации безопасным способом (при необходимости);
- соблюдению предосторожностей, соответствующих оцененным рискам, защите от прослушивания электронной связи, реализуемой через Интернет или иным образом, во время атаки на систему, сервис и (или) сеть;
- соблюдению предосторожностей, соответствующих оцененным рискам, для сохранения доступности электронной связи, осуществляемой через Интернет или иным образом, во время атаки на систему, сервис и (или) сеть;
- процессу сбора всех данных об информационной системе, сервисе и (или) сети и всех обрабатываемых данных;
- использованию криптографического контроля целостности, если это соответствует оцененным рискам, для содействия в определении наличия изменений и того, какие части системы, сервиса и (или) сети и данные подверглись изменениям;
- упрощению архивирования и защиты собранной информации (например, применяя цифровые подписи в записях в журнале регистрации или другие свидетельства перед хранением в автономном режиме на носителях, предназначенных только для чтения на устройствах CD или DVD ROM);
- подготовке распечаток (например, журналов регистрации), демонстрирующих развитие инцидента ИБ, процесс разрешения инцидента и обеспечивающих сохранность информации;
- восстановлению штатного режима работы информационной системы, сервиса и

(или) сети с помощью:

оптимальных процедур резервирования, четких и надежных резервных копий, тестирования резервных копий, контроля вредоносных программ;

исходных носителей информации с системным и прикладным программным обеспечением;

надежных и обновленных исправлений («патчей») для систем и приложений, согласованных с соответствующим планом обеспечения непрерывности деятельности организации.

Атакованная информационная система, сервис и (или) сеть могут функционировать неверно. Поэтому работа технического средства (программного или аппаратного обеспечения), необходимого для реагирования на инцидент ИБ, не должна быть основана на системах, сервисах и (или) сетях, используемых в организации. По возможности, технические средства реагирования на инциденты должны быть полностью автономными.

Все технические средства должны быть тщательно отобраны, правильно внедрены и регулярно тестироваться (включая тестирование полученных резервных копий).

Технические средства, описанные в настоящем подразделе, не включают в себя технические средства, используемые непосредственно для обнаружения инцидентов ИБ и вторжений и автоматического оповещения соответствующих лиц. Данные технические средства описаны в [1] и [2].

7.7 Обеспечение осведомленности и обучение

Менеджмент инцидентов ИБ — это процесс, включающий в себя не только технические средства, но также персонал, и, следовательно, этот процесс должен поддерживаться лицами, соответствующим образом обученными для работы в организации и осведомленными в вопросах безопасности информации.

Осведомленность и участие всего персонала организации очень важны для обеспечения успеха структурного подхода к менеджменту инцидентов ИБ. Поэтому роль менеджмента инцидентов ИБ должна активно поддерживаться как часть общей программы обучения и обеспечения осведомленности в вопросах ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала, включая новых служащих, пользователей сторонних организаций и подрядчиков. Должна существовать специальная программа обучения для группы обеспечения эксплуатации, для членов ГРИИБ, а при необходимости для персонала, ответственного за ИБ, и специальных администраторов. Следует заметить, что для каждой группы, непосредственно участвующей в менеджменте инцидентов, могут потребоваться различные уровни подготовки, зависящие от типа, частоты и значимости их взаимодействия с системой менеджмента инцидентов ИБ.

Инструктажи по обеспечению осведомленности должны включать в себя:

- основы работы системы менеджмента инцидентов ИБ, включая сферу ее действия и технологию работ по менеджменту инцидентов и событий ИБ;
- способы оповещения о событиях и инцидентах ИБ;
- защитные меры по обеспечению конфиденциальности источников (по необходимости);
- соглашения об уровнях сервиса системы;
- уведомление о результатах — на каких условиях будут информированы источники;
- любые ограничения, налагаемые соглашениями о неразглашении;
- полномочия организации менеджмента инцидентов ИБ и ее линия оповещения;
- кто и как получает отчеты от системы менеджмента инцидентов ИБ.

В некоторых случаях желательно специально включать подробности обеспечения осведомленности о менеджменте инцидентов ИБ в другие программы обучения

(например, в программы ориентирования персонала или в общие корпоративные программы обеспечения осведомленности в вопросах ИБ). Этот подход к обеспечению осведомленности может предоставить ценную информацию, связанную с определенными группами сотрудников, и может улучшить эффективность и результативность программы обучения.

До ввода в эксплуатацию системы менеджмента инцидентов ИБ весь соответствующий персонал должен ознакомиться с процедурами обнаружения и оповещения о событиях ИБ, а специально отобранный персонал должен быть хорошо осведомлен в отношении последующих процессов. Затем проводят регулярные инструктажи по обеспечению осведомленности и курсы подготовки. Подготовка должна сопровождаться специальными упражнениями и тестированием членов группы обеспечения эксплуатации и ГРИИБ, а также персонала, ответственного за ИБ, и специальных администраторов.

8 Этап «Использование»

8.1 Введение

Менеджмент инцидентов ИБ в процессе эксплуатации состоит из двух главных этапов: «Использование» и «Анализ», за которыми следует этап «Улучшение», на котором проводят любые усовершенствования, идентифицированные в результате извлечения уроков из инцидентов ИБ. Эти этапы и связанные с ними процессы представлены в Разделе 4.2. В настоящем разделе рассматривается этап «Использование», в Разделе 9 — этап «Анализ», а в Разделе 10 — этап «Улучшение». Эти три этапа и соответствующие им процессы представлены на Рисунке 2.

8.2 Обзор ключевых процессов

В этапе «Использование» ключевыми процессами являются:

а) обнаружение события ИБ и оповещение о нем одним из сотрудников персонала/клиентом организации или автоматически (например, сигналом тревоги от межсетевого экрана);

б) сбор информации о событии ИБ и проведение первичной оценки персоналом* группы обеспечения эксплуатации организации с целью определения, является ли событие инцидентом ИБ или ложным сигналом тревоги;

в) проведение второй оценки ГРИИБ с целью подтвердить, что событие является инцидентом ИБ и, в положительном случае, инициировать немедленное реагирование, а также необходимость правовой экспертизы и действий по передаче информации;

г) анализ, проводимый ГРИИБ, с целью определить, находится ли инцидент под контролем:

1) в положительном случае инициируется дальнейшее необходимое реагирование и обеспечивается готовность всей информации для использования в процессе анализа последствий инцидента,

2) при отрицательном ответе инициируются антикризисные действия с привлечением соответствующего персонала, например, руководителя и группы обеспечения непрерывности деятельности организации;

д) расширение области действия дальнейших оценок и (или) принятия решений, проводимое в течение всего этапа по требованию;

* Не следует ожидать, что персонал группы обеспечения эксплуатации будет иметь квалификацию экспертов в сфере безопасности.

е) обеспечение надлежащей регистрации всеми причастными лицами, в особенности членами ГРИИБ, всей деятельности для дальнейшего анализа;

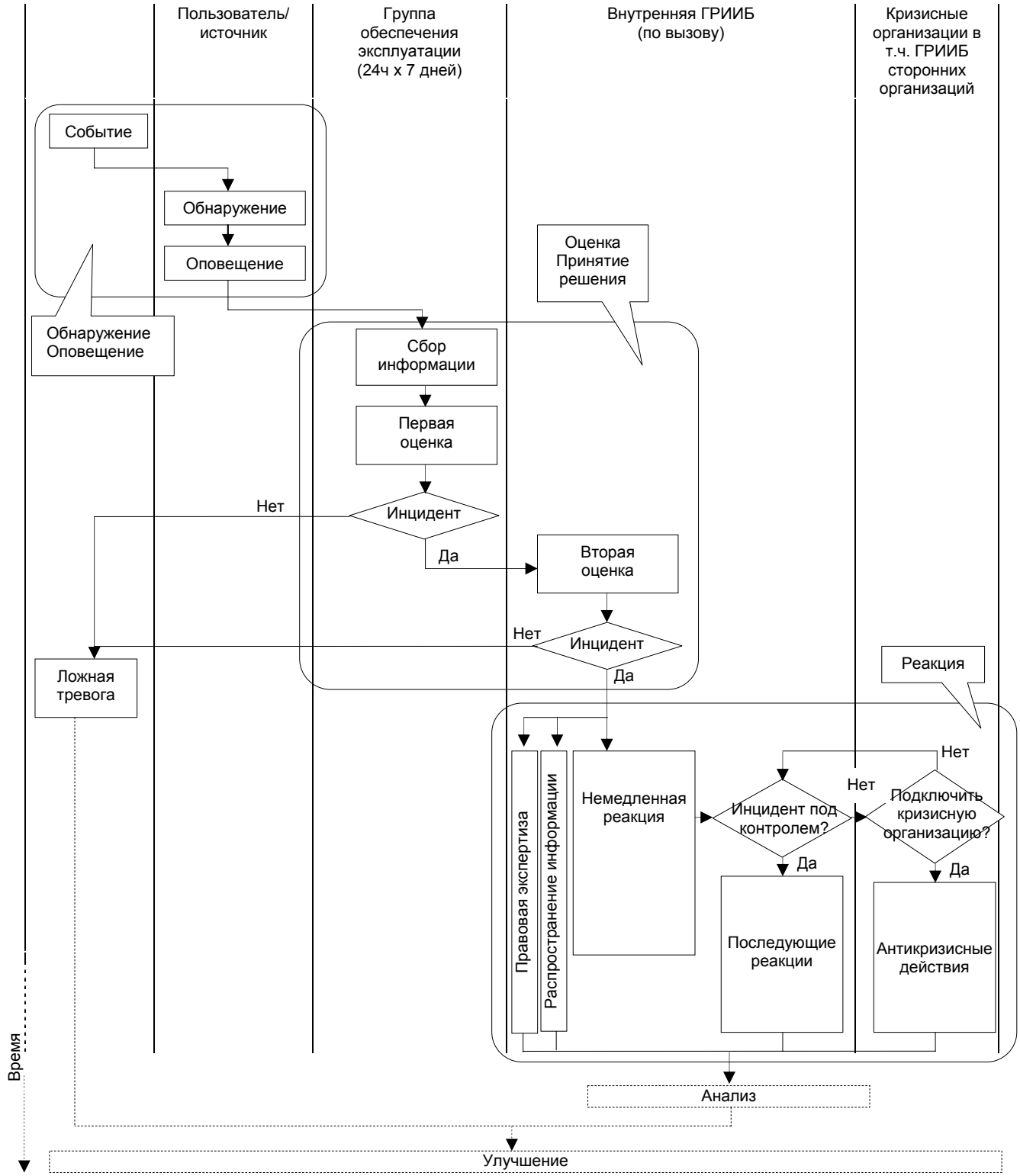


Рисунок 2 – Блок-схема последовательностей операций обработки событий и инцидентов ИБ (этап «Использование»)

ж) обеспечение сбора и защищенного хранения свидетельств в электронном виде и постоянного мониторинга защищенного хранения этих свидетельств на случай их востребованности для судебного преследования или внутреннего дисциплинарного разбирательства;

и) поддержка режима контроля изменений, включая отслеживание инцидентов ИБ и обновления отчетов по инцидентам с тем, чтобы база данных событий/инцидентов ИБ постоянно соответствовала действительности.

Вся собранная информация, касающаяся событий или инцидентов ИБ, должна храниться в базе данных событий/инцидентов ИБ, управляемой ГРИИБ. Информация, сообщаемая в течение каждого процесса, должна быть как можно более полной в любое время, чтобы обеспечить наиболее прочную основу для оценок и принятия решений, а также для предпринимаемых действий.После обнаружения события ИБ и сообщения о нем, целями последующих процессов являются:

а) распределение ответственности за деятельность, связанную с менеджментом инцидентов, через соответствующую иерархию персонала вместе с оценкой и принятием решений, а также за действия с привлечением персонала как связанного, так и не связанного с обеспечением безопасности;

б) обеспечение формальных процедур для каждого оповещенного лица, включая анализ и корректировку сделанного сообщения, оценку ущерба и уведомление соответствующего персонала (действия каждого лица зависят от типа и опасности инцидента);

в) использование рекомендаций для тщательного документирования событий ИБ, а позднее, если событие будет отнесено к инциденту ИБ, то и для последующих действий в отношении инцидента ИБ и обновления базы данных событий/инцидентов ИБ.

Рекомендации приведены:

а) по обнаружению и оповещению о событиях ИБ — в Разделе 8.3, оценке и принятию решений (является ли событие инцидентом ИБ) — в Разделе 8.4, реагированию на инциденты ИБ — в Разделе 8.5 и включают в себя:

- немедленное реагирование,
- анализ с целью определения, находится ли инцидент ИБ под контролем,
- последующие реагирования,
- антикризисные действия,
- правовую экспертизу,
- передачу информации,
- комментарий по вопросам расширения сферы менеджмента инцидентов ИБ,
- регистрацию деятельности.

8.3 Обнаружение и оповещение о событиях информационной безопасности

События ИБ могут быть обнаружены непосредственно лицом или лицами, заметившими что-либо, вызывающее беспокойство и имеющее технический, физический или процедурный характер. Обнаружение может осуществляться, например, детекторами огня/дыма или с помощью охранной сигнализации путем передачи сигналов тревоги в заранее определенные места (для осуществления человеком определенных действий). Технические события ИБ могут обнаруживаться автоматически, например, это могут быть сигналы тревоги, производимые устройствами анализа записей аудита, межсетевыми экранами, системами обнаружения вторжений, антивирусными программами, в каждом случае стимулируемые заранее установленными параметрами этих устройств.

Независимо от причины обнаружения события ИБ, лицо, непосредственно обратившее внимание на нечто необычное или оповещенное автоматическими средствами, несет ответственность за инициирование процесса обнаружения и

оповещения. Этим лицом может быть любой представитель персонала организации, работающий постоянно или по контракту. Этот представитель должен следовать процедурам и использовать форму отчета о событиях ИБ, определенную системой менеджмента инцидентов ИБ, с целью привлечения внимания, прежде всего группы обеспечения эксплуатации и менеджмента. Следовательно, важно, чтобы весь персонал был ознакомлен с рекомендациями, относящимися к вопросу оповещения о возможных событиях ИБ, включая формы отчета, имел доступ к ним и знал сотрудников, которых необходимо оповещать о каждом случае появления события ИБ. Необходимо, чтобы весь персонал организации был, по крайней мере, осведомлен о форме отчета, что способствовало бы его пониманию системы менеджмента инцидентов ИБ.

Обработка конкретного события ИБ зависит от того, что оно собой представляет, а также от последствий и воздействий, к которым это событие может привести. Для многих людей принятие решения о способе обработки события выходит за пределы их компетентности. Поэтому сотрудник, информирующий о событии ИБ, должен заполнить форму отчета так, чтобы в ней было как можно больше информации, доступной ему на тот момент. При необходимости он связывается со своим руководителем. Желательно, чтобы эта форма была в электронном виде (например, послана по электронной почте или представлена на веб-сайте), чтобы ее можно было передать безопасным способом в надлежащую группу обеспечения эксплуатации (работающую, по возможности, 24 ч. в сутки по семь дней в неделю), а копию сообщения - руководителю ГРИИБ. Образец формы отчета сообщения о событии ИБ приведен в Приложении А.

Следует подчеркнуть, что при заполнении формы отчета важна не только точность содержания, но и своевременность заполнения. Не следует задерживать представление формы отчета о событии ИБ по причине уточнения ее содержания. Если сообщающий сотрудник не уверен в данных какого-либо поля в форме отчета, то это поле должно быть помечено, а уточнение послано позже. Также следует признать, что некоторые механизмы электронного оповещения (например, электронная почта) сами являются очевидными целями атаки.

При наличии проблем или при существовании мнения о наличии проблем с установленными по умолчанию механизмами электронного оповещения (например, электронной почтой), включая случаи атаки на систему и считывание формы отчета несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть нарочные, текстовые сообщения, телефон. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться значительным.

Следует заметить, что, хотя в большинстве случаев группа обеспечения эксплуатации должна сообщать о событии ИБ с целью его дальнейшей обработки, могут быть случаи, когда событие ИБ может быть обработано на месте с помощью местного руководства. Событие ИБ можно быстро распознать как ложную тревогу или успешно разрешить. В этих случаях форму отчетов необходимо заполнить и отправить местному руководству, а также группе обеспечения эксплуатации и ГРИИБ с целью ее регистрации в базе данных событий/инцидентов ИБ. В этом случае лицо, сообщающее о закрытии события ИБ, может предоставить информацию, требуемую для заполнения формы отчета об инцидентах ИБ. В этом случае такая форма отчета об инциденте ИБ должна быть заполнена и отправлена по инстанции.

8.4 Оценка и принятие решений по событиям/инцидентам

8.4.1 Первая оценка и предварительное решение

В группе обеспечения эксплуатации системы менеджмента инцидентов ИБ принимающее лицо должно подтвердить получение заполненной формы отчета, ввести ее в базу данных событий/инцидентов ИБ и проанализировать данную форму отчета. Далее должностное лицо должно попытаться получить любые уточнения о событии ИБ и собрать требуемую дополнительную информацию, считающуюся доступной, как от сообщившего о событии лица, так и из любого другого источника. Затем представитель группы обеспечения эксплуатации должен провести оценку для определения, подходит ли это событие под категорию инцидента ИБ или является ложным. Если событие ИБ определяется как ложное, необходимо заполнить форму отчета и передать в ГРИИБ для записи в базу данных и дальнейшего анализа, а также создать копии для сообщившего о событии лица и его/ее местного руководителя.

Информация и другие свидетельства, собранные на этом этапе, могут потребоваться в будущем для дисциплинарного или судебного разбирательства. Лицо или лица, выполняющие задачи сбора и оценки информации, должны хорошо знать требования по сбору и сохранению свидетельств.

Дополнительно к дате (датам) и времени выполнения действий необходимо полностью документировать:

- проведенные мероприятия (включая использованные средства) и их цели;
- место хранения свидетельства наличия события;
- способ архивирования свидетельства (если оно уместно);
- способ верификации свидетельства (если оно уместно);
- детали хранения материалов и последующего доступа к ним.

Если событие ИБ определено как вероятный инцидент ИБ, а сотрудник группы обеспечения эксплуатации имеет соответствующий уровень компетентности, то проводится дальнейшая оценка. В результате могут потребоваться корректирующие действия, например, идентификация дополнительных «аварийных» защитных мер и обращение за помощью в их реализации к соответствующему лицу. Событие ИБ может быть определено как инцидент ИБ, причем значительный (по шкале серьезности, принятой в организации), в этом случае необходимо проинформировать непосредственно руководителя ГРИИБ. Может потребоваться объявление «кризисной ситуации» и, как следствие, уведомление руководителя обеспечения непрерывности деятельности организации о возможной активизации плана обеспечения непрерывности деятельности организации с одновременным информированием руководителя ГРИИБ и вышестоящего руководства. Однако наиболее вероятна ситуация передачи инцидента ИБ непосредственно в ГРИИБ для дальнейшей оценки и выполнения соответствующих действий.

Каким бы ни был следующий шаг, сотрудник группы обеспечения эксплуатации должен заполнить форму отчета по возможности наиболее подробно. Образец формы отчета по инциденту ИБ приведен в Приложении А. Отчет должен содержать информацию в описательном виде и, насколько это возможно, характеризовать:

- что представляет собой инцидент ИБ;
- что явилось его причиной, чем или кем он был вызван;
- на что он влияет или может повлиять;
- реальное или потенциальное воздействие инцидента ИБ на деятельность организации;
- указание на вероятную значительность или незначительность инцидента ИБ (по шкале серьезности, принятой в организации);
- как инцидент ИБ обрабатывался до этого времени.

При рассмотрении потенциального или фактического негативного воздействия инцидента на деятельность организации в результате несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и (или) сервиса, уничтожения информации и(или) сервиса в первую очередь необходимо определить, какое из перечисленных ниже последствий будет иметь инцидент ИБ.

Примерами последствий ИБ являются:

- финансовые убытки/прерывание операций;
- ущерб коммерческим и экономическим интересам;
- ущерб информации, содержащей персональные данные;
- нарушение правовых и нормативных обязательств;
- сбои операций по менеджменту и других операций;
- утрата престижа организации.

Для категорий, отнесенных к инциденту ИБ, должны использоваться соответствующие рекомендации по категорированию потенциальных или фактических воздействий для внесения их в отчет по инцидентам ИБ. Примеры рекомендаций приведены в Приложении В.

Если инцидент ИБ был разрешен, то отчет должен содержать детали предпринятых защитных мер и извлеченных уроков (например, защитные меры, которые должны быть приняты для предотвращения повторного появления подобных инцидентов ИБ).

После наиболее подробного, по мере возможности, заполнения форма отчета должна быть представлена в ГРИИБ для ввода в базу данных инцидентов и событий ИБ и анализа в будущем.

Если расследование проводится больше недели, то должен быть составлен промежуточный отчет.

Важно, чтобы сотрудник группы обеспечения эксплуатации, оценивающий инцидент ИБ, основываясь на руководстве, содержащемся в документации системы менеджмента инцидентов ИБ, был осведомлен о том:

- когда и кому необходимо направлять материалы об инциденте;
- что при осуществлении всех действий, выполняемых группой обеспечения эксплуатации, необходимо выполнять документированные процедуры контроля изменений.

При наличии проблем или мнения о том, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например, электронной почтой), включая случаи атаки на информационную систему и считывание несанкционированными лицами формы отчета об инцидентах ИБ, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть: телефон, текстовые сообщения, а также курьеры. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться «значительным».

8.4.2 Вторая оценка и подтверждение инцидента информационной безопасности

Вторая оценка и подтверждение инцидента ИБ или какое-либо другое решение относительно того, надо ли отнести событие ИБ к инциденту ИБ, должны входить в обязанности ГРИИБ. Принимающий отчеты сотрудник ГРИИБ должен:

а) подтвердить получение формы отчета, заполненной по возможности наиболее подробно, группой обеспечения эксплуатации;

б) ввести эту форму в базу данных событий/инцидентов ИБ;

в) обратиться за уточнениями к группе обеспечения эксплуатации;

г) проанализировать содержание отчетной формы;

д) собрать дополнительную необходимую информацию о событии ИБ (если существует) от группы обеспечения эксплуатации, лица, заполнившего отчетную форму, или из какого-либо иного источника.

Если все еще остается какая-либо неопределенность относительно аутентичности инцидента ИБ или полноты полученной информации, то сотрудник ГРИИБ должен провести вторую оценку для определения реальности или ложности инцидента ИБ. Если инцидент ИБ определен как «ложный», необходимо заполнить отчет о событии ИБ, добавить его в базу данных событий/инцидентов ИБ и передать руководителю ГРИИБ. Копии отчета необходимо передать группе обеспечения эксплуатации, лицу, сообщившему о событии, и его/ее местному руководителю.

Если инцидент ИБ определяется как «реальный», то сотрудник ГРИИБ, при необходимости привлекая коллег, должен провести дальнейшую оценку. Целью оценки является максимально быстрое подтверждение:

а) того, что представляет собой инцидент ИБ, что явилось его причиной, чем или кем был вызван, на что повлиял или мог повлиять, воздействие или потенциальное воздействие инцидента ИБ на деятельность организации, указание на вероятную значительность/незначительность инцидента (по шкале серьезности инцидентов, принятой в организации);

б) предумышленной технической атаки нарушителя на некоторую информационную систему, сервис и (или) сеть, например:

1) глубины проникновения нарушителя в систему, сервис и (или) сеть и степень контроля, которой он обладает,

2) данных об информации, к которой получил доступ нарушитель, были ли они скопированы, изменены или удалены,

3) о том, какое программное обеспечение было скопировано, изменено или разрушено нарушителем;

4) в отношении предумышленной физической атаки нарушителя на любую информационную систему аппаратной части, сервиса и (или) на сеть, и (или) на физическое месторасположение, например:

- масштаба прямых и косвенных последствий нанесенного физического ущерба (при отсутствии физической защиты доступа),

- прямых и косвенных последствий в отношении инцидентов ИБ, косвенно созданных действиями нарушителя (например, стал ли физический доступ возможным по причине пожара, является ли уязвимость информационной системы следствием неправильного функционирования программного обеспечения, линии связи или ошибки оператора),

в) используемого до настоящего времени способа обработки инцидента ИБ.

При анализе потенциального или реального негативного воздействия инцидента ИБ на деятельность организации вследствие несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и (или) сервиса, разрушения информации и (или) сервиса необходимо подтвердить, какие последствия имели место вследствие данного инцидента. Примерами категорий последствий являются:

а) финансовые убытки/прерывание операций;

б) ущерб коммерческим и экономическим интересам;

в) ущерб для информации, содержащей персональные данные;

г) нарушение правовых и нормативных обязательств;

д) сбои операций по менеджменту и других операций;

е) утрата престижа организации.

Для отнесения потенциальных или фактических воздействий к той или иной категории необходимо использовать соответствующие рекомендации, которые относили бы их к инциденту ИБ и вносились в отчет по инцидентам ИБ. Примеры рекомендаций приведены в Приложении Б.

8.5 Реагирование на инциденты

8.5.1 Немедленное реагирование

8.5.1.1 Обзор

В большинстве случаев после подтверждения инцидента член ГРИИБ выполняет действия по немедленному реагированию относительно инцидента ИБ, регистрации подробностей в форме отчета об инциденте ИБ, введению в базу данных событий/инцидентов ИБ и уведомлению сотрудников организации о требуемых действиях на инцидент ИБ. Результатом данных действий может быть принятие аварийных защитных мер (например; отключение атакованной информационной системы, сервиса и (или) сети по предварительному соглашению с соответствующим руководством ИТ - подразделения и (или) высшим руководством) и (или) определение дополнительных постоянных защитных мер и уведомление сотрудников организации о принятии этих мер. Если аварийные защитные меры не применены, то нужно определить значительность инцидента ИБ по оценочной шкале, принятой в организации, и если инцидент ИБ достаточно «значителен», то об этом необходимо непосредственно уведомить соответствующее вышестоящее руководство. Если очевидна необходимость объявления «кризисной ситуации», руководитель, отвечающий за обеспечение непрерывности деятельности организации, должен быть оповещен о возможной активизации плана обеспечения непрерывности деятельности организации, причем необходимо проинформировать руководителя ГРИИБ и вышестоящее руководство.

8.5.1.2 Примерные действия по реагированию

Примером действий по немедленному реагированию в случае преднамеренной атаки на информационную систему, сервис и (или) сеть может быть то, что они остаются подключенными к Интернету и другим сетям с целью:

- обеспечения правильного функционирования критически важных приложений;
- сбора наиболее полной информации о нарушителе при условии, если он не знает, что находится под наблюдением.

Однако при принятии решения по реагированию нужно учитывать следующие факторы:

- нарушитель может почувствовать, что находится под наблюдением, и предпринять действия, наносящие дальнейший ущерб атакованной системе, сервису и (или) сети и данным;
- нарушитель может разрушить информацию, которая способствует его отслеживанию.

Важно, чтобы при принятии соответствующего решения была техническая возможность быстро и надежно отключить атакованную информационную систему, сервис и (или) сеть. Однако для предотвращения такого отключения не имеющим на это право персоналом необходимо применять соответствующие средства аутентификации.

Предотвращение повторного проявления инцидента обычно является более приоритетной задачей. В некоторых случаях необходимо учитывать то, что нарушитель выявил слабое место, которое должно быть устранено, а выгоды от выявления нарушителя не оправдывают затраченных на это усилий. Это особенно справедливо, если нарушитель на самом деле не является злоумышленником и не нанес большого или вообще не причинил никакого ущерба.

Что касается других инцидентов ИБ, кроме преднамеренной атаки, то их источник должен быть идентифицирован. Может потребоваться отключение информационной системы, сервиса и (или) сети или изоляция соответствующих их частей после получения предварительного согласия соответствующего руководства ИТ и (или) высшего руководства на время внедрения защитных мер. Для этого может потребоваться больше времени, если уязвимое место для информационной системы, сервиса и (или) для сети окажется существенным или критически важным.

Другим действием по реагированию может быть активизация методов наблюдения [4]. Это действие должно осуществляться на основе процедур, документированных для системы менеджмента инцидентов ИБ.

Информация, которая могла быть повреждена в результате инцидента ИБ, должна быть проверена членом ГРИИБ по резервным записям на предмет изменения, стирания или модификации информации. Может возникнуть необходимость проверки целостности журналов регистрации, поскольку злонамеренный нарушитель может подделать их с целью сокрытия следов проникновения.

8.5.1.3 Обновление информации об инцидентах

Независимо от последующих действий, сотрудник ГРИИБ должен обновить отчет об инциденте ИБ с максимальной детализацией, добавить его в базу данных событий/инцидентов ИБ, оповестив об этом руководителя ГРИИБ и (при необходимости) других лиц. Обновляют следующую информацию:

- о том, что представляет собой инцидент ИБ;
- о том, что явилось причиной, чем или кем он был вызван;
- на что воздействует или мог воздействовать;
- о фактическом или потенциальном воздействии инцидента ИБ на деятельность организации;
- об изменениях в указании на вероятную значительность или незначительность инцидента ИБ (по шкале серьезности, принятой в организации);
- о том, как он обрабатывался до этого времени.

Если инцидент ИБ разрешен, то отчет должен содержать подробности предпринятых защитных мер и извлеченных уроков (например: дополнительные защитные меры, которые следует предпринять для предотвращения повторного появления данного инцидента ИБ или подобных ему инцидентов ИБ). Обновленный отчет следует добавлять в базу данных событий/инцидентов ИБ и уведомлять руководителя ГРИИБ и других лиц по их требованию.

ГРИИБ отвечает за обеспечение безопасного хранения информации, относящейся к данному инциденту ИБ, с целью возможного проведения дальнейшей экспертизы и возможного использования судом в качестве доказательства. Например, для инцидента ИБ, ориентированного на ИТ, после первоначального обнаружения инцидента ИБ все непостоянные данные должны быть собраны до отключения пораженной системы ИТ, сервиса и (или) сети до проведения судебного расследования. Предназначенная для сбора информация содержит сведения о любых функционирующих процессах и хранится в памяти, кэше и регистрах. При этом необходимо:

- в зависимости от характера инцидента ИБ провести полное дублирование пораженной системы, сервиса и (или) сети на случай судебного разбирательства или резервное копирование журналов и важных файлов;
- собрать и проанализировать журналы соседних систем, сервисов и (или) сетей, например, маршрутизаторов и межсетевых экранов;
- всю собранную информацию хранить на носителях только для чтения;

- при выполнении дублирования на случай судебного разбирательства обеспечить присутствие не менее двух лиц для утверждения и подтверждения того, что все действия были выполнены согласно действующему нормативному законодательству;
- документировать и хранить вместе с исходными носителями спецификации и описания сервисных команд, которые используются для дублирования на случай судебного разбирательства.

Член ГРИИБ также является ответственным, если это возможно, во время обновления информации об инцидентах ИБ за возвращение в безопасное рабочее состояние пораженных устройств (имеющих или не имеющих отношение к ИТ) в интересах исключения атак на эти устройства.

8.5.1.4 Дополнительные действия

При определении членом ГРИИБ реальности инцидента ИБ его дополнительными действиями должны быть:

- проведение правовой экспертизы;
- информирование лиц, ответственных за передачу информации внутри организации и за ее пределами, о фактах и предложениях по информации, которую надо передать, в какой форме и кому.

После возможно наиболее подробного заполнения отчета об инциденте ИБ отчет вводится в базу данных событий/инцидентов ИБ и передается руководителю ГРИИБ.

Если время расследования превышает время, ранее согласованное внутри организации, то составляется промежуточный отчет.

Член ГРИИБ, оценивающий инцидент ИБ, на основании руководства, содержащегося в документации системы менеджмента инцидентов ИБ, должен знать:

- когда и кому необходимо направлять материалы;
- что при осуществлении любой деятельности ГРИИБ необходимо следовать документированным процедурам контроля за внесением изменений.

При наличии проблем или если считается, что существуют проблемы в отношении обычных средств связи (например, с электронной почтой), включая случаи, когда система, возможно, подвергается атаке и целесообразно сделать вывод, что инцидент ИБ является значительным и (или) была определена «кризисная ситуация», то следует, в первую очередь, сообщить об инциденте ИБ ответственным лицам лично, по телефону или текстовым сообщением.

При необходимости руководитель ГРИИБ совместно с руководителем обеспечения безопасности ИБ организации и соответствующим руководителем организации (членом совета директоров) правления должны связаться со всеми отделами, которые вовлечены в инцидент ИБ как внутри организации, так и за ее пределами (см. Разделы 7.5.3 и 7.5.4).

Для быстрой и эффективной организации связи необходимо заранее установить надежный метод передачи информации, не зависящий полностью от системы, сервиса или сети, на которые может воздействовать инцидент ИБ. Такие меры предосторожности могут включать в себя назначение резервных консультантов или представителей организации на случай отсутствия кого-либо из ее основных руководителей.

8.5.2 Контролируемость инцидента

После инициирования членом ГРИИБ немедленного реагирования посредством соответствующей правовой экспертизы и действий по передаче информации необходимо срочно убедиться, находится ли инцидент ИБ под контролем. При необходимости, член ГРИИБ может проконсультироваться с коллегами, руководителем ГРИИБ и (или) другими сотрудниками организации.

Если подтверждается, что инцидент ИБ находится под контролем, то член ГРИИБ должен перейти к другим дальнейшим необходимым действиям по реагированию, проведению правовой экспертизы и передаче информации (см. Разделы 8.5.3, 8.5.5 и 8.5.6) с целью ликвидации инцидента ИБ и восстановления нормальной работы пораженной информационной системы.

Если не подтверждается, что инцидент ИБ находится под контролем, член ГРИИБ должен инициировать «антикризисные» действия (см. Раздел 8.5.4).

8.5.3 Последующее реагирование

Определив, что инцидент ИБ находится под контролем и не является объектом «антикризисной ситуации», член ГРИИБ должен определить необходимость и вероятные способы дальнейшего реагирования в отношении данного инцидента. Реагирование может включать в себя восстановление пораженных информационных систем (ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Затем член ГРИИБ должен занести детали в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а также проинформировать об этом лиц, ответственных за завершение соответствующих действий. Подробности успешного завершения этих действий необходимо внести в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а затем инцидент ИБ должен быть закрыт и соответствующий персонал должен быть проинформирован об этом.

Некоторые реагирования должны быть направлены на предотвращение повторения подобного ему инцидента ИБ. Например, если определено, что причиной инцидента ИБ является отказ аппаратурной части или программного обеспечения ИТ из-за отсутствия вставок в программу («патчей»), то в этом случае необходимо немедленно связаться с поставщиком. Если причиной инцидента ИБ была известная уязвимость ИТ, то она должна быть устранена соответствующим обновлением защиты ИБ. Необходимо также решить любые проблемы, связанные с конфигурацией ИТ и выявленным инцидентом ИБ. Другими мерами уменьшения возможности повторения или появления такого инцидента ИБ или подобного ему инцидента могут быть изменение системных паролей и отключение неиспользуемых сервисов.

Другая область деятельности по реагированию на инцидент ИБ может включать в себя мониторинг системы, сервиса и (или) сети ИТ. Следом за оценкой инцидента ИБ может оказаться целесообразным ввести дополнительные защитные меры мониторинга для содействия в обнаружении необычных или подозрительных событий, которые могут оказаться признаками инцидентов ИБ. Такой мониторинг поможет также глубже раскрыть инцидент ИБ и идентифицировать другие системы ИТ, которые подверглись компрометации.

Может возникнуть необходимость в активизации специальных реагирований, документированных в соответствующем плане обеспечения непрерывности бизнес-процесса, которые можно применить к инцидентам ИБ как связанным, так и не связанным с ИТ. Специальные реагирования должны быть предусмотрены для всех аспектов деятельности организации, связанных не только непосредственно с ИТ, но также с поддержкой ключевых функций организации и последующего восстановления с помощью речевой сети связи и физических устройств.

Еще одной областью реагирования является восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Восстановление пораженных систем(ы), сервисов(а) и (или) сетей(и) до безопасного рабочего состояния может быть осуществлено применением «патчей» для известных уязвимостей или отключением скомпрометированных элементов. Если вследствие уничтожения журналов регистрации во время действия инцидента ИБ исчезает

весь объем информации об инциденте ИБ, может потребоваться полная перестройка системы, сервиса и (или) сети. Также может потребоваться активизация части соответствующего плана непрерывности деятельности организации.

Если инцидент ИБ, не связанный с ИТ, например, спровоцирован пожаром, наводнением или взрывом, то выполняются действия по восстановлению, документированные в соответствующем плане обеспечения непрерывности деятельности организации.

8.5.4 «Антикризисные» действия

Если инцидент ИБ не находится под контролем и должен обрабатываться в режиме «антикризисных действий», то должен использоваться предварительно разработанный план (планы).

Лучшие варианты обработки всех возможных типов инцидентов ИБ, которые могут повлиять на доступность/разрушение и, в некоторой степени, на целостность информационной системы, должны быть определены в стратегии обеспечения непрерывности деятельности организации. Эти варианты должны быть непосредственно связаны с приоритетами деятельности организации и соответствующими временными рамками восстановления бизнес-процессов и, следовательно, с максимально приемлемым временем простоя ИТ, речевой связи, персонала и размещения. В плане необходимо определить:

- предупреждающие, поддерживающие меры обеспечения непрерывности деятельности организации и устойчивости к внешним изменениям;
- организационную структуру и обязанности, связанные с управлением планирования непрерывности деятельности организации;
- структуру и основные положения плана (планов) обеспечения непрерывности деятельности организации.

План (планы) обеспечения непрерывности деятельности организации и защитные меры для поддержки активизации этого (этих) плана (планов), протестированных и признанных удовлетворительными, должны создать основу для ведения наиболее «антикризисных» действий, для которых они предназначены.

Другие типы возможных «антикризисных действий» включают в себя (но не ограничиваются) активизацией:

- средств пожаротушения и процедур эвакуации;
- средств предотвращения наводнения и процедур эвакуации;
- средств предотвращения взрыва бомбы и соответствующих процедур эвакуации;
- работы специалистов по расследованию фактов мошенничества в информационных системах;
- работы специалистов по расследованию технических атак.

8.5.5 Правовая экспертиза

Если в ходе предыдущей оценки была определена необходимость правовой экспертизы в целях доказательства значительного инцидента ИБ, правовую экспертизу проводит ГРИИБ. В целях проведения более подробной экспертизы конкретного инцидента ИБ необходимо применять следственные методы и средства, основанные на ИТ и поддерживаемые документированными процедурами, не используемые ранее в процессе менеджмента инцидентов ИБ. Такую экспертизу проводят структурным методом и определяют, что может использоваться в качестве доказательства при внутренних дисциплинарных разбирательствах или в ходе судебных процессов.

Для проведения правовой экспертизы могут использоваться технические (например: средства и методы аудита, средства восстановления свидетельств) и программные

средства, защищенные служебные помещения, а также соответствующий персонал. Каждое действие правовой экспертизы должно быть полностью документировано, включая представление соответствующих фотографий, составление отчетов об анализе результатов аудита, проверку журналов восстановления данных. Квалификация лица или лиц, проводившего (их) правовую экспертизу, должна быть документирована так же, как результаты квалификационного тестирования. Необходимо также документировать любую другую информацию, способную продемонстрировать объективность и логический характер правовой экспертизы. Все записи о самих инцидентах ИБ, деятельности, связанной с правовой экспертизой этих инцидентов, и т. д., а также соответствующие носители информации должны храниться в физически защищенной среде и контролироваться соответствующими процедурами для предотвращения доступа к ним неавторизованных лиц с целью модификации записей. Средства правовой экспертизы, основанные на применении ИТ, должны точно соответствовать правовым нормам с целью исключения возможности оспаривания этого соответствия в судебном порядке и, в то же время, в них должны учитываться все текущие изменения в технологиях. В физической среде ГРИИБ необходимо создавать необходимые условия, гарантирующие неоспоримость обработки свидетельств. В любое время для обеспечения реагирования на инцидент ИБ число персонала должно быть достаточным.

Со временем, несомненно, возникнет необходимость разработки требований к анализу свидетельств в контексте многообразия инцидентов ИБ, включая мошенничество, кражу и акты вандализма. Следовательно, для содействия ГРИИБ потребуется большее число средств, основанных на ИТ, и вспомогательных процедур для раскрытия информации, скрытой в информационной системе, сервисе и(или) сети, включая информацию, которая, на первый взгляд, кажется стертой, зашифрованной или поврежденной. Эти средства должны учитывать все аспекты, связанные с известными типами инцидентов ИБ (разумеется, они должны быть документированы в процедурах ГРИИБ).

В современных условиях в правовую экспертизу часто включают сложные среды с сетевой структурой, в которых расследование распространяется на всю операционную среду, включая множество серверов (файловый сервер, серверы печати, связи, электронной почты), а также средства удаленного доступа. Существует много инструментальных средств, включая средства поиска текстов, программное обеспечение формирования изображений и пакеты программ для правовой экспертизы. Главной целью процедур правовой экспертизы является сохранение свидетельств в неприкосновенности, их проверка на предмет противостояния любым оспариваниям в суде и проведение правовой экспертизы на точной копии исходных данных с тем, чтобы избежать сомнений в целостности исходных носителей в ходе аналитической работы.

Общий процесс правовой экспертизы должен охватывать следующие виды деятельности:

- обеспечение защиты целевой системы, сервиса и (или) сети в процессе проведения правовой экспертизы от превращения их в недоступные, изменения или от иной компрометации, включая введение вирусов, и обеспечение защиты от воздействий или минимальных воздействий на их нормальную работу;

- назначение приоритетов сбора доказательств, то есть рассмотрение их от наиболее до наименее изменчивых (что в значительной степени зависит от характера инцидента ИБ);

- идентификация всех необходимых файлов в предметной системе, сервисе и (или) сети, включая нормальные файлы, файлы, кажущиеся уничтоженными, но не являющиеся таковыми, файлы, защищенные паролем или иным образом, и зашифрованные файлы;

- восстановление как можно большего числа стертых файлов и других данных;

- раскрытие IP-адресов, имен хостов, сетевых маршрутов и информации Web-сайтов;
- извлечение содержимого скрытых, временных файлов и файлов подкачки, используемых как программное обеспечение операционной системы, так и как прикладное программное обеспечение;
- доступ к содержимому программного обеспечения защищенных или зашифрованных файлов (если это не запрещено законодательством);
- анализ всех возможно значимых данных, найденных в специальных (обычно недоступных) областях памяти на дисках;
- анализ времени доступа к файлу, его создания и изменения;
- анализ журналов регистрации системы/сервиса/сети и приложений;
- определение деятельности пользователей и (или) приложений в системе/сервисе/сети;
- анализ электронной почты на наличие исходной информации и ее содержания;
- проведение проверок целостности файлов с целью обнаружения файлов, содержащих «Троянского коня», и файлов, изначально отсутствовавших в системе;
- по возможности, анализ физических доказательств ущерба имуществу, например, отпечатков пальцев, результатов видеонаблюдения, журналов регистрации системы сигнализации, журналов регистрации доступа по пропускам и опроса свидетелей;
- обработка и хранение добытых потенциальных свидетельств так, чтобы избежать их повреждения, приведения в негодность и предотвращения просмотра конфиденциального материала несанкционированными лицами. Следует подчеркнуть, что сбор доказательств всегда должен проводиться в соответствии с правилами судопроизводства или слушания дела, для которых возможно представление данного доказательства;
- получение выводов о причинах инцидента ИБ, необходимых действиях и времени их выполнения с приведением свидетельств, включая список соответствующих файлов, включенных в приложение к главному отчету;
- обеспечение экспертной поддержки для любого дисциплинарного или правового действия (при необходимости).

Метод(ы) выполнения вышеуказанных действий должен (ны) документироваться в работе процедуры ГРИИБ.

ГРИИБ должна обладать разнообразными навыками в обширной области технических знаний (включая знание средств и методов, которые, возможно, будут использоваться нарушителем), опытом проведения анализа/расследования (с учетом защиты используемых свидетельств), знанием правовых и нормативных положений и постоянной осведомленностью о тенденциях, связанных с инцидентами ИБ.

8.5.6 Передача информации

Во многих случаях, когда ГРИИБ подтвердила реальность инцидента ИБ, возникает необходимость информирования конкретных лиц как внутри организации (вне обычных линий связи между ГРИИБ и руководством), так и за ее пределами, включая прессу. Для этого могут потребоваться несколько этапов, например: подтверждение реальности инцидента ИБ и его подконтрольности, определение инцидента ИБ как объекта «антикризисной деятельности», закрытие и завершение анализа инцидента ИБ и формирование вывода об инциденте ИБ.

Для оказания содействия такой деятельности целесообразно заранее подготовить конкретную информацию с целью быстрой адаптации ее к обстоятельствам возникновения конкретного инцидента ИБ и предоставления этой информации прессе и (или) другим средствам массовой информации. Если прессе предоставляется неполная информация, относящаяся к инцидентам ИБ, то она должна быть предоставлена в

соответствии с политикой распространения информации организации. Информация, подлежащая распространению среди общественности, должна быть проанализирована соответствующими лицами, например высшим руководством, координаторами по связям с общественностью и персоналом ИБ.

8.5.7 Расширение области принятия решений

Могут возникнуть обстоятельства, когда в решение об инциденте ИБ придется вовлекать высшее руководство, другую группу внутри организации или лицо/группу сторонней организации. Речь может идти о принятии решения относительно рекомендуемых действий, относящихся к инциденту ИБ, или дальнейшей оценке с целью определения требуемых действий. Расширение области принятия решений может потребоваться вслед за процессами оценки в соответствии с подразделом 8.4 или происходить в ходе процессов оценки, если проблема становится очевидной на ранней стадии ее обнаружения. Для тех, кому когда-либо придется принимать решение о расширении области принятия решений, то есть для группы обеспечения эксплуатации и членов ГРИИБ, необходимо иметь соответствующее описание в документации системы менеджмента инцидентов ИБ.

8.5.8 Регистрация деятельности и контроль за внесением изменений

Следует подчеркнуть, что все, кто причастен к оповещению (информированию) и менеджменту инцидентов ИБ, должны надлежащим образом регистрировать все свои действия на случай их дальнейшего анализа. Информацию об этих действиях вносят в форму отчета об инцидентах ИБ и в базу данных событий/инцидентов ИБ, непрерывно обновляемую в течение всего времени действия инцидента ИБ, от первой формы отчета до завершения анализа инцидента ИБ. Эта информация должна храниться по возможности с применением средств защиты и обеспечением соответствующего режима резервирования. Кроме того, изменения, вносимые в процессе отслеживания инцидента ИБ, обновления форм отчета и баз данных событий/инцидентов ИБ, должны вноситься в соответствии с формально принятой системой контроля за внесением изменений.

9 Этап «Анализ»

9.1 Введение

После принятия решения о закрытии инцидента ИБ необходимо провести дальнейшую правовую экспертизу и анализ с целью определения извлеченных уроков и потенциальных улучшений общей безопасности и системы менеджмента инцидентов ИБ.

9.2 Дальнейшая правовая экспертиза

Иногда после закрытия инцидента ИБ может по-прежнему сохраняться необходимость проведения правовой экспертизы с целью определения свидетельств. Она должна проводиться ГРИИБ с использованием совокупности средств и процедур в соответствии с 8.5.5.

9.3 Извлеченные уроки

После завершения инцидента ИБ важно быстро идентифицировать уроки, извлеченные из его обработки, и предпринять соответствующие действия, которые могут рассматриваться с точки зрения:

- новых или изменившихся требований к мерам защиты ИБ. Это могут быть технические или нетехнические (включая физические) меры защиты. В зависимости от извлеченных уроков требования могут включать в себя необходимость быстрого

обновления материалов и проведения инструктажа с целью обеспечения осведомленности в вопросах безопасности (для пользователей, а также для другого персонала) и выпуска руководств и (или) стандартов по безопасности;

- изменений в системе менеджмента инцидентов ИБ и ее процессах, формах отчета и базе данных событий/инцидентов ИБ.

Кроме того, при изучении урока по инциденту ИБ необходимо рассматривать полученный опыт не только в рамках отдельного инцидента ИБ, но и проводить проверку наличия тенденций (закономерностей) появления предпосылок к инцидентам ИБ, которые могут быть использованы в интересах определения потребности в защитных мерах или изменениях подходов к устранению инцидента ИБ. Целесообразно также проведение тестирования ИБ, в особенности оценки уязвимостей, после ориентированного на ИТ инцидента ИБ.

Поэтому необходимо регулярно анализировать базы данных событий/инцидентов ИБ для определения:

- тенденций/образцов;
- проблемных областей;
- областей деятельности, где можно предпринять предупредительные меры для снижения вероятности появления инцидентов в будущем.

Существенная информация, получаемая в процессе обработки инцидента ИБ, должна направляться для анализа тенденций (закономерностей), что может в значительной мере способствовать ранней идентификации инцидентов ИБ и обеспечивать предупреждение о том, какие следующие инциденты ИБ могут возникнуть на основе предшествующего опыта и документов.

Необходимо также использовать информацию об инцидентах ИБ и соответствующих им уязвимостях, полученную от государственных и коммерческих КГБР и поставщиков.

Тестирование безопасности и оценка уязвимостей информационной системы, сервиса и (или) сети, следующие за инцидентом ИБ, не должны ограничиваться только информационной системой, сервисом и (или) сетью, пораженных этим инцидентом ИБ. Тестирование безопасности и оценку уязвимостей необходимо распространить на любые связанные с ними информационные системы, сервисы и (или) сети. Детальная оценка уязвимостей используется для того, чтобы в ходе инцидента ИБ выявить существование уязвимостей в других информационных системах, сервисах и (или) сетях, и исключить вероятность появления новых уязвимостей.

Важно подчеркнуть, что оценка уязвимостей должна проводиться регулярно и повторная оценка уязвимостей, проводимая после инцидента ИБ, должна быть частью, а не заменой непрерывного процесса оценки.

Необходимо опубликовывать итоговый анализ инцидентов ИБ для обсуждения его на каждом совещании руководства организации по вопросам обеспечения ИБ и (или) на других совещаниях, касающихся вопросов по общей организационной политике ИБ.

9.4 Определение улучшений безопасности

В процессе анализа, проведенного после разрешения инцидента ИБ, новые или измененные защитные меры могут быть определены как необходимые. Рекомендации и соответствующие им требования к защитным мерам могут оказаться такими, что их немедленное внедрение будет невозможно по финансовым или эксплуатационным причинам, в этом случае они должны быть предусмотрены в более долгосрочных целях организации. Например, по финансовым соображениям невозможно за короткое время осуществить переход к более совершенным межсетевым экранам, тем не менее, решение

этого вопроса необходимо внести в долговременные цели ИБ организации (см. Раздел 10.3).

9.5 Определение улучшений системы

После разрешения инцидента руководитель ГРИИБ или назначенное вместо него лицо должны проанализировать все произошедшее с целью оценки и определения степени результативности реагирования на инцидент ИБ. Подобный анализ предназначен для выявления успешно задействованных элементов системы менеджмента инцидентов ИБ и определения потребности в любых улучшениях.

Важным аспектом анализа, проводимого после реагирования на инцидент, является возвращение информации и полученных знаний в систему менеджмента инцидентов ИБ. Если инцидент ИБ достаточно серьезен, то вскоре после разрешения инцидента необходимо провести совещание всех заинтересованных сторон, владеющих информацией о нем. На этом совещании должны рассматриваться следующие вопросы:

- работали ли должным образом процедуры, принятые в системе менеджмента инцидентов ИБ;
- существуют ли процедуры или методы, которые способствовали бы обнаружению инцидентов;
- были ли определены процедуры или средства, которые использовались бы в процессе реагирования;
- применялись ли процедуры, помогающие восстановлению информационных систем после идентификации инцидента;
- была ли передача информации об инциденте всех причастных сторон эффективной в процессе обнаружения, сообщения и реагирования.

Результаты совещания должны быть документированы и по этим результатам осуществлены конкретные согласованные действия (см. Раздел 10.4).

10 Этап «Улучшение»

10.1 Введение

Этап «Улучшение» включает в себя внедрение рекомендаций этапа «Анализ», то есть рекомендаций по улучшению результатов менеджмента и анализа рисков ИБ, безопасности и системы менеджмента инцидентов ИБ. Каждая из тем рекомендаций рассматривается ниже.

10.2 Улучшение анализа рисков и менеджмента безопасности

В зависимости от серьезности инцидента ИБ и степени его воздействия, при оценке результатов анализа рисков ИБ и менеджмента ИБ, возможно, придется учитывать новые угрозы и уязвимости. В результате завершения обновленного анализа рисков ИБ и анализа менеджмента ИБ может возникнуть необходимость внесения изменений в существующие или применения новых защитных мер.

10.3 Осуществление улучшений безопасности

Следуя рекомендациям, сделанным в процессе этапа «Анализ» (см. Раздел 9.4), и анализу нескольких инцидентов, ИБ инициируют процесс внедрения обновленных и (или) новых защитных мер. В соответствии с 9.3 это могут быть технические (включая физические) защитные меры, которые могут включать в себя потребность быстрого обновления материала для проведения инструктажей с целью обеспечения осведомленности в вопросах безопасности (для пользователей и другого персонала) и выпуска рекомендаций и (или) нормативных документов по безопасности.

Информационные системы, сервисы и сети организации должны также регулярно подвергаться анализу с целью определения уязвимостей и обеспечения процесса непрерывного повышения надежности систем/сервисов/сетей.

Анализ связанных с безопасностью процедур и документации может проводиться сразу после инцидента, но более вероятно, что это потребуется позднее. После инцидента ИБ необходимо обновить политики и процедуры обеспечения ИБ с учетом собранной информации и любых проблем, выявленных в процессе менеджмента инцидента ИБ. Долговременной целью ГРИИБ вместе с руководителем ИБ организации является распространение в организации этих обновленных вариантов политики и процедур обеспечения ИБ.

10.4 Осуществление улучшений системы

Области системы менеджмента инцидентов ИБ, предназначенные для улучшения (см. Раздел 9.5), должны быть проанализированы, а обоснованные изменения внесены в обновленный вариант документации системы. Изменения в процессах, процедурах и формах отчета системы менеджмента инцидентов ИБ должны быть тщательно проверены и протестированы перед применением на практике.

10.5 Другие улучшения

На этапе «Анализ» могли быть установлены другие улучшения, например, изменения в политиках, стандартах и процедурах ИБ, а также изменения в конфигурациях аппаратного и программного обеспечения.

Приложение А
(информационное)

Образец формы отчета о событиях и инцидентах информационной безопасности

Отчеты о событиях и инцидентах информационной безопасности

А.1 Рекомендации по заполнению

Назначением данной формы (формы отчета о событиях и инцидентах ИБ) является обеспечение информацией о событии ИБ, а затем, если оно определено как инцидент ИБ, то и об инциденте ИБ, для определенных лиц.

Если подозревается, что событие ИБ развивается или уже свершилось, особенно событие, которое может привести к существенным потерям или ущербу собственности или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная информация будет использована для инициирования соответствующего процесса оценки, который определит, должно ли это событие категорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения или ограничения потерь или ущерба, следует предпринять. Поскольку процесс оценки по своему характеру является краткосрочным, то в данный момент необязательно заполнять все поля формы отчета.

Если сотрудник является членом группы обеспечения эксплуатации, анализирующим полностью/частично заполненные формы отчета, то он должен принять решение, надо ли отнести данное событие к категории инцидента ИБ. При положительном решении сотрудник должен внести в форму отчета об инциденте ИБ как можно больше информации и передать формы отчетов о событии и инциденте ИБ в ГРИИБ. Независимо от того, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена.

Если сотрудник является сотрудником ГРИИБ, анализирующим формы отчетов о событиях и инцидентах ИБ, переданные членом группы обеспечения эксплуатации, то форма отчета об инциденте ИБ должна обновляться по ходу расследования и, соответственно, должна обновляться база данных событий/инцидентов ИБ.

При заполнении форм следует соблюдать следующие рекомендации:

- по возможности формы отчета должны заполняться и передаваться в электронном виде[*]. В случае, если существуют проблемы или считается, что существуют проблемы с принятыми по умолчанию механизмами электронного оповещения (например, электронная почта), включая случаи, когда система может подвергаться атаке и формы отчета могут быть прочитаны несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть телефон или текстовые сообщения, а также использование курьеров;
- следует представить информацию, основанную на фактах, в которой сотрудник уверен: не следует что-либо придумывать для того, чтобы заполнить все формы. Если сотрудник считает уместным включить иную информацию, которую не может

[*] Если возможно, то формы отчетов должны быть, например, на безопасной web-странице с привязкой к электронной базе данных событий инцидентов ИБ. В настоящее время основанная на бумажной технологии система является слишком медленно действующей и далеко не самой эффективной в эксплуатации.

подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее недостоверности;

- следует подробно указать, как можно связаться с сотрудником. Немедленно или спустя некоторое время может возникнуть необходимость контакта с ним для получения дальнейшей информации, касающейся представленного отчета.

Если позднее сотрудник обнаружит, что какая-либо представленная им информация неточна, неполна или ошибочна, то следует внести поправки в отчет и представить его повторно.

А.2 Форма отчета о событии информационной безопасности

Отчет о событии информационной безопасности

Дата события

Номер события*

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия	_____	Адрес	_____
Организация	_____		_____
Телефон	_____	Электронная почта	_____

Описание события ИБ

Описание события:
Что произошло
Как произошло
Почему произошло
Пораженные компоненты
Негативное воздействие на организацию
Любые идентифицированные уязвимости

Подробности о событии ИБ

Дата и время наступления события
Дата и время обнаружения события
Дата и время сообщения о событии
Закончилось ли событие? (отметить в квадрате) Да □ Нет □
Если «да», то уточнить длительность события в днях/часах/минутах

* Номера событий назначаются руководителем ГРИИБ организации.

А.2 Отчет об инциденте информационной безопасности *(продолжение)*

Дата события
Номер инцидента*

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сотруднике группы обеспечения эксплуатации

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____

Информация о сотруднике ГРИИБ

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____

Описание инцидента ИБ

Дополнительное описание события:

Что произошло
Как произошло
Почему произошло
Пораженные компоненты
Негативное воздействие на организацию
Любые идентифицированные уязвимости

Подробности об инциденте ИБ

Дата и время возникновения инцидента
Дата и время обнаружения инцидента
Дата и время сообщения об инциденте

Закончилось ли событие? (отметить в квадрате) Да □ Нет □

Если «Да», то уточнить длительность события в днях/часах/минутах. Если «Нет», то уточнить, как долго оно уже длится

* Номера инцидентов назначаются руководителем ГРИИБ организации и привязываются к номеру(ам) соответствующих событий.

А.2 Отчет об инциденте информационной безопасности *(продолжение)*

Тип инцидента ИБ

(Сделать отметку в одном из квадратов, затем заполнить ниже соответствующие поля)	Действительный	□	Попытка □	Предполагаемый	□
(Один из)	Намеренная	□	(указать типы угрозы)		
	Хищение (TH)	□	Хакерство/логическое проникновение (HA)		□
	Мошенничество (FR)	□	Неправильное использование ресурсов (MI)		□
	Саботаж/физический ущерб (SA)	□	Другой ущерб (OD)		□
	Вредоносная программа (MC)	□			
			Определить:		
(Один из)	Случайная	□	(указать типы угрозы)		
	Отказ аппаратуры (HF)	□	Другие природные события (NE)		□
	Отказ ПО (SF)	□	Определить:		
	Отказ системы связи (CF)	□	потеря значимых сервисов (LE)		□
	Пожар (HE)	□	недостаточное кадровое обеспечение (SS)		□
	Наводнение (FL)	□	другие случаи (OA)		□
			Определить:		
(Один из)	Ошибка	□	(указать типы угрозы)		
	Операционная ошибка (OE)	□	Ошибка пользователя (UE)		□
	Ошибка в эксплуатации аппаратных средств (HE)	□	Ошибка проектирования (DE)		□
	Ошибка в эксплуатации ПО (SE)	□	Другие случаи (включая ненамеренные ошибки) (OA)		□
			Определить:		
Неизвестно		□	(Если еще не установлен тип инцидента ИБ (намеренный, случайный, ошибка), то следует сделать отметку в квадрате «неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)		
			Определить:		

А.2 Отчет об инциденте информационной безопасности *(продолжение)*

Пораженные активы

Пораженные активы (при наличии)	(Дать описания активов, пораженных инцидентами ИБ или связанных с ним, включая (где требуются) серийные, лицензионные номера и номера версий)
	Информация/данные _____
	Аппаратные средства _____
	Программное обеспечение _____
	Средства связи _____
	Документация _____

Негативное воздействие/влияние инцидента на деятельность организации

Сделать отметку в соответствующих квадратах для указанных ниже нарушений, затем в колонке «значимость» указать степень негативного воздействия на деятельность организации по шкале 1 10, используя следующие сокращения (указатели категорий): (FD) — финансовые убытки/прерывание операций, (CE) — коммерческие и экономические интересы, (PI) — информация, содержащая персональные данные, (LR) — правовые и нормативные обязательства (это необходимо сравнить с английским оригиналом), (MO) — менеджмент и операции, (LG) — потеря престижа (см. примеры в Приложении В). Записать кодовые буквы в колонке «указатели», а если известны действительные издержки, — указать их в колонке «стоимость».

		Значимость	Указатели	Издержки
Нарушение конфиденциальности (то есть несанкционированное раскрытие)	□			
Нарушение целостности (то есть несанкционированная модификация)	□			
Нарушение доступности (то есть недоступность)	□			
Нарушение неотказуемости	□			
Уничтожение	□			

Общие расходы на восстановление после инцидента ИБ

	Значимость	Указатели	Издержки
(Там, где возможно, необходимо указать общие расходы на восстановление после инцидента ИБ в целом по шкале 1 10 для «значимости» и в деньгах для «стоимости»)			

А.2 Отчет об инциденте информационной безопасности *(продолжение)*

Разрешение инцидента

Дата начала расследования инцидента ИБ _____
Фамилия (ии) лица (лиц), проводившего (их) расследование инцидента _____
Дата завершения инцидента ИБ _____
Дата окончания воздействия _____
Дата завершения расследования инцидента ИБ _____
Место хранения отчета о расследовании _____

Причастные к инциденту лица/нарушители

(Один из)
Лицо (PE) □
Организованная группа (GR) □
Легально учрежденная организация/учреждение (OI) □
Случайность (AC) □
Отсутствие нарушителя (NP) □
Например, природные факторы, отказ оборудования, человеческий фактор

Описание нарушителя

Действительная или предполагаемая мотивация

(Один из)
Криминальная/финансовая выгода(CG) □
Политика/терроризм (PT) □
Развлечение/хакерство (PH) □
Месть (RE) □
Другие мотивы (OM)

Определить:

Действия, используемые для разрешения инцидента ИБ
(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением...»)

Действия, запланированные для разрешения инцидента
(включая возможные приведенные выше действия)

Прочие действия
(например, по-прежнему требуется проведение расследования, но другим персоналом)

А.2 Отчет об инциденте информационной безопасности *(продолжение)*

	Заключение	
(Сделать отметку в одном из квадратов, является ли инцидент значительным или нет, и приложить краткое изложение обоснования этого заключения (Указать любые другие заключения)	Значительный □	Незначительный □
	_____	

Оповещенные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации)	Руководитель службы ИБ □	Руководитель ГРИИБ □
	Местный руководитель (уточнить, какого подразделения) □	Руководитель информационных систем □
	Автор отчета □	Руководитель автора отчета □
	Полиция □	Другие лица □ (например, справочная служба, отдел кадров, руководство, служба внутреннего аудита, регулятивный орган, сторонняя КСБР)

Определить:

Привлеченные лица

Инициатор	Аналитик	Аналитик
Подпись _____	Подпись _____	Подпись _____
Фамилия _____	Фамилия _____	Фамилия _____
Должность _____	Должность _____	Должность _____
Дата _____	Дата _____	Дата _____
Аналитик	Аналитик	Аналитик
Подпись _____	Подпись _____	Подпись _____
Фамилия _____	Фамилия _____	Фамилия _____
Должность _____	Должность _____	Должность _____
Дата _____	Дата _____	Дата _____

Приложение Б
(информационное)

Примеры общих рекомендаций по оценке инцидентов информационной безопасности

Б.1 Введение

В настоящем приложении представлены примерные рекомендации по оценке и категорированию негативных последствий инцидентов ИБ, где каждая рекомендация имеет шкалу от 1 до 10 (1 — низкий, 10 — высокий). (На практике могут использоваться другие шкалы, например, с градацией от 1 до 5. Каждая организация должна использовать шкалу, наиболее подходящую для ее условий).

Перед изучением рекомендаций необходимо ознакомиться со следующими пояснениями:

- в некоторых из рекомендаций, представленных ниже, содержится примечание «Нет записи», для негативных последствий, приведенных для каждой градации инцидента ИБ (от 1 до 10) и идентичных для других шкал (например, с градацией от 1 до 5). Однако на некоторых градациях (по шкале от 1 до 10) для конкретных инцидентов ИБ считается, что из-за отсутствия больших различий в записях о последствиях инцидента ИБ на более низких градациях делать запись нецелесообразно и в этом случае делается примечание «Нет записи». Аналогично вышеизложенному, при более высоких градациях инцидента ИБ считается, что негативные последствия для них не могут быть серьезнее негативных последствий, показанных для самой высокой градации, и, следовательно, для этих градаций действует примечание «Нет записи». (Таким образом, было бы неправильно исключить указания с пометкой «Нет записи» и тем самым градацию шкалы);
- для приведенных рекомендаций, в которых применяются финансовые показатели, приведенные пределы колебаний кажутся несколько необычными. Перед использованием эти рекомендации должны быть дополнены нормированием колебаний курса валюты, наиболее подходящей для организации.

Таким образом, при использовании перечисляемых рекомендаций для расследования негативных последствий инцидента ИБ для деятельности организации, являющихся следствием несанкционированного раскрытия информации, несанкционированного изменения информации, отказа от использованной информации, недоступности информации и (или) сервиса, уничтожения информации и (или) сервиса, в первую очередь, необходимо определить, какая из нижеследующих категорий является соответствующей. Необходимо применять рекомендации по категорированию для определения реального негативного воздействия на бизнес-процессы («значимость») с целью занесения в форму отчета об инциденте ИБ.

Б.2 Финансовые убытки/нарушение хода операций

Последствия несанкционированного раскрытия, модификации и искажения смысла переданной информации, а также недоступности и уничтожения такой информации могут привести к финансовым убыткам, например, в результате снижения цен на акции, мошенничества или разрыва контракта по причине бездействия или запоздалых действий в отношении этих последствий. Последствиями недоступности или уничтожения любой информации может быть также нарушение бизнес-процесса. На исправление ситуации и (или) восстановление бизнес-процесса после таких инцидентов ИБ потребуются время и усилия. Эти последствия в некоторых случаях могут быть значительными и должны обязательно приниматься во внимание. Для расчетов последствий необходимо, чтобы время восстановления вычислялось в единицах рабочего времени персонала и

пересчитывалось в стоимость рабочего времени (финансовые затраты). Эти финансовые затраты должны быть вычислены, исходя из средней стоимости 1 чел.-мес по соответствующей градации/уровню, принятой/принятого внутри организации. Предлагается руководствоваться следующими рекомендациями:

1) результат в финансовых убытках/затратах x_1 или менее;
2) результат в финансовых убытках/затратах между x_1 и x_2;
3) результат в финансовых убытках/затратах между $x_2 + 1$ и x_3;
4) результат в финансовых убытках/затратах между $x_3 + 1$ и x_4;
5) результат в финансовых убытках/затратах между $x_4 + 1$ и x_5;
6) результат в финансовых убытках/затратах между $x_5 + 1$ и x_6;
7) результат в финансовых убытках/затратах между $x_6 + 1$ и x_7;
8) результат в финансовых убытках/затратах между $x_7 + 1$ и x_8;
9) результат в финансовых убытках/затратах более x_8;
10) организация завершает деятельность.

Б.3 Коммерческие и экономические интересы

Коммерческая и экономическая информация нуждается в защите и оценивается с учетом ее значимости для конкурентов или по воздействию, которое оказывает ее компрометация на коммерческие интересы. Следует руководствоваться следующими рекомендациями по обеспечению защиты информации, представляющей интерес:

1) для конкурента, но не имеет коммерческой значимости (ценности);
2) для конкурента при значении параметра ценности информации, равном y_1 или менее (коммерческий оборот);
3) для конкурента при значении параметра ценности информации, находящегося в диапазоне $У_1$+ 1 и $У_2$ (оборот) или являющегося причиной финансовых убытков, или потери заработка, или облегчающего получение незаконной прибыли, или вызывающего нарушение обязательств по поддержанию достоверности информации, поставляемой третьими сторонами;
4) для конкурента при значении параметра ценности информации, находящегося в диапазоне $У_2 + 1$ и $У_3$ (товарооборот);
5) для конкурента при значении параметра ценности информации, находящегося в диапазоне $У_3 + 1$ и $У_4$ (товарооборот);
6) для конкурента при значении параметра ценности информации более $У_4 + 1$ (оборот); а также в случаях, когда:
7) нет записи*;
8) нет записи;
9) может существенно повлиять на коммерческие интересы или подорвать финансовое состояние организации;
10) нет записи.

Б.4 Информация, содержащая персональные данные

В местах хранения и обработки информации, содержащей персональные данные физических лиц, считают моральной и этически корректной, а при некоторых обстоятельствах юридически необходимой защиту этой информации от несанкционированного раскрытия, которое может привести в лучшем случае к созданию дискомфорта у юридического лица, а в худшем — к судебному преследованию лица, раскрывшего информацию, в соответствии с требованием законодательства в части

* Термин «Нет записи» означает, что для этой градации последствий инцидента ИБ соответствующая запись отсутствует.

защиты персональных данных. В равной степени необходимо, чтобы информация, содержащая персональные данные, была всегда правильной, поскольку ее несанкционированное изменение, приводящее к появлению некорректных данных, может иметь такое же последствие, что и ее несанкционированное раскрытие. Важно, чтобы информацию, содержащую персональные данные, нельзя было сделать доступной или уничтожить, поскольку это может привести к принятию неправильных решений юридическими лицами или их бездействию во время инцидента ИБ, что может иметь такое же воздействие, что и несанкционированное раскрытие или модификация информации. Следует руководствоваться следующими рекомендациями по градации нанесения ущерба информации, содержащей персональные данные:

1) нанесение (причинение) незначительного ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

2) нанесение (причинение) ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

3) нарушение правовых, нормативных или этических требований, а также опубликование намерения относительно нарушения защиты информации, приводящее к незначительному дискомфорту конкретного лица или группы лиц;

4) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к чувству значительного дискомфорта для конкретного лица или к незначительному дискомфорту группы лиц;

5) нарушение правовых, нормативных или этических требований, а также опубликованных намерений относительно защиты информации, приводящее к серьезным проблемам конкретного лица;

6) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к серьезному дискомфорту для группы лиц;

7) нет записи;

8) нет записи;

9) нет записи;

10) нет записи.

Б.5 Правовые и нормативные обязательства

Данные, хранимые и обрабатываемые организацией, могут подчиняться правовым и нормативным обязательствам или храниться и обрабатываться с целью обеспечения соответствия деятельности организации данным обязательствам. Несоблюдение таких обязательств, намеренное или ненамеренное, может привести к принятию правовых или административных мер к лицам, работающим в данной организации. Результатом принятия данных мер могут быть штрафы и (или) тюремное заключение. Предлагается руководствоваться следующими рекомендациями:

1) нет записи;

2) нет записи;

3) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу z_1 или меньше;

4) предупреждение, гражданский иск или уголовное преступление, приводящее к финансовому ущербу/штрафу между $z_1 + 1$ и z_2;

5) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между $z_2 + 1$ и z_3 или тюремному заключению сроком до двух лет;

6) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между $z_3 + 1$ и z_4 или тюремному заключению сроком от двух до 10 лет;

7) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу или тюремному заключению сроком более 10 лет;

8) нет записи;

9) нет записи;

10) нет записи.

Б.6 Менеджмент и операции

Информация может быть такой, что ее компрометация способна нанести ущерб эффективности работы организации. Например, будучи раскрытой, относящаяся к внесению изменений в политике информация может спровоцировать такую общественную реакцию, что реализация данной политики станет невозможной. Модификация, изменение смысла переданной информации или недоступность информации, касающейся финансовых аспектов или компьютерного программного обеспечения, могут также иметь серьезные последствия для работы организации. Кроме того, отказ от обязательств по обеспечению ИБ может иметь негативные последствия для деятельности организации. Предлагается руководствоваться следующими рекомендациями по оценке последствий:

1) неэффективная работа одного подразделения организации;

2) нет записи;

3) нарушение функций (деятельности) по эффективному руководству организацией и ее работы;

4) нет записи;

5) создание препятствий для эффективной разработки или функционирования политик организации;

6) причинение ущерба организации при коммерческих или политических переговорах с другими организациями;

7) создание препятствий для разработки или функционирования главных политик организации, отключение или значительное прерывание важных операций каким-либо другим способом;

8) нет записи;

9) нет записи;

10) нет записи

Б.7 Утрата престижа

Несанкционированное раскрытие информации, отказ от обязательств по обеспечению ИБ или модификация информации, а также недоступность информации могут привести к потере престижа организации с последующим возможным нанесением ущерба ее репутации, к потере доверия и другим негативным последствиям. Предлагается руководствоваться следующими рекомендациями по оценке престижа организации:

1) нет записи;

2) создание атмосферы недовольства внутри организации;

3) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям местного/регионального масштаба;

4) нет записи;

5) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям национального масштаба;

6) нет записи;

7) значительное негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям;

8) нет записи;

9) нет записи;

10) нет записи.

Библиография

[1] СТ РК ИСО/МЭК 13335-2-1998 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных технологий. Часть 1. Общие понятия и модели для управления защитой информационных и коммуникационных технологий.

[2] СТ РК ИСО/МЭК ТО 15947-2002 Информационная технология. Методы обеспечения защиты свод правил по управлению защитой информации.

[3] СТ РК ИСО/МЭК ТО 18043-2002 Информационная технология. Методы и средства обеспечения безопасности. Рекомендации по выбору, развертыванию и эксплуатации систем обнаружения и вторжения.

[4] СТ РК ИСО 9000-2005 Государственная система технического регулирования Республики Казахстан. Комплекс стандартов систем менеджмента качества.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: менеджмент инцидентов информационной безопасности, группа реагирования на инциденты информационной безопасности, событие информационной безопасности, система менеджмента информационной безопасности

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

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