ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ

Ақпараттық технология

Қауіпсіздікті қамтамасыз ету әдістері мен құралдары

АҚПАРАТТЫ ҚОРҒАУДЫ БАСҚАРУ ҚҰРАЛДАРЫ ЖӨНІНДЕГІ ЕРЕЖЕЛЕР ЖИНАҒЫ

Информационная технология

Методы и средства обеспечения безопасности

СВОД ПРАВИЛ ПО СРЕДСТВАМ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ

ҚР СТ ISO/IEC 27002-2015

(ISO/IEC 27002:2013 «Information technology — Security techniques — Code of practice for information security controls», IDT)

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ

Ақпараттық технология

Қауіпсіздікті қамтамасыз ету әдістері мен құралдары

АҚПАРАТТЫ ҚОРҒАУДЫ БАСҚАРУ ҚҰРАЛДАРЫ ЖӨНІНДЕГІ ЕРЕЖЕЛЕР ЖИНАҒЫ

ҚР СТ ISO/IEC 27002-2015

(ISO/IEC 27002:2013 «Information technology — Security techniques — Code of practice for information security controls», IDT)

Ресми басылым

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

Астана

Алғысөз

1 «Қазақстан стандарттау және сертификаттау институты» республикалық мемлекеттік кәсіпорны **ӘЗІРЛЕП ЕНГІЗДІ**

2 Қазақстан Республикасы Инвестициялар және даму министрлігінің Техникалық реттеу және метрология комитеті Төрағасының 2015 жылғы 24 қарашадағы №236-од бұйрығымен **БЕКІТІЛІП, ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт техникалық түзетуді есепке ала отырып, ISO/IEC 27002:2013 / Cor.1:2014 «Information technology — Security techniques — Code of practice for information security controls» (Ақпараттық технология – Қауіпсіздікті қамтамасыз ету әдістері мен құралдары – Ақпаратты қорғауды басқару құралдары жөніндегі ережелер жинағы) халықаралық стандартымен бірдей.

ISO/IEC 27002 халықаралық стандартын ОТК 1 ISO/IEC ОТК 1, *Ақпараттық технологиялар,* ІК 27, *Ақпараттық қауіпсіздікті қорғау әдістері* Ішкі комитеті дайындады.

Ағылшын тілінен аударылған (en)

Осы стандарт дайындалған (әзірленген) және сілтеме берілген халықаралық стандарттардың ресми данасы Бірыңғай мемлекеттік нормативтік техникалық құжаттар қорында бар.

Стандарттардың (мемлекет аралық) сілтемелік халықаралық стандарттарға сәйкестігі туралы мәліметтер В.А қосымшасында берілген.

«Нормативтік сілтемелер» тарауында және стандарт мәтінінде сілтемелік халықаралық стандарттар өзектендірілген.

Сәйкестік дәрежесі – бірдей, IDT

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2020 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

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

Кіріспе

1 Анықтамалық ақпарат және мәнмәтін

Осы стандарт ISO/IEC 27001 стандартына негізделген ақпараттық қауіпсіздік менеджмент жүйесін (бұдан әрі – АҚМЖ) енгізу процестерін басқару тәсілдерін таңдауға көмектесетін құжат ретінде пайдалану мақсатында ұйымдар үшін әзірленді. Сонымен қатар, осы стандартты ақпараттық қауіпсіздікті басқарудың жалпы қолданыстағы құралдарын енгізетін ұйымдар қолдана алады. Осы стандарт өнеркәсіптік және ұйымдастырушылық салаға байланысты ақпараттық қауіпсіздік менеджменті жөніндегі нұсқауларда қолдануға арналған. Ақпараттық қауіпсіздік саласындағы ерекше қауіпті есепке алған жөн.

Барлық типтегі және ауқымдағы ұйымдар (қоғамдық және көпшілік секторларды, коммерциялық және коммерциялық емес ұйымдарды қоса алғанда) электрондық, нақты және вербалды (мысалы, сұхбат немесе презентация) сияқты түрлі пішімдердегі ақпаратты жинайды, өңдейді, сақтайды және жібереді.

Ақпарат маңыздылығын сөздермен, сандармен немесе суреттермен сипаттау мүмкін емес: білім, тұжырымдар, идеялар мен брэндтер ақпарат түрлерінің мысалдары болып табылады. Ақпарат, оған байланысты процестер, жүйелер, желілер мен операция барысында қолданылатын жеке деректер, онымен жұмыс істеу және оны қорғау ұйым бизнесі үшін маңызды құралдар болып табылады. Яғни, ақпаратты қорғау қажет.

Осындай құралдар саналы және кездейсоқ қауіптерге ұшырайды, ал тиісті процестер, жүйелер, желілер мен адамдардың туа бітken осалдықтары болады. Іскерлік процестер немесе жүйелерде болатын өзгерістер, сондай-ақ, сыртқы өзгерістер (жаңа заңдар немесе регламенттер сияқты) жаңа қауіпсіздік қауіптерін тудыра алады. Ұйымға зиян келтіре алатын қауіптіліктердің көптігін есепке ала отырып, ақпарат қауіпсіздігінің қауіптерін де ескерген жөн. Ақпаратты тиімді қорғау осындай қауіптерді азайтады, осылайша, ұйымды ақпараттық қауіпсіздік қауіптерінен қорғап, жоғарыда аталған құралдарға әсерді азайтады.

Ақпарат қауіпсіздігі түрлі саясаттар, процестер, процедуралар, ұйым құрылымдары, бағдарламалық жасақтама функциялары мен техника функцияларын қоса алғандағы басқару құралдарының тиісті тобын енгізу арқылы жүзеге асырылады. Осы басқару құралдарын қажеттілігіне орай қондыру, енгізу, қадағалау, тексеру және жетілдіру қажет. бұл ұйымның іскерлік мақсаттары мен қауіпсіздік мақсаттарының сәйкестігін қамтамасыз етуге мүмкіндік береді. ISO/IEC 27001 белгіленген АҚМЖ тиісті менеджмент жүйесіне негізделетін ақпараттық қауіпсіздік менеджмент жүйесін енгізу үшін ақпараттық қауіпсіздік жүйесінің қауіптеріне толық қамтылған, келісілген шолуды жасайды.

Ақпаратты ISO/IEC 27001 және осы стандартта белгіленген түрде қорғау үшін ақпараттық жүйелердің көптеген түрлері әзірленген жоқ. Техникалық құралдар арқылы қол жеткізілетін қорғаныс шектелген, сондықтан, оны тиісті басқару және процедуралармен сүйемелдеу қажет. Менеджменттің қай түрі жарамды болатынын түсіну үшін барлығын жете жоспарлап, егжей-тегжейлерге көңіл аудару қажет. Сәтті енгізілген АҚМЖ, сонымен қатар, барлық ұйым қызметкерлерінің тарабынан сүйемелдеуді талап етеді. Сондай-ақ, мүдделі тараптар, жеткізушілер немесе басқа тараптардың қатысуы талап етілуі мүмкін. Басқа тарап маманының кеңесі талап етілуі мүмкін.

Жалпы, ақпаратты тиімді қорғау бизнесті табысты жүргізуге көмектесіп, қауіпсіздікті және зияннан мүқият қорғауды қамтамасыз етеді.

2 Ақпарат қауіпсіздігінің талаптары

Ұйымның қауіпсіздік талаптарын белгілеуі маңызды болып табылады. Қауіпсіздік талаптарының 3 басты дереккөзі бар:

a. ұйымның стратегиясы мен мақсаттарын есепке ала отырып, ұйым қауіптерін бағалау. Қауіптерді бағалау арқылы қаражаттарға (активтерге) төнетін қауіп анықталады, осалдық, оқиғалардың ұқсастығы мен потенциалды әсер бағаланады;

b. ұйым, оның сауда әріптестері, келісімшарт бойынша әріптестері мен қызметтерді жеткізушілер қанағаттандыруға тиіс заңды, заңнамалық және келісімшарт талаптары. Сонымен қатар, әлеуметтік-мәдени ортаны есепке алу қажет;

c. ақпарат, оны өңдеу, сақтау, тарату және мұрағаттаумен жұмыс істеуге қоса тіркелетін принциптер, мақсаттар мен іскерлік талаптар тобы. Осы барлық процестерді өзінің қызметін жүзеге асыруда көмектесу үшін ұйым әзірледі.

Менеджмент жүйелерін енгізу үшін қолданылатын ресурстар осындай менеджмент жүйелері болмаған кезде пайда болатын бизнеске келтірілетін зиянға қарсы тұруға қабілетті болуға тиіс. Қауіпті бағалау нәтижелері қауіпсіздік қауіптерін басқару және осындай қауіптерден қорғау үшін іріктелетін менеджмент жүйелерін енгізу бойынша басымдылықтарды басқару және бөлу бойынша тиісті әрекеттерді белгілеуге көмектеседі.

ISO/IEC 27005 қауіпті бағалау, қауіптермен жұмыс істеу, жол берілетін қауіп дәрежелері, қауіптер туралы хабарлау, қауіптерді қадағалау және оларға шолу жасау бойынша кеңестерді қоса алғандағы ақпараттық қауіптерді басқару жөніндегі нұсқауды қамтиды.

3 Менеджмент жүйелерін таңдау

Менеджмент жүйелері осы стандарттан немесе басқа басқару топтарынан таңдала алады. Сонымен қатар, ерекше талаптарға сәйкес келу үшін жаңа менеджмент жүйелері әзірленуі мүмкін.

Менеджмент жүйесін таңдау қауіптің қолайлығы, қауіпке әсер ету және қауіпті басқарудың жалпы тәсілі сияқты критерийлерге негізделетін ұйым шешіміне тәуелді болады. Сонымен қатар, ұйым шешімі қолданылатын ұлттық және халықаралық заңнама мен регламенттерді есепке алып қабылдануға тиіс. Менеджмент жүйесін таңдау қорғанысты терең қамтамасыз ету үшін жүйемен жұмыс істеу түріне тәуелді болады.

Осы стандартта белгіленген басқарудың кейбір түрлері жүйе қауіпсіздігін басқаруға арналған басшылыққа алынатын принциптер ретінде қарастырыла алады және оларды көптеген ұйымдар қолдана алады. Менеджмент жүйелері нұсқауды пайдаланып, осы стандартта толығырақ сипатталған. Менеджмент жүйесін таңдау және қауіптермен жұмыс істеуге қатысты көбірек ақпаратты ISO/IEC 27005 стандартында табуға болады.

4 Өзінің нұсқауларын әзірлеу

Осы стандарт ұйымға арналған нұсқауды әзірлеу үшін негіз ретінде қарастырыла алады. Осы ережелер жинағында сипатталған басқару құралдары мен нұсқаулардың барлығы қолданылмауы мүмкін. Сонымен қатар, осы стандартқа енгізілмеген қосымша басқару құралдары мен нұсқаулар талап етілуі мүмкін. Егер әзірленетін құжаттар қосымша нұсқауларды немесе басқару құралдарын қамтыса, аудиторлар мен бизнес бойынша әріптестер тексеретін сәйкестікті қамтамасыз ету үшін айқыш сілтемелерді енгізу орынды бола алады.

5 Өміршең цикл туралы пікірлер

Ақпараттың табиғи өміршең циклі болады: түпкілікті бұзылу немесе нашарлауға дейінгі сақтау, өңдеу, пайдалану және жіберу арқылы құру. Құралдардың құндылығы өміршең цикл ішінде түрлі бола алады (мысалы, компанияның қаржы есептерін жариялағаннан кейінгі оларды рұқсатсыз жариялау немесе ұрлау қауіпті емес). Алайда, кейбір сатыларда ақпараттық қауіпсіздік өте маңызды болады.

Ақпараттық жүйелердің ақпарат қабылданатынын, анықталатынын, әзірленетінін, сыналатынын, енгізілетінін, қолданылатынын, сақталатынын және қолданыстан шығарылатынын қадағалауға болатын өміршең циклі болады. Ақпараттық қауіпсіздік әр сатыда өте маңызды. Жүйелердің жаңа әзірлемелері мен бар жүйелерге енгізілген өзгерістер ұйымдарға ақпараттық қауіпсіздік оқиғалары мен қауіптерін есепке ала отырып, қауіпсіздік жүйесін басқаруды жаңарту және жетілдіру бойынша мүмкіндіктер береді.

6 Ұқсас ақпаратты қамтитын стандарттар

Осы стандарт көптеген ұйымдарда қолданылатын көптеген ақпараттық қауіпсіздік менеджмент жүйелері жөніндегі нұсқауларды қамтиды, ал ISO/IEC 27000 сериясының қалған стандарттары қосымша кеңестерді немесе ақпараттық қауіпсіздіктің басқа аспектілеріне қойылатын талаптарды қамтиды.

ISO/IEC 27000 сериясы АҚМЖ-не және осы стандарттар сериясына жалпы кіріспені қамтиды. ISO/IEC 27000 стандарты ISO/IEC 27000 сериясының стандарттарындағы терминдерді қамтитын глоссарийді қамтиды және осы серияның әр стандартының қолданылу саласы мен мақсаттарын сипаттайды.

Мазмұны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ

Ақпараттық технология

Қауіпсіздікті қамтамасыз ету әдістері мен құралдары

АҚПАРАТТЫ ҚОРҒАУДЫ БАСҚАРУ ҚҰРАЛДАРЫ ЖӨНІНДЕГІ ЕРЕЖЕЛЕР ЖИНАҒЫ

Енгізілген күні 2017–01–01

1 Қолданылу саласы

Осы стандарт ақпараттық қауіптің ұйымдастырушылық ортасын есепке ала отырып, басқару жүйелерін іріктеу, енгізу және басқаруды қоса алғандағы ақпараттық қауіпсіздік пен ақпаратты қорғауды басқару жөніндегі ұйымдастырушылық стандарттарға арналған нұсқауды қамтиды.

Осы стандарт ұйымдар үшін келесі мақсаттарда әзірленген:

a) [10] негізінде СМИБ енгізу барысында менеджмент жүйесін таңдау;

b) жалпы қолданыстағы ақпараттық қауіпсіздікті басқару жүйелерін енгізу;

c) ақпаратты қорғауды басқару жөніндегі жеке нұсқауларды әзірлеу.

2 Нормативтік сілтемелер

Осы стандартты (құжатты) қолдану үшін келесі сілтемелік құжаттар қажет. Күні қойылмаған сілтемелер үшін сілтемелік құжаттың соңғы басылымын (барлық өзгертулерін қоса алғанда) қолданады.

ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Жалпы шолу және сөздік)

3 Терминдер мен анықтамалар

Осы стандартта ISO/IEC 27000 бойынша терминдер қолданылады.

4 Осы стандарт құрылымы

Осы стандарт қауіпсіздікті басқару жүйелері жайлы 14-тарауды қамтиды. Оларда 35 басты қауіпсіздік санаттары мен 114 басқару жүйелері бар.

4.1 Тараулар

Қауіпсіздікті басқару жүйелерінің анықтамаларын қамтитын әр тарауда бір немесе одан артық басты қауіпсіздік санаттары болады.

Осы стандарттағы тараулар тәртібі қандай да болмасын тарау маңыздылығын білдірмейді. Жағдайларға тәуелді түрлі қауіпсіздік менеджменті жүйелері маңызды бола алады. Осы стандартты қолданатын әр ұйым менеджмент жүйелерін, олардың маңыздылығын және оларды бөлек кәсіби процестерге қолданылуын белгілеуі тиіс. Сонымен қатар, осы стандартта берілген тізімдегі тәртіп басымдылық дәрежесіне орай қалыптастырылмаған.

4.2 Басқару жүйелерінің санаттары

Қауіпсіздік менеджменті жүйелерінің әр санаты келесілерді қамтиды:

a) қол жеткізуге қажет басқару жүйесінің мақсаты;

b) қауіпсіздік жүйесінің мақсатына қол жеткізу үшін қолданылатын бір немесе одан артық басқару жүйелері.

Қауіпсіздік жүйесінің сипаты келесідей әзірленген:

Менеджмент жүйесі

Басқару жүйесінің мақсатына сәйкес келетін басқару жүйесінің ерекше спецификациясының анықтамасы

Басқару жүйелерін енгізу жөніндегі нұсқау

Басқару жүйесін енгізу және басқару жүйесі мақсатының сәйкес келуі үшін қажетті толық ақпаратты қамтиды. Нұсқау барлық жағдайлар үшін жарамды немесе жеткілікті бола алмайды. Сонымен қатар, нұсқау басқару жүйелерінің ерекше ұйымдастырушылық талаптарының орындалуына көмектесе алмайды.

Басқа ақпарат

Қарастыруға қажет ақпаратты қамтиды. Мысалы, заңдылық түсініктері мен басқа стандарттарға жасалған сілтемелер. Егер осы тарау болмаса, бұл мұндай ақпарат жоқ дегенді білдіреді.

5 Ақпараттың қауіпсіздік саясаты

5.1 Ақпараттық қауіпсіздік бағытын басқару

Мақсаты: Жоғары басшылықтың бизнес талаптары мен тиісті заңдар мен нормаларға сәйкес ақпараттық қауіпсіздікті басқару мен сүйемелдеуді қамтамасыз етуі.

5.1.1 Ақпараттық қауіпсіздік саясатын құжаттау

Бақылау және басқару шаралары мен құралдары

Ақпараттық қауіпсіздік саясатын басшылық бекітіп, басып шығарып, ұйымның барлық қызметкерлері мен тиісті шеттегі ұйымдардың қызметкерлеріне мәлімденуі тиіс.

Іске асыру жөніндегі ұсыныстар

Ақпараттық қауіпсіздік саясаты басшылық жауапкершілігін белгілеп, ұйымның ақпараттық қауіпсіздікті басқару тәсілін сипаттау қажет.

Саясат сипатталған құжатта келесілерге қатысты ережелер қамтылуы тиіс:

a) бизнес-стратегия;

b) регламенттер, заңдар мен келісімшарттар;

c) ақпараттық қауіпсіздік ортасына төнетін қазіргі уақыттағы және болжалды қауіптілік.

Ақпараттық қауіпсіздік саясаты келесілер жайлы ережелерді қамтуы тиіс:

a) ақпараттық қауіпсіздікті, ақпараттық қауіпсіздікке қатысты барлық әрекеттерді басқаратын мақсаттар мен принциптерді белгілеу;

b) ақпараттық қауіпсіздікті басқару үшін негізгі және ерекше жауапкершілікті түрлі адамдар арасында бөлу;

c) ауытқулар мен ерекше жағдайлармен жұмыс істеуге көмек беретін процестер.

Төмен деңгейде ақпараттық қауіпсіздік саясаты тақырыптар саясаты арқылы сүйемелденеді. Ол арқылы ақпараттық қауіпсіздікті басқару жүйелерін енгізуге көмек беруге болады. Осы тақырыптар ұйым шеңберінде белгілі мақсатты топтың барлық талаптарын қанағаттандыратындай немесе басқа белгілі тақырыптарға жауапты болатындай әзірленген.

Осындай тақырыптар мысалдары:

a) қолжетімділікті басқару (9-тарауды қараңыз);

b) ақпаратты жіктеу (онымен жұмыс істеу) (8.2 қараңыз);

c) нақты қауіпсіздік пен орта қауіпсіздігі (11-тарауды қараңыз);

d) соңғы тұтынушыға бағытталған тақырыптар:

1) активтердің қолжетімді қолданысы (8.1.3 қараңыз);

2) таза жұмыс үстелі мен экран (11.2.9 қараңыз);

3) ақпаратты жіберу (13.2.1 қараңыз);

4) мобильді құрылғылар мен телеөңдеу (6.2 қараңыз);

5) бағдарламалық жасақтаманы орнату және пайдалану бойынша шектеулер (12.6.2 қараңыз);

e) жүйені кейін шегіндіру (12.3 қараңыз);

f) ақпаратты жіберу (13.2 қараңыз);

g) хакер бағдарламаларынан қорғау (12.2 қараңыз);

h) техникалық осалдықты басқару (12.6.1 қараңыз);

i) криптографияны басқару жүйелері (10-тарауды қараңыз);

j) коммуникацияларды қорғау (13-тарауды қараңыз);

k) дербес анықталатын ақпараттың құпиялылығы мен оны қорғау (18.1.4 қараңыз);

l) жеткізушімен байланыс (15-тарауды қараңыз).

Осы ақпараттық қауіпсіздік саясаты барлық ұйым шеңберінде тұтынушыларға өзекті, қолжетімді және түсінікті формада жеткізілуі тиіс. Мысалы, «ақпараттық қауіпсіздік, білім алу және оқыту бағдарламалары туралы хабардарлық» мәнмәтінінде (7.2.2 қараңыз).

Басқа ақпарат

Ақпараттық технологияның сыртқы саясатында қажеттілік барлық ұйымдарда ерекшеленеді. Ішкі саясат басқару жүйелерінің болжалды деңгейлерін белгілеу және мақұлдау басқару жүйелерін қарапайым енгізуден немесе саясатты адамдарға немесе ұйым функцияларына қатысты қолданатын жағдайлардан бөлек болатын ірі және күрделі ұйымдарда аса пайдалы болады. Ақпараттық қауіпсіздік саясаты жалпы саясат жөніндегі құжаттың бөлігін немесе өзара байланысты бөлек құжаттар тобын құрай алады.

Кейбір ұйымдар осындай құжаттар үшін басқа терминдерді қолданады. Мысалы, «Стандарттар», «Директивалар» немесе «Ережелер».

5.1.2 Ақпараттық қауіпсіздік саясатын қайта қарау

Бақылау және басқару шаралары мен құралдары

Ақпараттық технология саясаты жоспарланған уақыт аралықтары өткен сайын немесе оның өзектілігін, дұрыстығын және тиімділігін қамтамасыз ету мақсатында елеулі өзгерістер енгізілген жағдайда қайта қаралуы тиіс.

Іске асыру жөніндегі ұсыныстар

Ақпараттық қауіпсіздік саясатының басшылықпен қауіпсіздік саясатын әзірлеуге, қайта қарауға және бағалауға жауапты ретінде бекітілген иесі болуы тиіс. Қайта қарау ұйымдастырушылық ортаның, бизнес жағдайларының, құқықтық шарттар немесе техникалық ортаның өзгерісіне жауап ретінде ұйымның ақпараттық қауіпсіздік саясатын және ақпаратты қорғауды басқару тәсілдерін жақсарту бойынша мүмкіндіктерді бағалау болып табылады.

Ақпараттық қауіпсіздік саясатын қайта қараған кезде, басқару әдістерін қайта қарау нәтижелерін есепке алған жөн.

Қайта қаралған басқару саясатын мақұлдау алынуы тиіс.

6 Ақпараттық қауіпсіздіктің ұйымдастырушылық аспектілері

6.1 Ұйым ішінде шешілетін мақсаттар

Мақсаты: Ақпараттық қауіпсіздікті ұйым шеңберінде басқару.

Бақылау және басқару шаралары мен құралдары

Ақпараттық қауіпсіздікті басқару бойынша барлық міндеттер анық белгіленуі тиіс.

Іске асыру жөніндегі ұсыныстар

Ақпараттық қауіпсіздікті басқару жөніндегі міндеттерді бөлуді ақпараттық қауіпсіздік саясатына сәйкес жүзеге асырған жөн (5.1.1 қараңыз). Бөлек активтерді қорғау және ақпараттық қауіпсіздікке байланысты нақты процестерді орындау бойынша міндеттерді анық белгілеген жөн. Осындай міндеттерді, қажеттілігіне орай, нақты пайдалану жерлері мен ақпаратты өңдеу құралдарына арналған толық нұсқаулармен толықтырған жөн. Активтерді қорғау және қауіпсіздікке байланысты ерекше процестерді жүзеге асыруға қатысты нақты міндеттер, мысалы, бизнестің үздіксіздігін жоспарлау, анық белгіленуі тиіс.

Қауіпсіздікті қамтамасыз ету бойынша міндет жүктелген тұлғалар қауіпсіздікке байланысты міндеттерді басқа тұлғаларға беруге құқылы. Алайда, олар жүктелген міндеттердің орындалуына жауапты болып қалады.

Әр басшының міндеттер аясы анық белгіленуі тиіс, соның ішінде:

a) әр нақты жүйеге байланысты қауіпсіздік активтері мен процестері (процедуралары) анық белгіленуі тиіс;

b) әр актив немесе қауіпсіздік процедурасына жауапты тұлғаларды тағайындап, олардың міндеттерін тиісті құжаттарда толық сипаттау қажет (8.1.2 қараңыз);

c) өкілеттілік деңгейлері анық белгіленіп, құжат түрінде ресімделуі тиіс;

d) ақпараттық қауіпсіздік саласындағы міндеттерді орындау мүмкіндігі. Тағайындалған қызметкерлер осы салада бәсекеге қабілетті болып, олардың дамуға сәйкес келу мүмкіндігі болуы тиіс;

e) ақпараттық қауіпсіздік аспектілерін үйлестіру және оларға шолу құжаттамада белгіленіп көрсетілуі тиіс.

Басқа ақпарат

Көптеген ұйымдарда қауіпсіздікті әзірлеу және іске асыруға және бақылау және басқару шаралары мен құралдарын белгілеуге жалпы жауапкершілік жүктелетін ақпараттық қауіпсіздік жөніндегі менеджер тағайындалады.

Алайда, бақылау және басқару шаралары мен құралдарының ресурстарын іздеу және оны іске асыруға қатысты міндеттер бөлек менеджерлерге бөлінеді. Жалпы қолданыстағы тәжірибе күн сайынғы қорғанысқа жауапты әр актив иесін тағайындау болып табылады.

6.1.2 Міндеттерді бөлу

Менеджмент жүйесі

Жауапкершілік саласындағы қарама-қайшы міндеттер ұйым активтерін заңсыз немесе байқаусыз өзгерту немесе дұрыс емес пайдалану мүмкіндігін азайту үшін бөлінуі тиіс.

Іске асыру жөніндегі ұсыныстар

Ешбір адам активтерді рұқсатсыз немесе анықтаусыз өзгерте, пайдалана алмау үшін немесе оларға қолжетімділік алмау үшін шаралар қабылдануы тиіс. Оқиғаны бастауды оған рұқсат беруден бөлген жөн. Басқару элементтерін жобалаған кезде, құпия келісім мүмкіндігін есепке алған жөн.

Кіші ұйымдар міндеттерді бөлуді аса күрделі деп санауы мүмкін, бірақ принцип мүмкіндіктер мен пайдалылығына орай қолданылуы тиіс. Бөлу күрделі болған жағдайда да, қызмет мониторингі, басқару аудиті мен оны қадағалау сияқты басқа басқару жүйелері қарастырылуы тиіс.

Басқа ақпарат

Міндеттерді бөлу ұйым активтерін байқаусыз немесе әдейі дұрыс емес пайдалану қаупін төмендету тәсілі болып табылады.

6.1.3 Түрлі инстанциялармен байланыс

Бақылау және басқару шаралары мен құралдары

Түрлі инстанциялармен тиісті байланыстар сүйемелденуі тиіс.

Іске асыру жөніндегі ұсыныстар

Ұйымдарда қандай инстанциялармен (мысалы, құқық қорғаушы, өрт сөндіруші және бақылау органдары) және қашан байланысқа түсу қажеттілігін және заңды бұзу мүмкіндігі туралы күдік болған жағдайда, анықталған ақпараттық қауіпсіздік оқиғалары туралы қалай уақтылы хабарлау қажеттілігін белгілейтін процедуралар қолданылуы тиіс.

Қосымша ақпарат

Интернет арқылы шабуылға ұшырайтын ұйымдарға шабуыл көзіне қарсы шаралар қабдылдау үшін сыртқы үшінші тарапты (мысалы, Интернет-қызметтер провайдері немесе телекоммуникациялық оператор) тарту қажет болуы мүмкін.

Осындай байланыстарды жүзеге асырған кезде, ақпараттық қауіпсіздік оқиғаларының менеджменті процесін (16-тарауды қараңыз) немесе бизнес үздіксіздігі мен төтенше жағдайлардағы әрекеттерді жоспарлау процесін (17-тарауды қараңыз) сүйемелдеу қажет болуы мүмкін. Сонымен қатар, ұйым сақтауға тиісті заңдар немесе нормаларда болжалды өзгерістерді болжау және оларға дайындалу үшін реттеуші органдармен байланысты сүйемелдеген жөн. Басқа инстанциялармен байланыстар коммуналдық қызметтермен, жедел көмек пен еңбекті қорғау қызметтерімен байланысты қамтиды, мысалы, өрт сөндіру органдары (бизнес үздіксіздігіне байланысты), телекоммуникациялық қызмет провайдерлері (байланыс желілерін тартуға және олардың қолжетімділігіне байланысты), сумен жабдықтау қызметтері (жабдықтарды салқындату құралдарына байланысты).

6.1.4 Бақылау және басқару шаралары мен құралдары

Мамандандырылған кәсіби топтармен немесе қауіпсіздік жөніндегі форумдар қатысушыларымен, сондай-ақ, кәсіби бірлестіктермен тиісті байланыстар сүйемелденуі тиіс.

Іске асыру жөніндегі ұсыныстар

Мамандандырылған топтар немесе формудардағы мүшелікті келесілерге арналған құрал ретінде қарастыру қажет:

a) ақпараттық қауіпсіздік саласында заманауи деңгейдегі «озық тәжірибе» мен жетістіктер туралы білімді арттыру;

b) ақпараттық қауіпсіздік мәселелерін түсіну заманауи және толық екендігін қамтамасыз ету;

c) ескерту, ақпараттық хабарландырулар мен патч түрінде ерте хабарландырулар алу;

d) ақпараттық қауіпсіздік мәселелері бойынша мамандардың кеңестерін алу мүмкіндігі;

e) жаңа технологиялар, өнімдер, қауіптер немесе осалдықтар туралы ақпаратты бірлесіп пайдалану және онымен алмасу;

f) ақпараттық қауіпсіздік оқиғаларын талқылау үшін адекватты байланысу нүктелерін қамтамасыз ету (16-тарауды қараңыз).

Қосымша ақпарат

Қауіпсіздік мәселелері бойынша ынтымақтастық пен үйлестікті арттыру мақсатында ақпаратты бірлесіп пайдалану туралы келісімдер орнатылуы мүмкін. Осындай келісімдерде осал ақпаратты қорғауға қатысты талаптар белгіленуі тиіс.

6.1.5 Жобаны басқарған кездегі ақпараттық қауіпсіздік

Басқару жүйелері

Жобаны басқарған кезде жоба типіне тәуелсіз ақпараттық қауіпсіздік есепке алынуы тиіс.

Іске асыру жөніндегі ұсыныстар

Ақпараттық қауіпсіздік қауіптері жоба шеңберінде анықталуын және шешілуін қамтамасыз ету үшін ақпараттық қауіпсіздік ұйым жобасын басқару әдісіне біріктірілуі тиіс. Бұл сипатына тәуелсіз кез келген жобаға қатысты болады. Мысалы, базалық бизнес-процесс, IT, ғимараттар мен басқа қосымша процестерді басқаруға арналған жоба. Жобаларды басқару әдістері қолданыста келесілерді талап етеді:

a) ақпараттық қауіпсіздік мақсаттары жоба мақсаттарына енгізіледі;

b) қажетті басқару жүйелерін белгілеу үшін ақпараттық қауіпсіздік қаупін бағалау жобаның ерте сатысында өткізіледі;

c) ақпараттық қауіпсіздік қолданылатын жоба әдіснамасының барлық сатыларының бөлігі болып табылады.

Ақпараттық қауіпсіздік салдарлары қарастырылып, барлық жобаларды жүйелі түрде қайта қаралады. Ақпараттық қауіпсіздікке жауапкершілік белгіленіп, жобаларды басқару әдістерінде белгіленген ерекше қызметкерлер анықталуы тиіс.

6.2 Мобильді құрылғылар мен телеөңдеу

Мақсаты: Телеөңдеу және мобильді құрылғыларды пайдалану қауіпсіздігін қамтамасыз ету.

6.2.1 Мобильді құрылғыларға қатысты саясат

Басқару жүйелері

Саясат пен сүйемелдеуші қауіпсіздік шаралары мобильді құрылғылар жұмысына байланысты қауіптерді басқару үшін қабылдануы тиіс.

Іске асыру жөніндегі ұсыныстар

Мобильді құрылғыларды пайдаланған кезде, бизнес туралы ақпарат зақымданбауын қамтамасыз етуге көңіл аудару қажет. Мобильді құрылғылар саясаты қорғалмаған ортада мобильді құрылғылармен жұмыс істеу қауіптерін назарға алуы тиіс.

Мобильді құрылғылар саясаты келесілерге көңіл аударуы қажет:

a) мобильді құрылғыны тіркеу;

b) жеке қорғаныс талаптары;

c) бағдарламалық жасақтаманы орнату бойынша шектеу;

d) мобильді құрылғылардың бағдарламалық жасақтамасының нұсқалары мен қолданылатын патчтарға қойылатын талаптар;

e) ақпараттық қызметтермен байланысты шектеу;

f) қолжетімділікті басқару;
g) криптографиялық техника;
h) хакер бағдарламаларынан қорғау;
i) ақпаратты қашықтықтан сөндіру, бұзу және бұғаттау;
j) жүйені кейін шегіндіру;
k) веб-қызметтер мен веб-қосымшаларды пайдалану.

Мобильді құрылғыларды қоғамдық жерлерде, конференц-залдарда және басқа қорғалмаған жерлерде пайдаланған кезде мұқият болған жөн. Қорғаныс осы құрылғыларда сақталатын және өңделетін ақпаратқа заңсыз қолжетімділікті немесе сол ақпаратты жариялауды болдыртпауға қабілетті болуы тиіс. Мысалы, криптографиялық әдістерді қолдану арқылы (10-тарауды қараңыз) немесе сәйкестендірудің құпия ақпаратын пайдалануды іске асыру (9.2.4 қараңыз).

Мобильді құрылғылар, сондай-ақ, әсіресе олар жоғалған кезде, ұрлаудан нақты түрде қорғалуы тиіс. Мысалы, автомобильдер мен басқа көлік түрлерінде, қонақ үй бөлмелерінде, конференц-орталықтарда және кездесу орындарында. Мобильді құрылғы ұрланған немесе жоғалған жағдайда, ұйымдағы заң, сақтандыру және басқа қауіпсіздік талаптарын есепке алатын белгілі процедура белгіленуі тиіс. Маңызды немесе аса маңызды бизнес-ақпарат сақталған құрылғыларды қараусыз қалдыруға болмайды. Мүмкіндігіне орай, оларды қауіпсіз жерде ұстаған немесе құрылғының қауіпсіздігін қамтамасыз ету үшін арнаулы құлыптарды пайдаланған жөн.

Мобильді құрылғыларды пайдаланатын персоналдың осы жұмыс істеу тәсіліне байланысты қосымша қауіптер мен пайдаланылуға тиісті басқару жүйелері туралы хабардарлығын арттыру үшін оларға оқыту жүргізілуі тиіс.

Егер мобильді құрылғылар саясаты мобильді құрылғыларды жеке меншікте пайдалануға мүмкіндік берсе, саясат пен оған байланысты қауіпсіздік шаралары келесілерді есепке алуы тиіс:

Басқа саясат

Сымсыз мобильді құрылғылар бойынша қосылыстар желі қосылыстарының типі болып табылады. Алайда, олардың басқару жүйелерін белгілеген кезде есепке алынуға тиісті кейбір айырмашылықтары болады. Айырмашылықтар:

a) кейбір қауіпсіздік хаттамалары жеткіліксіз және олардың кейбір осал жерлері болады;
b) мобильді құрылғыларда сақталатын ақпарат жоспарланған ақпаратты қайтару сәтіндегі желінің өткізу қабелеттілігіне немесе мобильді құрылғы қосылысының болмауына байланысты қайтарыла алмайды.

Әдетте, мобильді құрылғылардың тіркелген пайдалану құрылғыларымен ортақ функциялары болады. Мысалы, Интернетке кіру желілері, электрондық пошта мен файлдарды өңдеу. Мобильді құрылғыларға арналған ақпараттық қауіпсіздікті басқару негізінен тіркелген қолданыстағы негізгі құрылғылар мен ұйым аумағынан тыс пайдалануға байланысты қауіптерді жоятын құрылғылар үшін қабылданған принциптерден тұрады.

6.2.2 Телеөңдеу

Басқару жүйелері

Саясат пен сүйемелдеуші қауіпсіздік шаралары телеөңдеу жерлерінде қолжетімді, өңделген немесе сақталатын ақпаратты қорғау үшін іске асырылуы тиіс.

Іске асыру жөніндегі ұсыныстар

Телеөңдеуге рұқсат беретін ұйымдар телеөңдеуді пайдалану шарттары мен шектеулерін белгілейтін саясатты әзірлеуі тиіс. Егер телеөңдеуді пайдалануға жол беріліп, заңды түрде рұқсат етілсе, келесі мәселелер қарастырылуы тиіс:

a) ғимараттың нақты қауіпсіздігі мен жергілікті қоршаған ортаны есепке алатын телеөңдеу жерлерінің нақты қауіпсіздігі;

b) ұсынылған нақты телеөңдеу ортасы;

c) ішкі жүйенің байланыс желілері бойынша өтетін және кіру рұқсатын алатын ақпаратты қабылдауды, жүйенің ішкі жүйелеріне қашықтықтан кіру рұқсаты қажеттілігін есепке алатын коммуникациялардың қауіпсіздік талаптары;

d) жеке жабдықта ақпаратты өңдеу және сақтауды болдыртпайтын виртуалды жұмыс үстеліне кіру рұқсатын беру;

e) заңсыз тұлғалардың құрылғыларды пайдалану арқылы ақпараттар немесе ресурстарға заңсыз қол жеткізу қаупі. Мысалы, отбасы мүшелері мен достар;

f) үй желілерін пайдалану және сымсыз желі қызметтерінің конфигурацияларының талаптары немесе шектеулері;

g) жеке жабдықта әзірленген зияткерлік меншікке құқықтарға байланысты дауларды болдыртпауға арналған саясат пен процедуралар;

h) заңнама арқылы болдыртауға болатын жеке жабдыққа қол жеткізу (құрылғы қауіпсіздігін тексеру үшін немесе тергеу кезінде);

i) ұйым жеке қызметкерлердің немесе сыртқы тұтынушылардың жұмыс станцияларында клиент бағдарламалық жасақтамасын лицензиялауға жауапты болуы мүмкін бағдарламалық жасақтама туралы лицензиялық келісімдер;

j) зарарлы бағдарламалар мен брандмауэрлардан қорғау.

Басшылыққа алынатын принциптер мен механизмдер келесілерді қамтуы тиіс:

a) ұйым бақылауынан тыс жеке жабдықты пайдалануға тыйым салынған жерлерде телеөңдеу құрылғыларын сақтауға арналған тиісті жабдықтар мен жиһазды ұсыну;

b) жүргізілуі мүмкін рұқсат етілген жұмысты, жұмыс сағаттарын, ақпарат жіктелуін және қашықтықтан жұмыс істейтін қызметкер кіре алатын ішкі жүйелер мен қызметтерді белгілеу;

c) тиісті байланыс жабдықтарын ұсыну, соның ішінде, қашықтықтан кіруді қамтамасыз ету әдістері;

d) нақты қауіпсіздік;

e) жабдықтар мен ақпаратқа отбасы мүшелері мен қонақтардың қолжетімділігі мәселелері жөніндегі ережелер мен ұсыныстар;

f) аппараттық және бағдарламалық жасақтамаларды ұсыну мен техникалық қызмет көрсету;

g) сақтандыруды ұсыну;

h) резервтік көшіру және бизнес үздіксіздігін қамтамасыз етуге арналған процедуралар;

i) қауіпсіздікті қамтамасыз етуге арналған аудит пен мониторинг;

j) телеөңдеу бойынша жұмыс тоқтатылған кезде, биліктен және кіру құқығынан айыру және жабдықты қайтару.

Басқа ақпарат

Телеөңдеу офистен тыс жұмыстың барлық пішімдеріне, соның ішінде, дәстүрлі емес жұмыс шарттарына қатысты болады. Осындай жұмысты «қашықтықтан жұмыс істеу», «икемді жұмыс орны» және «виртуалды жұмыс» деп атайды.

7 Жұмыс персоналының қауіпсіздігі

7.1 Жұмысқа орналасар алдында

Мақсаты: Қызметкерлер, мердігерлер мен үшінші тарап өкілдері өзінің міндеттерін түсінгендігін және оларға тағайындалған қызметтерді орындауға және ақпаратты өңдеу

құралдарын ұрлау, оларға қатысты айлакерлік жасау немесе оларды мақсатқа сай пайдаланбау қауіптерін төмендетуге қабілетті екендігін қамтамасыз ету.

Басқару шаралары

Тұрақты жұмысқа алынатын барлық кандидаттарды, мердігерлерді және үшінші тарап өкілдерін мұқият тексеру бизнес талаптарына, кіру рұқсаты берілетін ақпарат жіктелуіне және болжалды қауіптерге пропорционал түрде тиісті заңдарға, нұсқаулықтарға және этика қағидаларына сәйкес жүргізілуі тиіс.

Іске асыру жөніндегі ұсыныстар

Тексерік барысында құпиялылықты, дербес деректердің қорғалуын және (немесе) еңбек заңнамасын есепке алған жөн. Осындай тексеріс келесі элементтерді қамтуы тиіс:

a) жақсы мінездемелердің болуы, соның ішінде, үміткердің кәсіби және жеке қасиеттеріне қатысты;

b) үміткер биографиясын тексеру (биография толықтығы);

c) белгіленген білім деңгейі мен кәсіби біліктілікті растау;

d) жеке басын куәландыратын құжаттардың (паспорт немесе оны ауыстыратын құжат) түпнұсқалығын тәуелсіз түрде тексеру;

e) толығырақ тексеріс, мысалы, кредит төлеу қабілеті немесе сотталғандықтың болуы.

Қызметкер жұмысқа ақпараттық қауіпсіздік бойынша ерекше маман ретінде қабылданған кезде, ұйым:

a) үміткердің осы жұмысқа арналған тиісті құзыреті болуына;
b) егер қызмет ұйым үшін аса маңызды болса, үміткерге осы қызметті беруге сенімді болуы тиіс.

Жұмысқа қабылдағаннан кейін дереу немесе келешекте жаңа қызметкерге ақпаратты өңдеу құралдарына, соның ішінде, осал ақпаратты өңдейтін құралдарға, мысалы, қаржы немесе құпия ақпарат, қолжеткізілім берілген жағдайда, ұйым қосымша, толығырақ тексеріс өткізген жөн.

Процедуралар тексеріс процесінің критерийлері мен шектеулерін белгілеуі тиіс, мысалы, кім қызметкерлерді тексеруге құқылы, осы тексеріс қалай, қашан және қандай мақсатта жүргізіледі.

Алдын ала тексерісті мердігерлер мен үшінші тарап өкілдері үшін де өткізген жөн. Мердігерлер кадрлық агенттік арқылы ұсынылған жағдайда, агенттікпен жасалған келісімшарт агенттіктің үміткерлерді алдын ала тексеру және алдын ала тексеріс аяқталмаған немесе оның нәтижелері күдік тудырған жағдайда, мәлімдеу процедуралары бойынша міндеттерін анық белгілеуі тиіс.

Ұйымдағы қызметтерге орналасуға талаптанатын барлық қарастырылатын кандидаттар туралы ақпаратты тиісті заң құзыретіне қарасты заңнамаға сәйкес жинап, өңдеген жөн. Қолданылатын заңнамаға тәуелді осы кандидаттар алдын ала тексеріске байланысты қызмет туралы алдын ала хабарлануы тиіс.

7.1.2 Жұмысбастылық шарттары

Басқару шаралары

Жұмысқа үміткер мен ұйым арасындағы келісімшарт жасау туралы келесімдерде ақпараттық қауіпсіздікке жауапкершілік анық белгіленуі тиіс.

Іске асыру жөніндегі нұсқау

Жұмысбастылық шарттары ұйымның қауіпсіздік саясатын көрсетіп, сонымен қатар, келесілер түсіндіруі және белгілеуі тиіс:

a) осал ақпаратқа қолжетімділігі бар барлық қызметкерлер, мердігерлер мен үшінші тарап өкілдеріне ақпаратты өңдеу құралдарына қолжетімділік берілгенге дейін, олар құпиялылық немесе жарияламау туралы келісімге қол қоюы тиіс (13.2.4 қараңыз);

b) қызметкерлердің, мердігерлердің және кез келген басқа клиентердің құқықтық жауапкершілігі мен құқықтары, мысалы, авторлық құқық туралы заңдарға немесе дербес деректерді қорғау туралы заңнамаға қатысты (18.1.2 және 18.1.4 қараңыз);

c) ақпараттық жүйелер мен қызметтерге байланысты ақпаратты жіктеуге және ұйым активтерінің менеджментіне қатысты міндеттерді қызметкер, мердігер немесе үшінші тарап өкілі орындайды (8-тарауды қараңыз);

d) басқа фирмалар мен шеттегі ұйымдардан қабылданатын ақпаратты өңдеуге қызметкердің, мердігредің немесе үшінші тарап өкілінің жауапкершілігі;

e) ұйымның дербес ақпаратты өңдеуге жауапкершілігі, соның ішінде, ұйымда жұмыс істеу нәтижесінде немесе барысында алынған дербес ақпарат (7.2.3 қараңыз).

Ұйым қызметкерлер, мердігерлер мен үшінші тарап өкілдерінің ақпараттық қауіпсіздікке қатысты болатын және ақпараттық жүйелер мен қызметтерге байланысты ұйым активтеріне қолжетімділік типі мен көлеміне сәйкес келетін шарттармен келіскендігін қамтамасыз етуі тиіс.

Қажеттілігіне орай, жұмысбастылық шарттары бойынша қызметкерге жүктелетін жауапкершілік ұйымдағы қызметі аяқталғаннан кейін де белгілі уақыт ішінде сақталуы тиіс (7.3 қараңыз).

Қосымша ақпарат

Қызметкерлердің, мердігерлердің немесе үшінші тарап өкілдерінің құпиялылыққа, ақпаратты қорғауға, этика ережелеріне, ұйымның жабдықтары мен құралдарын тиісті пайдалануға, сондай-ақ, қызмет ету тәртібіне қатысты міндеттері туралы ақпаратты таратуға арналған тәртіп кодексі қолданылуы мүмкін. Мердігер немесе үшінші тарап өкілдері шеттегі ұйымға байланысты болуы мүмкін, осы ұйыммен шартқа қол қойған тұлға атынан келісімшарт жасау талап етілуі мүмкін.

7.2 Жұмысқа орналасқан кезде

Мақсаты: Қызметкерлердің, мердігерлердің және үшінші тарап өкілдерінің ақпараттық қауіпсіздікке байланысты қауіптер мен мәселелер туралы, олардың жауапкершілігі мен міндеттері туралы хабардар болуын, сондай-ақ, адам факторының қаупін төмендететін ұйымның қаупсіздік саясатын сүйемелдеу үшін барлық қажетті құралдармен жабдықталуын қамтамасыз ету.

7.2.1 Басшылық міндеттері

Басқару шаралары

Ұйым басшылығы қызметкерлердің, мердігерлердің және үшінші тарап өкілдерінің ұйымның белгіленген саясаты мен процедураларына сәйкес қауіпсіздікті қамтамасыз етуін талап етуі тиіс.

Іске асыру жөніндегі нұсқау

Басшылық қызметкерлердің, мердігерлердің және үшінші тарап өкілдерінің:

a) оларға осал ақпаратқа немесе ақпараттық жүйелерге қолжетімділік берілгенге дейін өздерінің ақпараттық қауіпсіздік саласындағы қызметтері мен міндеттері туралы хабардар болуын;

b) ұйым шеңберінде қауіпсіздікке қатысты олардың болжалды қызметтерін қалыптастыру бойынша ұсыныстармен қамтамасыз етілуін;

c) ұйымның қауіпсіздік саясатын сақтауға мүдделі болуын;

d) олардың ұйымдағы қызметтері мен міндеттеріне сәйкес келетін қауіпсіздікке қатысты хабардарлық деңгейіне жетуін;

e) ұйымның ақпараттық қауіпсіздік саясаты мен тиісті жұмыс әдістерін қамтитын жұмысбастылық шарттарын сақтауын;

f) тиісті дағдылар мен біліктілікті сүйемелдеуді жалғастыруын;

g) ақпараттық қауіпсіздік саясатын немесе процедураларын бұзу туралы хабарландыруларды қабылдайтын жасырын қызметпен жабдықталуын қамтамасыз етуі тиіс.

Басшылық ақпараттық қауіпсіздік саясатын, оның процедуралары мен басқару шараларын сүйемелдеуін көрсетуі тиіс.

Қосымша ақпарат

Егер қызметкерлер, мердігерлер мен үшінші тарап өкілдері өздерінің қауіпсіздікке қатысты міндеттері туралы мәлімет алмаса, олар ұйымға елеулі нұқсан келтіре алады. Мүдделі персонал сенімдірек болып, ақпараттық қауіпсіздікке қатысты аз оқиғаларға ұшырайтыны ықтимал.

Тиімсіз менеджмент персоналдың өзін жете бағаланбағанын сезінуінің себебі болуы мүмкін, бұл келешекте ұйым үшін жағымсыз салдарларға әкеле алады. Мысалы, тиімсіз менеджмент қауіпсіздікті елемеуге немесе ұйым активтерін қолданысына сай емес пайдалануға әкелуі мүмкін.

7.2.2 Ақпараттық қауіпсіздік саласындағы хабардарлық, оқыту және тренинг

Бақылау және басқару шаралары мен құралдары

Барлық ұйым қызметкерлері, сонымен қатар, қажет болған жерде, мердігерлер мен үшінші тарап өкілдері тиісті оқытудан өтіп, ұйымда қабылданған және олардың жұмыс функцияларына қажетті саясат пен процедуралардың жаңартылған нұсқаларын жүйелі түрде алып тұрулары тиіс.

Іске асыру бойынша ұсыныс

Хабардарлықты қамтамасыз ететін оқытуды ақпарат немесе қызметтерге қолжетімділік берілгенге дейін қауіпсіздік саласындағы саясат пен болжалдармен таныстыруға арналған ресми кіріспе процесінен бастаған жөн.

Ақпараттық қауіпсіздік бағдарламасы қорғалуға тиіс ұйым ақпараты мен ақпаратты қорғау үшін іске асырылған үкімдерді есепке ала отырып, ұйымның ақпараттық қауіпсіздік саясаты мен тиісті процедураларына сәйкес белгіленуі тиіс. Ақпараттық бағдарлама науқандар (мысалы, «ақпараттық қауіпсіздік күні») және буклеттерді басып шығару немесе жаңалық жіберілімі сияқты ақпараттық-ағартушылық шараларды қамтуы тиіс.

Ақпараттық бағдарлама қызметкерлердің ұйымдағы рөлі мен ұйымның мердігерлерден қандай дәрежеде хабардарлығын күтетінін есепке алып жоспарлануы тиіс. Хабардарлықты арттыру бағдарламасының шеңберіндегі қызмет белгілі уақыт ішінде жоспарлануы тиіс. Осылайша, қызмет қайталанады және жұмысқа жаңа қызметкерлер мен мердігерлерді алуға мүмкіндік береді. Ақпараттандыру бағдарламасы, сондай-ақ, ұйым саясаты мен процедураларына сәйкес болып, жүйелі түрде жаңартылуы тиіс. Ол ақпараттық қауіпсіздік инциденттерінен алынған қорытындыларға сүйенуі тиіс.

Хабардарлыққа оқыту ұйымның ақпараттық қауіпсіздік бағдарламасының талаптарына сәйкес орындалуы тиіс. Хабардарлыққа оқыту түрлі оқыту құралдарын, соның ішінде, сынып негізіндегі оқыту, қашықтықтан оқыту, веб-интерфейс, өз бетінше және басқа оқыту түрлерін пайдалана алады.

Ақпараттық қауіпсіздікке оқыту келесі жалпы аспектілерді қамтуы тиіс:

a) ұйымның ақпараттық қауіпсіздік алдындағы міндеттерін белгілеу;

b) саясатта, стандарттарда, заңдарда, қағидаттарда, келісімшарттарда және келісімдерде белгіленген ақпараттық қауіпсіздік ережелері мен міндеттермен бірге қолданылатын қауіпсіздік ережелерімен танысу және оларды сақтау қажет;

c) өздерінің әрекеттері мен әрекетсіздігі үшін жүктелетін жеке жауапкершілік және ұйым мен үшінші тараптардың ақпаратын қорғауды қамтамасыз етуге қатысты жалпы міндеттер;

d) ақпараттық қауіпсіздік (мысалы, ақпараттық қауіпсіздік инциденттері туралы мәлімдемелер) пен базалық басқару элементтерінің (мысалы, қауіпсіздік құпиясөзі, зарарлы басқару элементтері мен таза жұмыс үстелдері) негізгі процедуралары;

е) ақпараттық қауіпсіздік мәселелері бойынша, соның ішінде, ақпараттық қауіпсіздікке қосымша оқыту және оқу материалдары бойынша қосымша ақпарат пен кеңестер алуға арналған байланыс пунктері мен ресурстары.

Ақпараттық қауіпсіздікке оқыту жүйелі түрде жүргізілуі тиіс. Бастапқы оқыту тек жаңа қызметкерлерге ғана емес, сондай-ақ, ақпараттық қауіпсіздікті қамтамасыз етудің түрлі талаптары қойылатын жаңа орындар немесе қызметке ауысатын қызметкерлерге де қатысты болады. Оқыту еңбек қызметі басталғанға дейін өткізілуі тиіс.

Ұйым оқыту мен дайындықты тиімді өткізу үшін білім беру және оқыту бағдарламаларын әзірлеуі тиіс. Бағдарлама қорғалуға тиіс ұйым ақпараты мен ақпаратты қорғау үшін қажетті басқаруды есепке ала отырып, ұйымның ақпараттық қауіпсіздік саясаты мен тиісті процедураларына сәйкес болуы тиіс. Бағдарлама білім мен кәсіби дайындықтың түрлі формаларын қарастыруы тиіс. Мысалы, дәрістер немесе өз бетімен жүргізілетін зерттеулер.

Қосымша ақпарат

Ақпараттандыру бағдарламасын әзірлеген кезде, тек «не» және «қалай» сұрақтарына ғана жауап бермей, «не үшін» деген сұраққа да жауап іздеу қажет. Қызметкерлердің ақпараттық қауіпсіздік мақсаттары мен өз тәртібінің болжалды оң және теріс әсерлерін түсінуі маңызды.

Хабардарлық, білім беру және оқыту басқа оқу шараларының бөлігі бола алады немесе олармен бірге өткізіле алады. Мысалы, жалпы IT оқыту немесе жалпы қауіпсіздікке оқыту. Хабардарлық, білім беру және кадрларды дайындау лауазымдар, міндеттер мен дағдылар үшін жарамды және өзекті болулары тиіс.

Білімді тексеру үшін жұмыскерлердің түсінігін бағалау оқыту және дайындық соңында жүргізіле алады.

7.2.3 Тәртіптік процесс

Бақылау және басқару шаралары мен құралдары

Қауіпсіздікті бұзған қызметкерлерге қатысты қолданылатын ресми тәртіптік процесс болуы тиіс.

Іске асыру жөніндегі ұсыныс

Қауіпсіздік бұзылғандығы туралы алдын ала растауды алғанға дейін тәртіптік процесті бастамаған жөн (16.1.7 қараңыз).

Ресми тәртіптік процесс қауіпсіздікті бұзуда күдікті қызметкерлердің істерін дұрыс және әділ қарастырғандығын қамтамасыз етуге арналған. Бұзушылықтың типі мен ауырлығы, оның бизнеске жағымсыз әсері, бұзушылықтың алғаш рет немесе қайта жасалғандығы, бұзушының тиісті дайындықтан өткендігі, тиісті заңнама, бизнес саласындағы шарттар мен, қажеттілігіне қарай, басқа факторларды есепке алатын сараланған жауап қайтару үшін ресми тәртіптік процесті қамтамасыз еткен жөн.

Қызметкерлерге ұйымның саясаты мен процедураларын бұзуға немесе ақпараттық қауіпсіздікке зиян келтіруге бөгет жасау үшін тәртіптік процесс тежеушілік құрал ретінде қолданылуы тиіс. Қасақана жасалған бұзышулық дереу жауап қайтаруды талап ете алады.

Қосымша ақпарат

Тәртіптік процесті, сондай-ақ, қызметкерлерң, мердігерлер және үшінші тарап өкілдері ұйымда қабылданған саясат пен қауіпсіздік процедураларын бұзудан және қандай да болмасын басқа қауіпсіздік бұзушылықтарын жасаудан алдын алатын тежеушілік құралы ретінде пайдаланған жөн.

7.3 Жұмысбастылықты тоқтату немесе ауыстыру

Мақсаты: Жұмысқа орналастыру шарттарын өзгерту немесе тоқтату бойынша процесс бөлігі ретінде ұйым мүдделерін қорғау.

7.3.1 Міндеттерді тоқтату

Бақылау және басқару шаралары мен құралдары

Жұмысбастылықты тоқтату немесе ауыстыруға қатысты міндеттер анық анықталуы және белгіленуі тиіс.

Іске асыру жөніндегі ұсыныстар

Міндеттерді тоқтату туралы мәлімдеу өзекті қауіпсіздік талаптары мен құқықтық жауапкершілікті, қажеттілігіне қарай, құпиялылық туралы келісімдегі міндеттерді (13.2.4 қараңыз), сондай-ақ, қызметкерлердің, мердігерлердің немесе үшінші тарап өкілдерінің қызметін тоқтатқаннан кейін белгілі уақыт аралығында әрекетін жалғастыратын жұмысбастылық шарттарын (7.1.2 қараңыз) қамтуы тиіс.

Жұмысбастылықты аяқтағаннан кейін жарамды болып қалатын жауапкершілік пен қызметтік міндеттер қызметкерлермен, мердігерлермен немесе үшінші тарап өкілдерімен жасалатын келісімшарттарда қамтылуы тиіс (7.1.2 қараңыз).

Міндеттер мен жұмысбастылықты өзгерту тиісті міндеттер мен жұмысбастылықты тоқтату және жаңа міндеттер немесе жұмысбастылықты бастау ретінде басқарылуы тиіс.

Қрсымша ақпарат

Әдетте, кадр бөлімі жұмысбастылықты тоқтатудың жалпы процесіне жауапты болып, маңызды процедуралардың қауіпсіздік аспектілерін басқаруды қамтамасыз ету үшін жұмыстан босатылатын тұлғаның басшысымен бірге әрекет етеді. Мердігерге қатысты бұл процесті мердігерге жауапты агенттік, ал үшінші тарап өкілдеріне қатысты оның ұйымы жүзеге асырады.

Қызметкерлерге, клиенттерге, мердігерлерге немесе үшінші тарап өкілдеріне кадрлық құрамдағы өзгерістер мен қолданылатын келіскендіктер туралы хабарлау қажет.

8 Активтерді басқару

8.1 Активтер үшін жауапкершілік

Мақсаты: Ұйым активтері мен оларды қорғау бойынша тиісті міндеттерді белгілеу.

8.1.1 Активтерді есепке алу

Басқару шаралары

Ақпарат пен ақпаратты өңдейтін құралдарға байланысты активтер белгіленуі тиіс. Осы активтердің тізілімі құрылып, оның тәртібі сақталуы тиіс.

Іске асыру жөніндегі ұсыныстар

Ұйым ақпарат циклдерінің тиісті кезеңдерінде активтерді белгілеп, олардың маңызын құжаттауы тиіс. Ақпараттың өміршең циклі құруды, өңдеуді, сақтауды, жіберуді, жоюды және бұзуды қамтуы тиіс. Құжаттау арнаулы немесе бар есепке алу құжаттарында жүргізілуі тиіс.

Активтерді есепке алу дәл, өзекті және басқа есептерге сәйкес болуы тиіс. Әр анықталған актив үшін активтерге арналған меншік құқығы тағайындалуы тиіс (8.1.2 қараңыз) және жіктеу белгіленуі тиіс (8.2 қараңыз).

Қосымша ақпарат

Активтерді есепке алу тиімді қорғаныстың жүзеге асырылуына кепіл бере алады. Немесе активтерді есепке алу денсаулық сақтау және қауіпсіздік, сақтандыру және қаржы (активтерді басқару) себептері сияқты басқа мақсаттар үшін талап етілуі мүмкін.

[11] сілтемеде ұйым активтерді анықтаған кезде қарастыруға тиіс активтер мысалдары берілген. Активтер тізілімін құру процесі қауіптерді басқарудың маңызды алғышарты болып табылады (сондай-ақ, ISO/IEC 27000 және [11] қараңыз).

8.1.2 Активтердің меншік құқығы

Басқару шаралары

Есепте сақталатын активтердің иесі болуы тиіс.

Іске асыру жөніндегі ұсыныстар

Активтердің өміршең циклін басқаруға жауапкершілік жүктелген жеке тұлғалар, сондай-ақ, басқа тұлғалар активтердің иесі ретінде тағайындалуы тиіс.

Әдетте, активтерді иеленуге уақтылы тағайындаулы қамтамасыз ету процесі іске асырылады. Меншік құқығы, активтер құрылған кезде немесе активтер ұйымға көшірілген кезде, тағайындалуы тиіс. Активтердің иесі активтердің барлық өміршең циклі барысында активтерді тиісті басқаруға жауапты болады.

Активтер иесі:

a) активтер есебін қамтамасыз етуі;

b) активтердің тиісінше жіктелуі мен қорғалуын қамтамасыз етуі;

c) қолжетімділікті шектеу саясатын есепке алып, маңызды активтерге қолжетімділікті шектеу және олардың жіктелуін анықтауы және жүйелі түрде қайта қарауы;

d) актив жойылған кезде, тиісті қарауды қамтамасыз етуі тиіс.

Қосымша ақпарат

Белгілі иеленуші барлық өміршең цикл барысында активтерді басқаруға жауапкершілікті бекітетін жеке немесе заңды тұлға бола алады. Белгілі иеленушінің активке арналған меншік құқықтарының болуы міндетті емес.

Қарапайым міндеттер, мысалы, активтерді күнделікті негізде сақтайтын сақтаушыға жүктеле алады, бірақ жауапкершілік иеленушіге жүктеледі.

Күрделі ақпараттық жүйелерде белгілі қызметті қамтамасыз ету үшін бірлесіп әрекет ететін активтер тобын белгілеу пайдалы бола алады. Бұл жағдайда, осы сервис иесі қызмет көрсетуге, соның ішінде, өз активтерінің жұмысына жауапты болады.

8.1.3 Активтерді рұқсат етілген пайдалану

Басқару шаралары

Ақпаратты және ақпарат пен ақпаратты өңдеу құралдарына байланысты активтерді рұқсат етілетін пайдалану ережелері белгіленуі, құжатталуы және іске асырылуы тиіс.

Іске асыру жөніндегі ұсыныстар

Ұйым активтерін қолданатын немесе оларға қолжетімділігі бар қызметкерлер мен сыртқы тұтынушылар ақпарат пен ақпаратты өңдеу құралдарына және ресурстарға байланысты ұйым активтерінің ақпараттық қауіпсіздік талаптары туралы ақпарат алулары тиіс. Олар ақпарат өңдеудің кез келген ресурстарын пайдалануға жауапты болып, кез келген осындай пайдалану олардың жауапкершілігінде болады.

8.1.4 Активтерді қайтару

Бақылау және басқару шаралары мен құралдары

Барлық қызметкерлер, мердігерлер мен үшінші тарап өкілдері, олардың жұмысбастылығы, шарты немесе келісімі аяқталған кезде, олардың қолданысындағы барлық активтерді ұйымға қайтаруға міндетті.

Іске асыру жөніндегі ұсыныстар

Жұмысбастылықты тоқтату процесі бұрын берілген барлық бағдарламалық жасақтаманы, корпоративтік құжаттарды және жабдықтарды қайтаруды қамтитындай ресімделуі тиіс.

Қызметкер, мердігер немесе үшінші тарап өкілі ұйым жабдығын сатып алған немесе өзінің жеке жабдығын пайдаланған жағдайда, барлық маңызды ақпарат ұйымға беріліп,

жабдықтардан қауіпсіз тәсілмен жойылғанын қамтамасыз ететін процедураларды сақтау қажет (11.2.7 қараңыз).

Қызметкер, мердігер немесе үшінші тарап өкілінде жалғастырылатын жұмыстар үшін маңызды білімі болған жағдайда, осындай ақпаратты құжат түрінде ресімдеп, ұйымға беру қажет.

Шартты бұзған кезде, ұйым жұмыстан босатылған қызметкерлердің және мердігерлердің өзекті ақпаратты (мысалы, зияткерлік меншікті) рұқсатсыз көшіруін бақылауы тиіс.

8.2 Ақпаратты жіктеу

Мақсаты: Ақпараттың ұйым үшін маңыздылығына сәйкес тиісті қорғаныс деңгейін алуын қамтамасыз ету.

8.2.1 Ақпаратты жіктеу

Басқару шаралары

Ақпарат құқықтық тұрғыдан, құндылық тұрғысынан, қауіптілік тұрғысынан және рұқсатсыз ашылуға немесе осындай ақпаратты түрлендіруге сезімділігіне қатысты жіктелуі тиіс.

Іске асыру жөніндегі ұсыныстар

Жіктеу және және оған байланысты ақпаратқа арналған қорғайтын басқару элементтері ақпаратты бірлесіп пайдалану немесе ақпаратқа қолжетімділікті шектеуге арналған бизнес талаптарын, сондай-ақ, заң талаптарын есепке алуы тиіс. Ақпараттан басқа активтер де сақтауға, өңделуге немесе активпен қорғалуға тиісті ақпарат жіктелуіне сәйкес жіктеле алады.

Ақпараттық активтер иелері оларды жіктеу үшін есеп беруші болулары тиіс.

Жіктеу схемасы жіктеу келісімдері мен уақыт ішінде жіктеуді қарастыруға арналған критерийлерді қамтуы тиіс. Схемадағы қорғаныс деңгейі құпиялылықты, бүтіндікті және қолжетімділікті талдау арқылы бағалануы тиіс. Схема қолжетімділікті басқару саясатымен үйлесуі тиіс (9.1.1 қараңыз).

Әр деңгейдің өз атауы болады, бұл схема жіктеуі пайдалану тұрғысынан маңызды.

Схема әр қызметкер ақпарат пен оған байланысты активтерді бірдей жіктейтіндей, қорғаныс талаптары туралы жалпы түсінік алатындай және тиісті қорғанысты қолданатындай барлық ұйымға сәйкес келуі тиіс.

Жіктеу ұйым процестерінде қамтылып, барлық ұйым шеңберінде дәйекті және үйлесуі тиіс. Жіктеу нәтижелері активтердің ұйым үшін қауіптілігі мен сезімділігіне тәуелді активтер бағасын белгілеуі тиіс. Мысалы, құпиялылық, бүтіндік және қолжетімділік тұрғысынан. Жіктеу нәтижелері олардың бағасы, сезімділігі мен өміршең циклінің қауіптілігі өзгергеніне сәйкес жаңартылуы тиіс.

Қосымша ақпарат

Жіктеу ақпаратпен айналысатын адамдарға оны қалай пайдалану және қорғау қажеттігін белгілейді. Ұқсас қорғаныс қажеттіліктері бар ақпарат тобын құру және әр топтағы барлық ақпаратқа қолданылатын ақпараттық қауіпсіздік процедураларын белгілеу осыған көмектеседі. Осы тәсіл қауіптерді бағалау және басқару элементтерінің жеке дизайн қажеттілігін төмендетеді.

Ақпарат белгілі уақыт аралығы өткеннен кейін сезгіштік немесе қауіптілік қасиеттерін жоя алады, мысалы, ақпарат жария етілген жағдайда. Осы аспектілер есепке алынуы тиіс, өйткені, қайта жіктеу қосымша шығын себебі болып, қажет емес басқару шараларын іске асыруға әкеле алады. Немесе жеткіліксіз жіктеу іскерлік мақсаттарға жетуге бөгет бола алады.

Құпиялылық туралы ақпаратты жіктеу схемасының мысалы төрт деңгейде келесідей негізделе алады:

a) ақпаратты ашу зиян келтірмейді;

b) ақпаратты ашу кішігірім қиыншылықтар немесе кішігірім оперативтік қолайсыздықтар тудырады;

c) ақпаратты ашу қызметке немесе тактикалық мақсаттарға қысқа мерзімді елеулі әсерін тигізеді;

d) ақпаратты ашу ұзақ мерзімді стратегиялық мақсаттарға елеулі әсерін тигізеді немесе ұйымның сақталуына қауіп төндіреді.

8.2.2 Ақпаратқа таңбашаларды бекіту

Басқару шаралары

Ақпараттық маркалаудың тиісті процедуралар жинағы ұйымда қабылданған ақпараттық жіктеу жүйесіне сәйкес дамытылып, жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқау

Ақпараттық маркалау процедуралары ақпарат пен оған байланысты нақты және электрондық пішімдердегі активтерге қатысты болуы тиіс. Маркалау 8.2.1 белгіленген жіктеу жүйесін көрсетуі тиіс. Таңбашалар оңай айырып танылатын болулары тиіс. Процедуралар таңбашалардың қайда және қалай бекітілгенін, ақпаратқа қалай қолжетімділікті алу қажеттігін немесе активтердің қалай өңделетінін белгілейді. Процедуралар таңбаша жоқ жағдайларды анықтай алады. Мысалы, жұмыс жүктемесінің төмендеуін белгілейтін құпия емес ақпаратты маркалау. Қызметкерлер мен мердігерлер процедураларды маркалау туралы хабардар болулары тиіс.

Сезгіш немесе маңызды ретінде жіктелген ақпаратты қамтитын жүйелерден өзгеше өнімінде тиісті жіктеу маркалауы болуы тиіс.

Басқа ақпарат

Құпия деректерді маркалау – ақпаратты бірлесіп пайдалану шаралары үшін ең басты талап. Нақты таңбашалар мен метадеректер – маркалаудың стандартты пішімі.

Ақпарат пен оған байланысты активтерді маркалаудың кейде теріс әсерлері болады. Қолжетімділігі бар тұлғалар немесе сыртқы хакерлер үшін жіктелген активтерді анықтау және сәйкесінше оларды ұрлап алу оңайырақ болады.

8.2.3 Активтерді өңдеу

Басқару шаралары

Активтерді өңдеу тәсілдері ұйымда қабылданған ақпараттық жіктеу жүйесіне сәйкес әзірленіп, жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқау

Процедуралар жіктелуімен үйлесетін ақпаратты өңдеу, сақтау және хабарлау үшін әзірленуі тиіс (8.2.1 қараңыз).

Келесі тармақтарды қарастырған жөн:

a) жіктеудің әр деңгейі үшін қорғаныс талаптарын сүйемелдейтін қолжетімділікті шектеу;

b) активтерді өкілетті алушыларына ресми есеп бойынша қызмет көрсету;

c) түпнұсқалық ақпаратты қорғаумен үйлесетін деңгейде ақпараттың уақытша немесе тұрақты көшірмелерін қорғау;

d) IT активтерін дайындаушылардың техникалық талаптарына сәйкес сақтау;

e) өкілетті алушышарды мәлімдеу үшін барлық деректер көшірмелерін анық маркалау.

Ұйымда қолданылатын жіктеу жүйесі, деңгей атаулары бірдей болған жағдайда да, басқа ұйымдарда қолданылатын схемаларға тең бола алмайды; сондай-ақ, ұйымдар арасында жіберілетін ақпарат, жіктеу жүйелері бірдей болған жағдайда да, әр ұйымда оның мәнмәтініне тәуелді жіктеу бойынша өзгере алады.

Басқа ұйымдармен жасалатын ақпаратты бірлесіп пайдалануды қамтитын келісімдер осы ақпарат жіктелуін анықтауға және басқа ұйымдардан алынған жіктеу таңбашаларын түсіндіруге арналған процедураларды қамтуы тиіс.

8.3 Деректерді өңдеу

Мақсаты: БАҚ-да сақталған ақпаратты рұқсатсыз ашуды, түрлендіруді немесе жоюды болдыртпау.

8.3.1 Алмалы-салмалы деректер тасымалдаушыларын басқару

Басқару шаралары

Процедуралар ұйымда қабылданған жіктеу жүйелеріне сәйкес алмалы-салмалы тасымалдаушыларын басқару үшін жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқаулар

Алмалы-салмалы тасымалдаушыларды басқаруға арналған келесі ұсыныстарды қарастыру қажет:

a) ұйымнан өшірілуге тиісті, қайта қолданылатын кез келген деректердің мазмұны, келешекте қажет болмаған жағдайда, қалпына келтірілмейтін етіп жасалуы тиіс;

b) қажеттілігіне орай, ұйымда өшірілген деректер үшін рұқсат алу қажет және бақылау журналын жүргізу үшін осындай өшірулер есебін жүргізу қажет;

c) барлық деректер дайындаушылардың техникалық талаптарына сәйкес ортада сақталуы тиіс;

d) егер деректердің құпиялылығы немесе бүтіндігі маңызды болса, алмалы-салмалы тасымалдаушылардағы деректерді қорғау үшін шифрлау әдістерді қолдану қажет;

e) сақталған деректер қажет болған жағдайда, деректерді зақымдау қаупін төмендету үшін деректер оқылмайтын болғанға дейін жаңа тасымалдаушыға көшірілуі тиіс;

f) деректердің ұқсас зақымдалу немесе жоғалу қаупін төмендету үшін маңызды деректердің көптеген көшірмелері бөлек тасымалдаушыларда сақталуы тиіс;

g) алмалы-салмалы тасымалдаушыларды тіркеу деректерді жоғалту мүмкіндігін шектейді;

h) оларды қолдану үшін себеп болған жағдайда, алмалы-салмалы тасымалдаушыларға рұқсат берілуі тиіс;

i) алмалы-салмалы тасымалдаушыларды пайдалану қажеттілігі болған кезде, ақпаратты көшіру немесе жіберу процесі бақылануы тиіс.

Рұқсат ету процедуралары мен деңгейлері тіркелуі тиіс.

8.3.2 Деректердің орналасуы

Басқару шаралары

Деректерді ресми процедураларды пайдаланып, сенімді түрде орналастыру қажет.

Іске асыру жөніндегі нұсқаулар

Құпия ақпараттың басқа адамдарға жайылу қаупін азайту үшін деректерді қауіпсіз орналастырудың ресми тәртіптері белгіленуі тиіс. Құпиялы ақпаратты қамтитын деректерді қауіпсіз орналастыру процедуралары осы ақпараттың сезімділігіне пропорционал болуы тиіс.

Келесі тармақтарды қарастыру қажет:

a) құпия ақпаратты қамтитын деректер сенімді түрде сақталуы және орналасуы тиіс. Мысалы, пайдалану деректерін жою ұйымдағы құрылғы арқылы жүргізілуі тиіс;

b) қауіпсіз басқаруды талап ете алатын тармақтарды анықтау үшін процедуралар болуы тиіс;

c) маңызды тармақтарды бөліп көрсетудің орнына барлық деректер тармақтары жинап, сенімді түрде орналастыру үшін шараларды қолданған жөн;

d) көптеген ұйымдар деректерді жинау және орналастыруды ұсынады; тиісті бақылау мен тәжірибесі бар үшінші тарапты мұқият таңдау қажет;

e) бақылау журналын жүргізу үшін маңызды тармақтарды орналастыру тіркелуі тиіс.

Орналастыруға арналған деректерді жинаған кезде, құпия ақпараттың зор көлемін маңызды қылатын жинақталу әсеріне көңіл аудару қажет.

Басқа ақпарат

Осал деректерді қамтитын зақымданған құрылғылар, қауіп дәрежесін бағалау жөндеуге жіберу немесе бас тартудан бөлек оларды нақты түрде жою қажеттілігін анықтауын талап ете алады (11.2.7 қараңыз).

8.3.3 Деректерді нақты түрде жіберу

Басқару шаралары

Ақпаратты қамтитын деректер тасымалдау барысында рұқсат етілмеген қолжетімділіктен, дұрыс емес қолданудан немесе жемқорлықтан қорғалуы тиіс.

Іске асыру жөніндегі нұсқаулар

Келесі ұсыныстар жіберілетін ақпаратты қамтитын деректерді қорғауға көмектеседі:

a) сенімді көлік немесе курьер қолданылуы тиіс;

b) өкілетті курьерлер тізіміне басқармамен келісу қажет;

c) курьерлерді сәйкестендіруді тексеруге арналған тәсілдер әзірленуі тиіс;

d) орауыш ішіндегісін тасымал барысында кез келген нақты зақымданудан қорғау үшін жеткілікті болып, кез келген дайындаушылардың техникалық талаптарына сәйкес келуі тиіс. Мысалы, жоғары температура, ылғалдылық немесе электрмагнитті өрістер әсерлері сияқты деректерді қалпына келтіру тиімділігін азайта алатын қоршаған ортаның кез келген факторларынан қорғаныс;

e) тіркеу деректер мазмұнын анықтап, сақталуы тиіс, қорғаныс қолданылып, тасымал сақтаушыларына беру уақыты мен тағайындалу жерінде алу уақыты жазып алынуы тиіс.

Басқа ақпарат

Ақпарат нақты тасымал кезінде рұқсат етілмеген қолжетімділік, дұрыс емес пайдалану үшін осал бола алады немесе зақымдала алады. Мысалы, пошта қызметі немесе курьер арқылы жіберу. Бұл жағдайда деректер баспа құжаттарды қамтиды.

Деректер туралы құпия ақпарат шифрланбаған кезде, деректерді қосымша нақты түрде қорғауды қарастыру қажет.

9 Қолжетімділікті басқару

9.1 Қолжетімділікті басқаруға қойылатын іскерлік талаптар

Мақсаты: ақпаратты өңдеу құралдары мен ақпаратқа қолжетімділікті шектеу.

9.1.1 Қолжетімділікті басқару саясаты

Басқару шаралары

Қолжетімділікті басқару саясаты ақпараттық қауіпсіздік жұмысы мен талаптарына негізделіп, белгіленуі, тіркелуі және қарастырылуы тиіс.

Іске асыру жөніндегі нұсқаулар

Активтердің иеленушілері байланысты ақпараттық қауіптерді көрсететін нақтылаулар мен қатаңдықпен қолжетімділікті басқарудың тиісті қағидаттарын, қолжетімділік құқықтарын және белгілі тұтынушылар үшін олардың активтеріне шектеуді белгілеуі тиіс.

Қолжетімділікті басқару құралдары (қисындық және нақты) (11-тарауды қараңыз) бірге қарастырылуы тиіс.

Тұтынушылар мен қызметтерді жеткізушілерге қолжетімділікті басқару құралдарына сәйкес келетін іскерлік талаптарды анық мәлімдеу қажет.

Саясат келесілерді есепке алуы тиіс:

a) бизнес-қосымшалардың қауіпсіздік талаптары;

b) ақпараттың таралу саясаты. Мысалы, «білуге тиіс» принципі және ақпараттық қауіпсіздік деңгейлері мен ақпаратты жіктеу (8.2 қараңыз);

c) қолжетімділік құқықтары және жүйелер мен желілерді жіктеудің ақпараттық саясаты арасындағы жүйелілік;

d) деректер немесе қызметтерге қолжетімділікті шектеуге қатысты тиісті заңнама мен кез келген шарттық міндеттемелер (18.1 қараңыз);

e) қолжетімді байланыстардың барлық типтерін мойындайтын таратылған және желілік қоршаған ортада қолжетімділік құқықтарын басқару;

f) қолжетімділікті басқару рөлдерін бөлектеу. Мысалы, қолжетімділікке сұрау салу, қолжетімділікке рұқсат беру, қолжетімділікті басқару;

g) қолжетімділікке сұрау салуларға ресми рұқсат беруге арналған талаптар (9.2.1 және 9.2.2 қараңыз);

h) қолжетімділік құқықтарына кезеңдік шолу талаптары (9.2.5 қараңыз);

i) қолжетімділік құқықтарын жою (9.2.6 қараңыз);

j) тұтынушылардың сәйкестендіру туралы құпия ақпаратты пайдалануы және басқаруына қатысты барлық маңызды оқиғалар есептерін мұрағаттау;

k) артықшылықты қолжетімділігі бар рөлдер (9.2.3 қараңыз).

Басқа ақпарат

Қолжетімділікті басқару қағидаттарын белгілеген кезде мұқият болған жөн:

a) «Егер айқын тыйым салу болмаса, барлығына рұқсат етілген» емес, «Егер айқын рұқсат болмаса, барлығына тыйым салынады» алғышартына негізделген қағидатты белгілеу;

b) ақпаратты өңдеу құралдары автоматты түрде бастаған, сондай-ақ, тұтынушының қарауына байланысты басталған ақпаратты маркалаудағы (8.2.2 қараңыз) өзгерістер;

c) ақпараттық жүйе автоматтық түрде бастаған, сондай-ақ, әкімшінің қарауына байланысты басталған тұтынушы рұқсаттарындағы өзгерістер;

d) қаулы шығару алдында белгілі мақұлдауды талап ететін және талап етпейтін қағидаттар.

Қолжетімділікті басқару қағидаттары ресми процедуралар (9.2, 9.3, 9.4 қараңыз) және белгілі міндеттермен (6.1.1, 9.3 қараңыз) сүйемелденуі тиіс.

Қолжетімділікті басқаруға негізделген рөл қолжетімділік құқықтарын іскерлік рөлдермен байланыстыру үшін көптеген ұйымдарда қолданылатын тәсіл болып табылады.

Қолжетімділікті басқару саясатын бағыттайтын екі жиі қолданылатын принциптер:

a) «Арнаулы ақпаратқа қолжетімділік қажеттілігі» принципі өз мақсаттарын орындау үшін тек сіз үшін ғана ақпаратқа қолжетімділік ұсынады (түрлі мақсаттар/рөлдер түрлі қажеттілікті, яғни, түрлі қолжетімділік профильдерін білдіреді);

b) «Пайдалану қажеттілігі» принципі: тек сізге ғана ақпаратты өңдеу құралдарына (IT жабдықтары, арыздар, процедуралар, бөлмелер) қолжетімділік ұсынылады.

9.1.2 Желілер мен желі қызметтеріне қолжетімділік

Басқару шаралары

Тұтынушыларға пайдалануға арналған желілер мен желі қызметтеріне қолжетімділікті ұсыну қажет.

Іске асыру жөніндегі нұсқаулар

Саясат желілер мен желі қызметтерін пайдалануға қатысты белгіленуі тиіс. Осы саясат келесіні қамтуы тиіс:

a) қолжетімділік берілетін желілер мен желі қызметтері;

b) желілер мен желі қызметтеріне қолжетімділік кімге рұқсат етілетінін анықтау үшін авторизация процедуралары;

c) желілер мен желі қызметтеріне қолжетімділікті қорғау үшін әкімшілік басқару және процедуралар;

d) қолжетімділік желілері мен желі қызметтеріне бекітілген құралдар (мысалы, VPN немесе сымсыз желіні пайдалану);

e) түрлі желі қызметтеріне қолжетімділікке арналған тұтынушылық сәйкестендіру талаптары;

f) желі қызметтері пайдалануды бақылау.

Желі қызметтерін пайдалануға қатысты саясат ұйымның қолжетімділікті басқару саясатымен (9.1.1 қараңыз) үйлесуі тиіс.

Басқа ақпарат

Желі қызметтерімен рұқсатсыз және қауіпті байланыс бүкіл ұйымға жағымсыз әсерін тигізе алады. Осы басқару шарасы сезгіш немесе қауіпті бизнес-қосымшалары бар желілер үшін немесе қауіпті жерлерде орналасқан тұтынушылар үшін аса маңызды. Мысалы, қоғамдық жерлер немесе ұйымның қауіпсіздікті ақпараттық басқару және бақылауынан тыс орналасқан жерлер.

9.2 Тұтынушының қолжетімділікті басқаруы

Мақсаты: тіркелген тұтынушының қолжетімділігіне кепіл беру және жүйелер мен қызметтерге рұқсатсыз қолжетімділікті болдыртпау.

9.2.1 Тұтынушыны тіркеу және ұйымды жою

Басқару шаралары

Қолжетімділік құқықтарын белгілеуге рұқсат ету үшін ресми тұтынушыны тіркеу және тіркеуді жою процесі жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқау

Тұтынушылардың сәйкестендіргіштерін басқару процесі келесілерді қамтуы тиіс:

a) тұтынушылардың әрекеттермен байланысы мен оларға жауапкершілігін анықтау үшін тұтынушылардың бірегей сәйкестендіргіштерін пайдалану; тұтынушының жалпы сәйкестендіргіштерін пайдалануға тек бизнес үшін қажетті болған кезде немесе жұмыс жағдайларына байланысты рұқсат етілуі тиіс. Осы қолданыс мақұлданып, тіркелуі тиіс;

b) ұйымнан шығып кеткен тұтынушылардың сәйкестендіргіштерін дереу сөндіру немесе өшіру (9.2.6 қараңыз);

c) тұтынушылардың резервтік сәйкестендіргіштерін кезеңдік түрде анықтау және өшіру немесе сөндіру;

d) тұтынушылардың резервтік сәйкестендіргіштерінің басқа тұтынушыларға байланбағанына кепіл беру.

Басқа ақпарат

Ақпарат немесе ақпаратты өңдеу құралдарына қолжетімділікті қамтамасыз ету немесе оның күшін жою әдетте екі сатылы процедура түрінде жүзеге асыралады:

a) тұтынушы сәйкестендіргішін тағайындау және оған мүмкіндік ұсыну немесе оның күшін жою;

b) осындай тұтынушы сәйкестендіргішіне қолжетімділік құқықтарын қамтамасыз ету немесе олардың күшін жою (9.2.2 қараңыз).

9.2.2 Тұтынушылық қамтамасыз етуші қолжетімділік

Басқару шаралары

Барлық жүйелер мен қызметтерге барлық тұтынушылық типтер үшін қолжетімділік құқықтарын тағайындау немесе олардың күшін жою үшін қолжетімділікті қамтамасыз ететін ресми тұтынушылық процесс жүзеге асырылады.

Іске асыру жөніндегі нұсқау

Тұтынушы сәйкестендіргіштеріне берілген қолжетімділік құқықтарын тағайындау немесе олардың күшін жою үшін қамтамасыз етуші процесс келесілерді қамтуы тиіс:

a) ақпараттық жүйе немесе қызмет иесінен ақпараттық жүйені немесе қызметті пайдалануға рұқсат алу (8.1.2 басқару шарасын қараңыз); басшылықтан қолжетімділік құқықтарын алу үшін бөлек мақұлдау талап етілуі мүмкін;

b) берілген қолжетімділік деңгейі қолжетімділік саясатына (9.1 қараңыз) сәйкес келетінін және міндеттерді бөлу (6.1.2 қараңыз) сияқты басқа талаптармен үйлесетінін растау;

c) қолжетімділік процедурасын аяқтау алдында қолжетімділік құқықтарының активтендірілмеуін (мысалы, қызмет жеткізушілері арқылы) қамтамасыз ету;

d) ақпараттық жүйелер мен қызметтерге қолжетімділік алу үшін берілген тұтынушы сәйкестендіргішінің қолжетімділік құқықтары бойынша орталықтандырылған есепті сүйемелдеу;

e) өздерінің қызметтерін немесе жұмыс орындарын өзгерткен тұтынушылардың қолжетімділік құқықтарын үйлестіру немесе ұйымнан шығып кеткен тұтынушылардың қолжетімділік құқықтарын бұғаттау;

f) ақпараттық жүйелер немесе қызметтер иелерімен қолжетімділік құқықтарды кезеңдік түрде тексеру (9.2.5 қараңыз).

Басқа ақпарат

Типтің тұтынушылық қолжетімділік профильдерінде көптеген қолжетімділік құқықтарын қамтитын іскерлік талаптарға негізделген тұтынушылық қолжетімділік рөлдеріне көңіл аударған жөн. Қолжетімділікке сұрау салу және тексеру (9.2.4 қараңыз) ерекше құқықтар деңгейіне қарағанда, осындай рөлдер деңгейінде оңайырақ іске асырылады.

Қызметкерлердің келісімшарттарында және қызмет көрсету жөніндегі келісімшарттарда персоналдың немесе мердігерлердің рұқсатсыз қолжетімділік талпыныстары жағдайындағы айыппұл санкцияларын белгілейтін тармақтардың енгізілуіне көңіл аударған жөн (7.1.2, 7.2.3, 13.2.4, 15.1.2 қараңыз).

9.2.3 Артықшылықты қолжетімділік құқықтарын басқару

Басқару шаралары

Артықшылықты қолжетімділік құқықтарын бөлу және пайдалану шектеулі және басқарылатын болуы тиіс.

Іске асыру жөніндегі нұсқау

Артықшылықты қолжетімділік құқықтарын бөлу тиісті қолжетімділікті басқару саясатына сәйкес ресми рұқсат беру процесі арқылы басқарылуы тиіс (9.1.1 қараңыз). Келесі қадамдарды қарастырған жөн:

a) әр жүйе немесе процеске, мысалы, операциялық жүйе, деректер базасы, басқару жүйесіне байланысты артықшылықты қолжетімділік құқықтары, сондай-ақ, әр қолданыс пен бөліп таратылуға тиісті тұтынушылар белгіленуі тиіс;

b) артықшылықты қолжетімділік құқықтары тұтынушыларға қолданыс қажеттілігінің негізінде және қолжетімділікті басқару саясатына (9.1.1 қараңыз) сәйкес «әрекетке әрекет ету» негізінде, яғни, олардың функционалды рөлдеріне қойылатын минимал талап негізінде тағайындалуы тиіс;

c) барлық тағайындалған артықшылықтарға рұқсат беру процестері мен оларды жазып алу туралы есеп жүргізілуі тиіс. Артықшылықты қолжетімділік құқықтарын қолжетімділікке рұқсат беру процесі орындалмағанша беруге тыйым салынады;

d) артықшылықты қолжетімділік құқықтары аяқтауына арналған талаптар белгіленуі тиіс;

e) артықшылықты қолжетімділік құқықтары тұрақты іскерлік қызметке арналған артықшылықтардан өзгеше тұтынушы сәйкестендіргішіне тағайындалады. ID арқылы кірген кезде жүйелі іскерлік қызмет орындалмауы тиіс;

f) тұтынушылардың білімі олардың міндеттеріне сәйкес келетінін тексеру үшін оларды артықшылықты қолжетімділік құқықтарымен бірге жүйелі түрде тексерілуі тиіс;

g) жүйелер конфигурацияларының мүмкіндіктеріне сәйкес әкімшінің бірегей сәйкестендіргіштерін рұқсатсыз пайдалануды болдыртау үшін нақты тәртіп белгіленіп, сақталуы тиіс;

h) әкімшінің бірегей сәйкестендіргіштері үшін сәйкестендіру туралы құпия ақпараттың құпиялылығы оны бөлген кезде сақталуы тиіс (мысалы, артықшылықты тұтынушы жұмыстан шығып кеткен кезде немесе жұмысты өзгерткен кезде, өз құпиясөздерін тиісті механизмдері бар артықшылықты тұтынушыларға айтып, құпиясөздерді жиі және мүмкіндікке орай тез өзгерту).

Басқа ақпарат

Жүйелік әкімшіліктің артықшылықтарын тиісті емес пайдалану (тұтынушыға жүйені немесе басқару құралдарын елемеуге мүмкіндік беретін ақпараттық жүйенің кез келген ерекшелігі немесе құралы) жүйе сәтсіздіктеріне немесе бұзылуына әкелетін басты фактор болып табылады.

9.2.4 Тұтынушыларды сәйкестендіру туралы құпия ақпаратты басқару

Басқару шаралары

Сәйкестендіру туралы құпия ақпаратты бөлуді ресми басқарушылық процесс арқылы басқару қажет.

Іске асыру жөніндегі нұсқау

Процесс келесі талаптарды қамтуы тиіс:

a) жеке құпия ақпаратты сақтау үшін және сәйкестендіру туралы құпия ақпаратты тек топ мүшелері арасында сақтау үшін тұтынушылар арызға қол қоюға тиісті; осы қол қойылған арыз жұмысбастылық қағидаттары мен шарттарына енгізіле алады (7.1.2 қараңыз);

b) тұтынушылар сәйкестендіру туралы өзінің жеке құпия ақпаратын сүймелдеуге міндетті болған кезде, олар бірінші пайдаланудан кейін өзгертуге тиісті сәйкестендіру туралы қауіпсіз уақытша құпия ақпаратпен қамтамасыз етілуге тиіс;

c) жаңа, ауыстырылған немесе уақытша сәйкестендіру туралы құпия ақпаратпен қамтамасыз еткенге дейін тұтынушының жеке басын тексеру үшін тәртіп белгіленуі тиіс;

d) сәйкестендіру туралы уақытша құпия ақпарат тұтынушыларға қауіпсіз тәсілмен берілуі тиіс; үшінші тарап қызметтерін немесе электрондық пошта арқылы қорғалмаған (ашық мәтін) хабарламаны қолданбаған жөн;

e) сәйкестендіру туралы уақытша құпия ақпарат адам үшін бірегей және сенімді болуы тиіс;

f) тұтынушылар сәйкестендіру туралы құпия ақпаратты алғандығын растаулары тиіс;

g) сатушыны сәйкестендіру туралы ақпарат жүйелер немесе бағдарламалық жасақтаманы қондырғаннан кейін әдепкі қалпы бойынша өзгертілуі тиіс.

Басқа ақпарат

Құпиясөз сәйкестендіру туралы құпия ақпараттың дәстүрлі қолданылатын типі болып табылады және тұтынушы жеке басын растаудың жалпы құралы болып табылады. Сәйкестендіру туралы құпия ақпараттың басқа типтері – криптографиялық кілттер мен сәйкестендіру кодтарын өндіретін, тасымалдаушыларда сақталатын (мысалы, микропроцессорлық карточка) басқа деректер.

9.2.5 Тұтынушылық қолжетімділік құқықтарына шолу

Басқару шаралары

Активтердің иелері тұтынушылардың қолжетімділік құқықтарын біркелкі қарастырулары тиіс.

Іске асыру жөніндегі нұсқау

Қолжетімділік құқықтарын тексеру келесілерді ескеру қажет:

a) тұтынушылардың қолжетімділік құқықтары жұмыс бабында жоғарылау, төмендеу немесе жұмысбастылықты аяқтау сияқты кез келген өзгертулерден кейін де біркелкі қарастырылуы тиіс (7-тарауды қараңыз);

b) тұтынушылық қолжетімділік құқықтары осы ұйымдағы бір рөлден басқа рөлге көшіп, қарастырылуы және қайта бөлінуі тиіс;

c) артықшылықты қолжетімділік құқықтарына рұқсат беру жиірек аралықта қарастырылуы тиіс;

d) рұқсатсыз артықшылықтар алынбағанына кепіл беру үшін артықшылықтарды бөлу тексерілуі тиіс;

e) артықшылықты шоттардың өзгерісі кезеңдік тексеріс үшін тіркелуі тиіс.

Басқа ақпарат

Осы басқару шарасы 9.2.1, 9.2.2 және 9.2.6 басқару шараларын іске асырған кездегі ықтимал осал жерлерді өтейді.

9.2.6 Қолжетімділік құқықтарын жою немесе реттеу

Басқару шаралары

Барлық қызметкерлер мен үшінші тарап тұтынушыларына арналған ақпарат пен ақпаратты өңдеу құралдарына қолжетімділік құқықтары олардың еңбек шарты, келісімшарты немесе келісімі аяқталған кезде жойылуы тиіс немесе тиісінше өзгертілуі тиіс.

Іске асыру жөніндегі нұсқау

Ақпарат пен ақпаратты өңдеу құралдарына және ақпаратты өңдеу қызметтеріне байланысты активтерге қолжетімділік құқықтарының мерзімі өткен кезде, осы қолжетімділік құқықтары жойылуы немесе уақытша тоқтатылуы тиіс. Бұл қолжетімділік құқықтарын өшіру қажеттілігін көрсетеді. Еңбек шартын өзгерту жаңа еңбек шарты үшін мақұлданбаған барлық қолжетімділік құқықтарын жойған кезде көрсетілуі тиіс. Жойылуға немесе өзгертілуге тиісті қолжетімділік құқықтары нақты және логикалық қолжетімділікті қамтиды. Қолжетімділік құқықтарын жою немесе өзгерту криптографиялық кілттерді, жеке куәліктерді, ақпаратты өңдеу құралдарын немесе қолжетімділік құқықтарына жазылымды жою, оның күшін жою немесе оларды ауыстыру арқылы жүзеге асырыла алады. Қызметкерлер мен мердігерлердің қолжетімділік құқықтарын белгілейтін кез келген құжаттама қолжетімділік құқықтарын жою немесе өзгертуді көрсетуі тиіс. Егер іссапарға кететін немесе қызметтен босатылатын қызметкер тұтынушылық белсенді құпиясөзді білсе, құпиясөз жұмысбастылықты, келісімшартты немесе келісімді аяқтағаннан немесе ауыстырғаннан кейін өзгертілуі тиіс.

Ақпарат пен ақпаратты өңдеу құралдарына байланысты активтерді алуға арналған қолжетімділік құқықтары келесідей қауіп факторларын бағалауға тәуелді еңбек шарты өзгергенге немесе аяқталғанға дейін азайтылуы немесе жойылуы тиіс:

a) еңбек шартын аяқтау немесе өзгертуді қызметкер, үшінші тарап тұтынушысы немесе басқарманың бастауы және еңбек шартын бұзу себептері;

b) қызметкердің, үшінші тарап тұтынушысының немесе кез келген басқа тұтынушының ағымдағы міндеттері;

c) қазіргі уақыттағы қолжетімді активтердің құндылығы.

Басқа ақпарат

Белгілі жағдайларда қолжетімділік құқықтары қолжетімділіктің жұмыстан шығып кеткен қызметкер немесе үшінші тарап тұтынушысынан артық адам санына қажеттілігінің

негізінде бөліне алады. Осындай жағдайларда жұмыстан шығатын қызметкерлер қолжетімділік топтарының кез келген тізімдерінен жойылуы тиіс. Барлық басқа қызметкерлер мен үшінші тарап тұтынушыларына осы ақпаратты жұмыстан шығып кеткен қызметкермен бөліспейтінін ескерту қажет.

Еңбек шартын басшылық бастамасымен бұзған жағдайда, ренжіген қызметкерлер немесе үшінші тарап тұтынушылары әдейі ақпаратты бұза алады немесе ақпаратты өңдеу құралдарына зақым келтіре алады. Отставка немесе жұмыстан босатқан жағдайда, осындай қызметкерлер келешек қолданыс үшін ақпарат жинауы мүмкін.

9.3 Тұтынушы міндеттері

Мақсаты: тұтынушыларға олардың сәйкестендіру туралы ақпаратын қорғау үшін жауапкершілікті жүктеу.

9.3.1 Сәйкестендіру туралы құпия ақпаратты пайдалану

Басқару шаралары

Тұтынушылар сәйкестендіру туралы құпия ақпаратты пайдаланған кезде ұйым әдістерін сақтауға міндетті.

Іске асыру жөніндегі нұсқау

Барлық тұтынушылар:

a) сәйкестендіру туралы құпия ақпаратты өкіметті қоса алғандағы ешқандай да басқа тараптарға жариялануына кепіл беріп сақтағаны;

b) егер бұл сенімді түрде сақтала алмаса, ал сақтау әдісі мақұлданса (мысалы, құпиясөзді сақтау орны), сәйкестендіру туралы құпия ақпарат есебін жүргізуді болдыртпау (мысалы, қағаз нұсқада, бағдарламалық жасақтама файлында немесе тасымалды құрылғыда);

c) сәйкестендіру туралы құпия ақпаратты ықтимал бұзу белгісі болған әр уақытта оны өзгерткені;

d) құпиясөздер сәйкестендіру туралы құпия ақпарат ретінде қолданылған кезде, жеткілікті минимал ұзындықты сапалы құпиясөздерді таңдағаны:

1) есте сақтауға оңай;

2) аңғаруға немесе адам туралы тиісті ақпаратты қолданып алуға оңай мәліметтерге негізделмеген. Мысалы, есімдер, телефон нөмірлері, туған күндер және т.б.;

3) сөздік шабуылға төзімді (яғни, сөздіктерде қамтылған сөздерден тұрмайды);

4) жүйелі ұқсас барлық сандық немесе барлық әріптік символдардан еркін;

5) егер уақытша болса, жүйеге алғаш рет кірген кезде өзгертілген құпиясөз;

e) бөлек тұтынушының сәйкестендіру туралы құпия ақпаратын таратпау;

f) құпиясөздер жүйеге автоматтандырылған кіру процедураларында сәйкестендіру туралы құпия ақпарат петінде қолданған кезде және сақталған кезде, құпиясөздердің тиісті қорғанысын қамтамасыз еткені;

g) бизнес пен іскерлік емес мақсаттар үшін сәйкестендіру туралы бірдей құпия ақпаратты қолданбағаны жөн.

Басқа ақпарат

Single Sign On (SSO – желіде бірыңғай тіркеу) немесе сәйкестендіру туралы ақпаратты басқарудың басқа құпия аспаптарын ұсыну тұтынушылардың қорғауға тиісті сәйкестендіру туралы құпия ақпараттың көлемін азайтады, осылайша, осы басқару шарасының тиімділігін арттырады. Алайда, осы аспаптар, сондай-ақ, сәйкестендіру туралы құпия ақпараттың жариялануының әсерін арттыра алады.

9.4 Жүйе және қолжетімділікті қолданбалы басқару

Мақсаты: жүйелер мен арыздарға рұқсатсыз қолжетімділікті болдыртпау.

9.4.1 Қолжетімділікті ақпараттық шектеу

Басқару шаралары

Ақпараттық және қолданбалы жүйе функцияларына қолжетімділік қолжетімділікті басқару саясатына сәйкес шектелуі тиіс.

Іске асыру жөніндегі нұсқау

Қолжетімділікті шектеу бизнес-қосымшаның бөлек талаптарына және қолжетімділікті басқарудың белгілі саясатына сәйкес негізделуі тиіс.

Қолжетімділікті шектеу талаптарын сүйемелдеу үшін келесілерді қарастыру қажет:

a) қолданбалы жүйенің функцияларына қолжетімділікті басқару үшін мәзір ұсыну;

b) ерекше тұтынушының қандай деректерге қолжетімділікті ала алатынын басқару;

c) тұтынушылардың қолжетімділік құқықтарын басқару, мысалы, оқу, жазу, өшіру және орындау;

d) басқа қосымшалардың қолжетімділік құқықтарын басқару;

e) ақпаратты шектеу өнімде қамтылады;

f) осал арыздар, қосымша немесе жүйе деректерін оқшаулау үшін қолжетімділікті басқарудың нақты немесе логикалық құралдарын қамтамасыз ету.

9.4.2 Жүйеге кірудің қауіпсіз процедуралары

Басқару шаралары

Қажеттілігіне орай, қолжетімділікті басқару саясатын, жүйелер мен арыздарға қолжетімділікті жүйеге кірудің қауіпсіз процедурасы басқаруы тиіс.

Іске асыру жөніндегі нұсқау

Тұтынушының талап етілетін тұлғасын растау үшін тиісті сәйкестендіру әдісі таңдалады.

Сәйкестендіру және сәйкестікті қатаң тексеру талап етілетін жерде, шифрлау құралдары, смарт-карталар, символдар немесе биометриялық құралдари сияқты сәйкестендіру әдістерінің құпиясөзге баламасы қолданылуы тиіс.

Рұқсатсыз қолжетімділік мүмкіндігін азайту үшін жүйеге тіркелу немесе қолдану процедурасы әзірленуі тиіс. Жүйеге кіру процедурасы авторизацияланбаған тұтынушыға кез келген қажет емес көмек көрсетуді болдыртпау үшін жүйе немесе қолданыс туралы минимум ақпаратты ашуы тиіс. Жүйеге кірудің тиімді процедурасы:

a) жүйеге кіру процесі сәтті аяқталғанға дейін жүйе немесе қолданбалы сәйкестендіргіштерді көрсетпеуге;

b) компьютерге тек тіркелген тұтынушылардың қолжетімділік алуын ескертетін жалпы мәлімдемені көрсетуге;

c) жүйеге кіру процедурасы барысында авторизацияланбаған тұтынушыға көмектесе алатын көмек мәлімдемелерін бермеуге;

d) жүйеге кіру туралы ақпаратты барлық кіру деректерін аяқтағаннан кейін ғана растау. Егер қате пайда болса, жүйе деректердің қай бөлігі дұрыс емес екендігін көрсетпеуге тиіс;

e) дөрекі күштің жүйеге кіру әрекеттерінен қорғауға;

f) сәтсіз және сәтті әрекеттерді тіркеуге;

g) егер жүйеге кіруді басқару құралдары ықтимал түрде бұзылса, қорғаныс процестерін бастауға;

h) жүйеге сәтті кіру процедурасының аяқталуы туралы келесі ақпаратты көрсетуге:

1) жүйеге соңғы сәтті кірудің күні мен уақыты;

2) жүйеге соңғы сәтті кіруден бастап, жүйге кез келген сәтсіз кіру әрекетінің егжей-тегжейлері;

i) енгізілген құпиясөзді көрсетпеуге;

j) құпиясөздерді желі бойынша ашық мәтінмен жібермеуге;

k) белгілі әрекетсіздік кезеңінен кейін, әсіресе, ұйымның қауіпсіздік басқаруынан тыс қоғамдық аймақтар сияқты аса қауіпті жерлерде немесе мобильді құрылғыларда жұмыс істемейтін сессияларды аяқтауға;

l) қауіпті қосымшалар үшін қосымша қауіпсіздікті қамтамасыз ету және рұқсатсыз қолжетімділік мүмкіндігін азайту үшін қосылу уақытын шектеуге тиіс.

Басқа ақпарат

Құпиясөздер тек тұтынушы ғана білетін құпияға негізделген сәйкестендіру және сәйкестікті қамтамасыз ететін кеңінен таралған тәсіл болып табылады. Осыған шифрлау құралдары мен аутентификация хаттамалары арқылы жетуге болады. Тұтынушылық сәйкестендіру қуаты қолжетімділік алынатын ақпаратты жіктеу үшін жарамды болуы тиіс.

Егер құпиясөздер желі бойынша жүйеге кіру сессиясы барысында ашық мәтінмен жіберілсе, оларды желілік бағдарлама іліп алуы мүмкін.

9.4.3 Құпиясөзді басқару жүйесі

Басқару шаралары

Құпиясөзді басқару жүйелері интерактивті болып, сапалы құпиясөздермен қамтамасыз етуі тиіс.

Іске асыру жөніндегі нұсқау

Құпиясөзді басқару жүйесі:

a) есептілікті сүйемелдеу үшін тұтынушылардың бөлек сәйкестендіргіштері мен құпиясөздерін пайдалануға;

b) тұтынушыларға өзінің жеке құпиясөздерін таңдау және өзгерту мүмкіндігін беруге және кіру қателеріне жол беру үшін растау процедурасын қосуға;

c) сапалы құпиясөздерді таңдауға;

d) тұтынушылар жүйеге алғаш рет кірген кезде өзінің құпиясөздерін өзгертуге мәжбүрлеуге;

e) құпиясөзді жүйелі түрде, сондай-ақ, қажеттілігіне орай өзгертуді іске асыруға;

f) бұрын қолданылған құпиясөздер есебін жүргізуге және қайта пайдалануды болдыртпауға;

g) енгізілген құпиясөздердің экранда көрсетпеуге;

h) құпиясөздері бар файлдарды қолданбалы жүйе туралы деректерден бөлек сақтауға;

i) құпиясөздерді қорғалған формада сақтауға және жіберуге тиіс.

Басқа ақпарат

Кейбір арыздар тұтынушылық құпиясөздердің тәуелсіз тараппен тағайындалуын талап етеді; осы жағдайда жоғарыда берілген нұсқаудың b), d) және e) тармақтары қолданылмайды. Көптеген жағдайларда құпиясөздерді тұтынушы таңдайды және сақтайды.

9.4.4 Артықшылықты утилиталарды пайдалану

Басқару шаралары

Жүйелер мен қосымшаларды басқару құралдарын айналып өте алатын бағдарлама-утилиталарды пайдалану шектеулі және қатал түрде бақыланатын болуы тиіс.

Іске асыру жөніндегі нұсқау

Жүйелер мен қосымшаларды басқару құралдарын айналып өте алатын утилиталарды пайдалану үшін келесі ұсыныстарды қарастыру қажет:

a) сәйкестендіру, аутентификация және утилиталарға рұқсат беру процедураларын пайдалану;

b) утилиталарды қолданбалы бағдарламалық жасақтамадан бөлу;

c) утилатиларды пайдалануды сенімді, рұқсат етілген тұтынушылар минимал санына дейін шектеу (9.2.3 қараңыз);

d) утилиталарды арнайы пайдалануға рұқсат беру;

e) утилиталардың қолжетімділігін шектеу, мысалы, санкцияланған өзгерту барысында;

f) бағдарлама-утилиталарды пайдаланудың барлық түрлерін тіркеу;

g) утилиталар үшін рұқсат беру деңгейлерін белгілеу және құжаттау;

h) барлық қажет емес утилиталарды жою немесе қолданыстан шығару;

i) міндеттерді бөлу талап етілетін жүйелердегі қосымшаларға қолжетімділігі бар тұтынушылар үшін утилиталарға қолжетімділік бермеу.

Басқа ақпарат

Көптеген компьютерлік қондырғыларда жүйені немесе қосымшаларды басқару құралдарын айналып өте алатын бір немесе одан артық утилиталар бар.

9.4.5 Бастапқы кодты бағдарламалауға арналған қолжетімділікті басқару

Басқару шаралары

Бағдарламаның бастапқы кодына қолжетімділік шектеулі болуы тиіс.

Іске асыру жөніндегі нұсқау

Рұқсат етілмеген функционалдықты енгізуді және байқаусыз өзгертулерді болдыртпау үшін, сондай-ақ, құнды зияткерлік меншік құпиялылығын сақтау үшін бағдарламаның бастапқы коды мен оған байланысты тармақтарға (жобалар, техникалық талаптар, тексеріс жоспарлары сияқты) қолжетімділікті қатал түрде басқару қажет. Бағдарламаның бастапқы коды үшін осыған басқарылатын орталық сақтау арқылы қол жеткізуге болады, мысалы, бағдарламаның бастапқы библиотекаларында. Келесі ұсыныстар компьютерлік бағдарламаларға зиян келтіруді төмендету үшін осындай бағдарлаамалардың бастапқы библиотекаларына қолжетімділікті басқаруға арналған:

a) мүмкіндігіне орай, бағдарламалардың бастапқы библиотекалары пайдаланатын жүйелерде жүргізілмеуге тиіс;

b) бағдарламаның бастапқы коды мен бағдарламалардың бастапқы библиоткеларын белгіленген тәртіпке сәйкес басқару қажет;

c) қосалқы персоналда бастапқы библиотекаларды бағдарламауға шексіз қолжетімділігі болмауға тиіс;

d) бағдарламашы бағдарламалардың бастапқы библиотекаларын және тиісті тармақтарды жаңартуды және бастапқы бағдарламарды құруды тек тиісті рұқсат алғаннан кейін ғана орындауға тиіс;

e) бағдарламалар тізімдері қауіпсіз қоршаған ортада жүргізілуге тиіс;

f) бақылау журналы бағдарламалардың бастапқы библиотекаларына барлық кіру сессияларын сақтауға тиіс;

g) бағдарламалардың бастапқы библиотекаларына қызмет көрсету және оларды көшіру өзгерістерді бақылаудың қатал процедураларына ұшырауға тиіс (14.2.2 қараңыз).

Егер бағдарламаның бастапқы коды жариялануға тиіс болса, бүтіндікті қамтамасыз ету үшін қосымша басқару құралдарын қарастырған жөн (мысалы, электрондық қол).

10 Криптография

10.1 Басқарудың шифрлау құралдары

Мақсаты: ақпараттың құпиялылығын, түпнұсқалығын және/немесе бүтіндігін қорғау үшін криптографияны тиісті және тиімді түрде пайдалануға кепіл беру.

10.1.1 Басқарудың шифрлау құралдарын пайдалануға қатысты саясат

Басқару шаралары

Ақпаратты қорғау үшін басқарудың шифрлау құралдарын пайдалануға қатысты саясат дамытылып, енгізілуі тиіс.

Іске асыру жөніндегі нұсқау

Шифрлау саясатын дамытып, келесіні қарастыру қажет:

a) бизнес-ақпаратты қорғауға тиісті жалпы принциптерді қоса алғандағы барлық ұйым бойынша басқарудың шифрлау құралдарын пайдалануға арналған басқарушылық тәсіл;

b) талап етілетін шифрлау алгоритмнің типін, қуаты мен сапасын есепке ала отырып, қауіп дәрежесін бағалауға негізделген қажетті қорғаныс деңгейі белгіленуі тиіс;

c) мобильді немесе алмалы-салмалы тасымалдаушы құрылғыларымен тасымалданатын немесе коммуникациялық желілер арқылы өтетін ақпаратты қорғау үшін шифрлауды пайдалану;

d) шифр кілттерін қорғауға және кілттер жоғалған, оларға қауіп төнген немесе олар бұзылған жағдайда шифрланған ақпаратты қалпына келтіруге қатысты әдістерді қоса алғандағы кілт менеджментіне арналған тәсіл;

e) рөлдер мен міндеттер, мысалы:

1) саясатты енгізуге;

2) кілт буынын қоса алғандағы кілт менеджментіне жауапты адам (10.1.2 қараңыз);

f) барлық ұйым бойынша тиімді жүзеге асыру үшін қабылданатын стандарттар (бизнес-процесс үшін қандай шешім қолданылады);

g) мазмұнды бақылауға негізделетін басқару құралдары туралы шифрланған ақпаратты пайдалану әсері (мысалы, зиянды анықтау).

Ұйымның шифрлау саясатын өткізі отырып, әлемнің түрлі бөліктерінде шифрлау әдістерін пайдалануға және шифрланған ақпарат трансбордерінің ағым мәселелеріне (18.1.5 қараңыз) қатысты бола алатын нұсқаулықтар мен ұлттық шектеулерге көңіл аудару қажет.

Басқарудың шифрлау құралдары түрлі ақпараттық қауіпсіздік мақсаттарына қол жеткізу үшін қолданылуы мүмкін, мысалы:

a) құпиялылық: сақталған немесе жіберілген сезгіш немесе маңызды ақпаратты қорғау үшін ақпаратты шифрлауды пайдалану;

b) бүтіндік/түпнұсқалық: сақталған немесе жіберілген сезгіш немесе маңызды ақпараттың түпнұсқалығын немесе бүтіндігін тексеру үшін сандық қолдарды немесе аутентификация кодтарын пайдалану;

c) міндеттерден бас тартпау: оқиға немесе әрекеттің пайда болу немесе пайда болмау айғақтарын ұсыну үшін шифрлау әдістерін пайдалану;

d) сәйкестендіру: жүйелік тұтынушыларға, кәсіпорындарға және ресурстарға қолжетімділікке сұрау салатын немесе белгіленген тұлғалар мен ұйымдармен істер жүргізетін тұтынушылар мен басқа жүйелік кәсіпорындардың шынайылығын растау үшін шифрлау әдістерін пайдалану.

Басқа ақпарат

Шифрлау шешімі жарамдылығына қатысты шешім қабылдау қауіп дәрежесін бағалау және басқару құралдарын таңдаудың кеңірек процесс бөлігі болуы тиіс. Осы бағалау басқарудың шифрлау құралының жарамдылығын, қандай бақылау және қандай мақсаттар мен іскерлік процестер үшін қолданылатынын анықтау үшін қолданыла алады.

Шифрлау әдістерін пайдалану артықшылықтарын арттыру және қауіптерін азайту үшін және сәйкес емес немесе дұрыс емес қолданысты болдыртпау үшін басқарудың шифрлау құралдарын пайдалануға қатысты саясат қажет.

Қауіпсіздік саясатының ақпараттық мақсаттарына қол жеткізу үшін маман басқарудың тиісті шифрлау құралдарын пайдалануы тиіс.

10.1.2 Кілт менеджмент

Басқару шаралары

Криптографиялық кілттерді пайдалануға қатысты саясат барлық пайдалану кезеңі барысында дамытылып, енгізілуі тиіс.

Іске асыру жөніндегі нұсқау

Саясат шифр кілттерін басқаруға қойылатын талаптарды қамтуы тиіс, алайда, оларды пайдалану кезеңі кілттерді құру, сақтау, мұрағаттау, қалпына келтіру, бөлу, өшіру және жоюды қамтиды.

Шифрлау алгоритмдері, кілт ұзындығы мен пайдалану әдістері ең сәтті тәжірибеге сәйкес іріктелуі тиіс. Кілттерді тиісті басқару шифр кілттерін құру, сақтау, мұрағаттау, қалпына келтіру, бөлу, өшіру және жоюдың қауіпті процестерін талап етеді.

Барлық шифр кілттері түрлендіру мен жоғалудан қорғалуы тиіс. Сонымен қатар, құпия және жеке кілттерді рұқсат етілмеген қолданыстан, сондай-ақ, ашудан қорғалуы тиіс. Кілттерді өндіру, сақтау және мұрағаттау үшін қолданылатын жабдық нақты түрде қорғалуы тиіс.

Кілттерді басқару жүйесі келесілерге арналған стандарттар, процедуралар мен қауіпсіз әдістердің келісілген жинағына негізделуі тиіс:

a) түрлі шифрлау жүйелері мен түрлі қосымшаларға арналған кілттерді жасау;

b) ашық кілт сертификаттарын өндіру және алу;

c) кілттер алынғаннан кейін қалай активтендірілуге тиіс екендігін қоса алғандағы осы кәсіпорынға арналған кілттерді бөлу;

d) тіркелген тұтынушылар кілттерге қолжетімділікті қалай алатынын қоса алғандағы кілттерді сақтау;

e) кілттер қашан өзгертілуге тиіс және қалай өзгертілетіні туралы ережелерді қоса алғандағы кілттерді өзгерту немесе жаңарту;

f) қауіп төнген кілттермен жұмыс істеу;

g) кілттер қалай қайтарылып алынатынын немесе дезактивацияланатынын қоса алғандағы кілттердің күшін жою, мысалы, кілттерге қауіп төнген жағдайда немесе тұтынушы ұйымнан шығып кеткен кезде (кілттер мұрағатталуға тиіс болған жағдайда);

h) жоғалған немесе бұзылған кілттерді қалпына келтіру;

i) кілттерді сақтау немесе мұрағаттау;

j) кілттерді бұзу;

k) кілттерді басқаруға байланысты әрекеттерді тіркеу және тексеру.

Дұрыс емес қолданыс ықтималдығын төмендету үшін кілттер тек кілттерді басқару жөніндегі тиісті саясатта белгіленген уақыт аралығында ғана қолданылатындай, кілттерді активациялау және дезактивациялау күндері белгіленуі тиіс.

Сенімді басқарылатын құпия және жеке кілттерге қосымша түрде, сондай-ақ, ашық кілттердің түпнұсқалығын қарастыру қажет. Қажетті сенімділік деңгейін қамтамасыз ету үшін тиісті басқару құралдары мен процедуралары бар әйгілі ұйым болуға тиісті сертификаттау органы шығаратын ашық кілт куәліктерін пайдаланып, осы сәйкестендіру процесі орындала алады.

Сыртқы шифрлау қызметтерін жеткізушілерімен, мысалы, сертификаттау органымен сервистік қызмет көрсету туралы келісімдер немесе келісімшарттар мазмұны жауапкершілік, қызмет сенімділігі мен қызмет көрсетуге кеткен уақыт мәселелерін қамтуы тиіс (15.2 қараңыз).

Басқа ақпарат

Шифр кілттерін басқару шифрлау әдістерін тиімді пайдалану үшін маңызды.

[2], [3], [4] кілттерді басқару туралы қосымша ақпарат берілген.

Шифрлау әдістері шифр кілттерін қорғау үшін де қолданыла алады. Процедуралар шифр кілттеріне қолжетімділікке сұрау салу үшін қарастырыла алады, мысалы, шифрланған ақпарат сот процесінде айғақ ретінде талап етіле алады.

11 Нақты және экологиялық қауіпсіздік

11.1 Қауіпсіз аймақ

Мақсаты: ұйымның ақпараты мен ақпаратты өңдеу құралдарына рұқсат етілмеген нақты қолжетімділікті, бұзуды және араласуды болдыртпау.

11.1.1 Нақты қорғаныс периметрі

Басқару шаралары

Қауіпсіздік периметрлері сезгіш немесе маңызды ақпаратты және ақпаратты өңдеу құралдарын қамтитын аумақты қорғау үшін белгіленуі және қолданылуы тиіс.

Іске асыру жөніндегі нұсқау

Нақты қорғаныс периметрлері үшін келесі ұсыныстарды тиісті жағдайларда қарастыру және жүзеге асыру қажет:

a) қауіпсіздік периметрлері белгіленіп, әр периметрдің орналасуы және қуаты периметр шеңберінде қауіпсіздік талаптарына және қауіп дәрежесін бағалау нәтижелеріне тәуелді болуы тиіс;

b) ақпаратты өңдеу құралдары бар ғимарат немесе жер периметрлері нақты адекватты болулары тиіс (яғни, оңай бұзыла алатын периметрде немесе аумақтарда аралықтардың болмауы); жердің сыртқы төбесі, қабырғалары мен едені сенімді түрде құрастырылып, барлық сыртқы есіктер рұқсат етілмеген қолжетімділіктен тиісінше қорғалуы тиіс (мысалы, бөгет құралдары, дабыл, құлыптар); қорғаныста терезелер үшін қарастырған кезде, әсіресе, жер деңгейінде есіктер мен терезелер бекітіліп тұруы тиіс;

c) тиісті қабылдау бөлмесі немесе сайтқа нақты қолжетімділікті немесе ғимаратты басқарудың басқа құралдары болуы тиіс; орынжайлар мен ғимараттарға қолжетімділікті өкілетті персонал шектеуі тиіс;

d) рұқсат етілмеген нақты қолжетімділікті және экологиялық ластануды болдыртпау үшін нақты бөгеттер құрылуы тиіс;

e) қауіпсіздік периметріндегі барлық өрт жағдайында өту орындары қауіпсіздік режимінде болып, жарамды аймақтық, ұлттық және халықаралық стандарттарға сәйкес қажетті қарсыласу деңгейін орнату үшін қабырғалармен бірге тексерілуі тиіс; олар жергілікті өрт қауіпсіздігі нормаларына сәйкес жұмыс жасаулары тиіс;

f) тиісті зиянкестерді анықтау жүйелері ұлттық, аймақтық немесе халықаралық стандарттарға сәйкес орнатылып, барлық сыртқы есіктер мен қолжетімді терезелерді қорғау үшін жүйелі түрде тексерілуі тиіс; бос аймақтар қауіпсіздік режимінде болуы тиіс; қорғаныс басқа аймақтар үшін, мысалы, компьютерлер, бөлмелер немесе түрлі талқылауларға арналған бөлмелер үшін қамтамасыз етілуі тиіс;

g) ұйым басқаратын ақпаратты өңдеу құралдары үшінші тарап басқаратын құралдардан нақты түрде бөлініп тасталуы тиіс.

Басқа ақпарат

Ұйым орынжайы мен ақпаратты өңдеу құралының айналасында бір немесе бірнеше нақты бөгет құру арқылы нақты қорғанысқа қол жеткізуге болады. Дүркін бөгеттерді пайдалану жалғыз бөгеттің сәтсіздігі қауіпсіздікке дереу қауіп төндіретінін білдірмейтін қосымша қорғанысты береді.

Қауіпсіз аймақ бұғатталатын офис немесе нақты қорғаныстың үздіксіз ішкі бөгетімен қоршалған бірнеше бөлме болуы мүмкін. Нақты қолжетімділікті басқару үшін қажетті қосымша бөгеттер мен периметрлер қауіпсіздік периметріндегі түрлі қауіпсіздік

талаптары қойылатын аумақтар арасында қажет бола алады. Көптеген ұйымдардың активтерін ұстайтын ғимараттар жағдайында нақты қауіпсіздікке көңіл бөлінеді.

Нақты басқару құралдарын пайдалану, әсіресе, қауіпсіз аймақтар үшін, қауіп дәрежесін бағалауда белгіленген ұйымның техникалық және экономикалық жағдайына үйлестірілуі тиіс.

11.1.2 Кіруді нақты басқару құралдары

Басқару шаралары

Қауіпсіз аймақтар тек өкілетті персоналға қолжетімділік рұқсат етілетініне кепіл беру үшін тиісті кіруді басқару құралдарымен қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстарды қарастыру қажет:

a) келушілердің келу және кету күні мен уақыты тіркелуі тиіс, егер келушілердің кіруі бұрын мақұлданбаса, олардың барлығы бақылануы тиіс; оларға белгілі, санкцияланған мақсаттарда қолжетімділік ұсынып, саланың қауіпсіздік талаптары мен төтенше шараларға қатысты нұсқаулықтар беріп кіргізу қажет. Келушілердің жеке басы тиісті құрал арқылы расталуы тиіс;

b) құпия ақпарат өңделетін немесе сақталатын аумақтарға қолжетімділік тек тиісті қолжетімділікті басқару құралдарын енгізгеннен кейін ғана өкілетті адамдармен шектеле алады, мысалы, қолжетімділік картасы мен құпия PIN сияқты екі факторлы аутентификация механизмін енгізу;

c) барлық қолжетімділікке арналған нақты есеп журналы немесе электрондық бақылау журналы сенімді түрде күзетілуі және тексерілуі тиіс;

d) барлық қызметкерлер, мердігерлер мен үшінті тараптар белгілі көрінетін сәйкестендіру формасын киюге міндетті және олар жетектеушісіз келушілерді және көрінетін сәйкестендірусіз адамдарды кездестірген жағдайда, қауіпсіздік қызметі персоналына дереу хабарлауға тиіс;

e) аумақты немесе құпия ақпаратты өңдеу құралдарын тек қажеттілігіне орай күзету үшін үшінші тараптың сүйемелдеу қызметі персоналына шектеулі қолжетімділік ұсыну қажет; осы қолжетімділік рұқсат етілген және тексерілген болуы тиіс;

f) қауіпсіз аймақтарға арналған қолжетімділік құқықтары жүйелі түрде қарастырылуы және жаңартылуы және олардың күші жойылуы тиіс (9.2.5 және 9.2.6 қараңыз).

11.1.3 Офистер, бөлмелер мен құралдарды қорғау

Басқару шаралары

Офистерге, бөлмелер мен құралдарға арналған нақты қорғаныс әзірленіп, қолданылуы тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстар офистер, бөлмелер мен құралдардың қорғанысын қамтамасыз етеді:

a) кілттермен жұмыс істеуге арналған құралдар қоғамдық қолжетімділікті болдыртпайтындай орналастырылуы тиіс;

b) ғимараттар қарапайым болып, өзінің құрылыс мақсатын минимал түрде белгілеп, ақпаратты өңдеу әрекеттерін көрсететін ғимарат ішінде немесе сыртында анық белгісіз болуы тиіс;

c) құралдар құпия ақпараттың немесе әрекеттердің сырттан көрінуіне және естілуіне бөгет жасайтындай құрылуы тиіс. Электрмагнит қоршауды да қарастырған жөн;

d) құпия ақпаратты өңдеу құралдарының орналасуын белгілейтін анықтамалықтар мен ішкі телефон кітаптары авторизацияланбаған тұлғалар үшін қолжетімді болмауы тиіс.

11.1.4 Сыртқы және экологиялық қауіптерден қорғау

Басқару шаралары

Табиғи апаттардан, зиянды шабуылдан немесе жазатайым оқиғалардан нақты қорғау әзірленіп, қолданылуы тиіс.

Іске асыру жөніндегі нұсқау

Өрт, су тасқыны, жер сілкінісі, жарылыс, қоғамдық тәртіпсіздік пен табиғи апаттардың және техногендік апаттардың басқа формаларынан бұзылуды болдыртпауға қатысты маман кеңесі алынуы тиіс.

11.1.5 Қауіпсіз аймақтағы жұмыс

Басқару шаралары

Қауіпсіздік аймақта жұмыс істеу процедуралары әзірленіп, қолданылуы тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстарды қарастырған жөн:

a) персонал қажетті деректер негізінде қауіпсіз аймақтың болуы туралы немесе қауіпсіз аймақ шеңберіндегі қызмет туралы білуі тиіс;

b) қауіпсіздікке байланысты қауіпсіз аймақтағы қадағалаусыз жұмысты болдыртпаған және қасақана жасалатын әрекеттер мүмкіндігін болдыртпаған жөн;

c) бос қауіпсіздік аймақтары нақты жабылып, кезеңдік түрде тексерілуі тиіс;

d) егер рұқсат алынбаса, мобильді құрылғылардағы камералар сияқты фотографиялық, видео, аудио немесе басқа жазып алатын жабдықтарды қауіпсіз аймақ аумағына өткізуге тыйым салынады.

Қауіпсіз аймақта жұмыс істеуге арналған шаралар қауіпсіз аймақта жұмыс істейтін қызметкерлер мен үшінші тарап тұтынушыларына арналған басқару құралдарын қамтиды және олар қауіпсіз аймақта жүзеге асырылатын барлық әрекеттерді есепке алады.

11.1.6 Жеткізу және тиеу орны

Басқару шаралары

Рұқсат етілмеген қолжетімділікті болдыртпау үшін бөгде адамдар орынжайға кіре алатын жеткізу және тиеу аймақтары сияқты қолжетімділік жерлерін басқару және ақпаратты өңдеу құралдарынан оқшаулау қажет.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстарды қарастырған жөн:

a) ғимараттан тыс орналасқан жеткізу және тиеу аймағына қолжетімділік белгілі және өкілетті персоналмен шектелуі тиіс;

b) жеткізу және тиеу аймағы жеткізілімдер ғимараттың басқа бөліктеріне қолжетімділік алатын жеткізу персоналынсыз тиеліп, түсірілетіндей әзірленуі тиіс;

c) жеткізу және тиеу аймағының ішкі есіктері ашық болған кезде, сыртқы есіктер жабық болуы тиіс;

d) түсетін материал жеткізу және тиеу аймағынан көшірілгенге дейін жарылғыш заттар, химикаттар немесе басқа қауіпті материалдардың болуына қаралып, тексерілуі тиіс;

e) түсетін материал активтерді басқару процедураларына сәйкес (8-тармақты қараңыз) немесе аумаққа кіреберісте тіркелуі тиіс;

f) түсетін және коммуникативтік жеткізілімдер нақты түрде бөлінуі тиіс;

g) түсетін материал жолда араласу айғақтарының болуына тексерілуі тиіс. Егер осындай араласу анықталса, ол қауіпсіздік қызметі персоналына дереу хабарлануы тиіс.

11.2 Жабдық

Мақсаты: активтердің жоғалуын, бұзылуын, ұрлануын және ұйым әрекеттерін тоқтатуды болдыртпау.

11.2.1 Жабдықтың орналасуы және оны қорғау

Басқару шаралары

Жабдық экологиялық қауіптерді және рұқсат етілмеген қолжетімділік мүмкіндік қауіптерін азайту үшін орналастырылып, қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстар жабдықты қорғауға көмектесе алады:

a) жабдық түрлі жұмыс салаларына қажет емес қолжетімділікті азайтатындай орналастырылады;

b) осал деректерді өңдейтін ақпаратты өңдеу құралдары рұқсат алмаған персоналдың ақпаратты ашу қаупін азайту үшін мұқият орналастырылуы тиіс;

c) рұқсат етілмеген қолжетімділікті болдыртпау үшін қоймалар болғаны жөн;

d) талап етілетін қорғаныстың жалпы деңгейін төмендету үшін арнаулы қорғаныста талап ететін жабдық ұсынылады;

e) ұрлық, өрт, жарылғыш заттар, түтін, су (немесе сумен жабдықтау мәселелері), шаң, діріл, химиялық әсерлер, электр қуатының әсері, коммуникациялық әсер, электрмагнит радиация және вандализм сияқты потенциалды нақты және экологиялық қауіптерді азайту үшін басқару құралдары қабылдануы тиіс;

f) ақпаратты өңдеу құралдарына таяу тамақтану, ішу және темекі тартуға арналған ұсыныстар белгіленуі тиіс;

g) температура мен ылғалдылық сияқты қоршаған орта жағдайлары ақпаратты өңдеу құралдарына жағымсыз әсерін тигізе алатын жағдайлар үшін тексерілуі тиіс;

h) найзағайдан қорғаныс барлық ғимараттарға қолданылып, найзағайдан қорғай сүзгіштері кез келген түсетін қуаттылық пен коммуникациялық желілер үшін бейімделуі тиіс;

i) пернелі мембраналар сияқты арнаулы қорғаныс әдістерін қолдануды өнеркәсіптік орталардағы жабдықтар үшін қарастыру қажет;

j) электрмагнит әсеріне байланысты ақпараттың таратылу қаупін азайту үшін құпия ақпаратты өңдейтін жабдық қорғалуы тиіс.

11.2.2 Коммуналдық қызметтерді сүйемелдеу

Басқару шаралары

Жабдық коммуналдық қызметтерді сүйемелдеудегі қиыншылықтардан туындаған қуат беру іркілістерінен немесе басқа бұзылулардан қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Коммуналдық қызметтерді (мысалы, электр қуаты, телекоммуникациялар, сумен жабдықтау, газ, ағын сулар, вентиляция және ауаны кондициялау) сүйемелдеу:

a) жабдық өндірушісінің техникалық талаптарына және жергілікті заң талаптарына сәйкес келуге;

b) олардың іскерлік дамуға сәйкестік пен басқа коммуналдық қызметтермен әрекеттесу мүмкіндіктерін жүйелі турде бағалауға;

c) тиісті қызмет етуді қамтамасыз ету үшін жүйелі түрде тексеріліп, сыналуға;

d) іркілістерді анықтау үшін қорғау режимінде болуға;

e) қажеттілігіне орай, түрлі нақты түрде қолжетімді көптеген жіберу желілері болуға тиіс.

Апаттық жарықтандыру мен коммуникациялар қамтамасыз етілуі тиіс. Электр қуатын, суды, газды немесе басқа коммуналдық қызметтерді апаттық сөндіргіштер немесе ауыстырып қосқыштар жабдық бөлмелерінің немесе қосымша есіктердің қасында орналасуы тиіс.

Басқа ақпарат

Желілік қосылыс үшін қосымша артықтығы бірден артық сервистік жеткізушіден көптеген маршруттар арқылы алына алады.

11.2.3 Кабельдердің қауіпсіздігі

Басқару шаралары

Деректерді өткізетін немесе қосымша ақпарат қызметтерін өткізетін телекоммуникациялық кабельдер мен қуаттандыру кабельдері ұстап алудан, араласудан немесе бұзылудан сақталуы тиіс.

Іске асыру жөніндегі нұсқау

Кабельдерді қорғау үшін келесі ұсыныстарды қарастыру қажет:

a) ақпаратты өңдеу құралдарындағы қуаттандыру кабельдері мен телекоммуникациялық кабельдер қапталуы тиіс немесе балама қорғаныстық қарастыру қажет;

b) бөгеттерді болдыртпау үшін күш кабельдері коммуникациялық кабельдерден бөлек болулары тиіс;

c) сезгіш немесе маңызды жүйелер үшін қарастырылатын келешек басқару құралдары келесілерді қамтиды:

1) бақылау және аяқтау барысында сауытты құбыр мен құлыпты бөлмелер немесе қораптарды орнату;

2) кабельдерді қорғау үшін электрмагнит қоршауды пайдалану;

3) кабельдерге бұрын қосылған рұқсат етілмеген құрылғылар үшін техникалық тазарту мен нақты тексерулерді бастау;

4) панельдер мен кабельдік бөлмелерді қорғауға арналған бақыланатын қолжетімділік.

11.2.4 Жабдықтарға қызмет көрсету

Басқару шаралары

Жабдықтың ұзық қолжетімділігі мен бүтіндігін қамтамасыз ету үшін ол дұрыс сақталуы тиіс.

Енгізу нұсқаулығы

Жабдыққа қызмет көрсету үшін келесі ұсыныстарды қарастыру қажет:

a) жабдық ұсынылатын сервистік аралықтарға және жеткізушінің техникалық талаптарына сәйкес сақталуы тиіс;

b) тек өкілетті қызмет көрсету персоналы ғана сервистік қызмет көрсету мен жөндеу жұмыстарын орындауға тиіс;

c) барлық болжалды немесе іс жүзіндегі қателердің, сонымен қатар, барлық профилактикалық және түзетуші қызмет көрсету есебін жүргізу қажет;

d) қызмет көрсету ұйым аумағында немесе одан тыс орындалғанын есепке ала отырып, жабдыққа қызмет көрсетілуі тиіс болған кезде, тиісті басқару құралдары жүзеге асырылуы тиіс; қажет болған жағдайда, құпия ақпарат жабдықтан тазартылуы немесе қызмет көрсету персоналы тазартылуы тиіс;

e) сақтандыру полистері белгілеген қызмет көрсетуге қойылатын барлық талаптар орындалуы тиіс;

f) жабдыққа қызмет көрсетілгеннен кейін оны қайта қолданысқа енгізерт алдында, жабдыққа ешқандай араласулар өткізілмегеніне және ол іркіліссіз жұмыс істейтініне кепіл беру үшін жабдық тексерілуі тиіс.

11.2.5 Активтерді жою

Басқару шаралары

Жабдықтар, ақпарат немесе бағдарламалық жасақтама тиісті рұқсатсыз жұмыс аумағынан тыс алынбауға тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстарды қарастыру қажет:

a) активтерді қашықтықтан жоюға рұқсат беру өкілеттілігі бар қызметкерлер мен үшінші тарап тұтынушылары анықталуы тиіс;

b) активті жою мерзімі белгіленіп, оларды қалпына келтіру сәйкестікке тексерілуі тиіс;

c) қажет болған жағдайда, активтер қашықтықтан жойылған ретінде тіркеліп, қалпына келтірілген кезде, тіркелуі тиіс;

d) активтерге сұрау салатын немесе оларды пайдаланатын әр адам жеке басы, рөлі мен қосылуы тіркелуі тиіс және осы құжаттама жабдық, ақпарат немесе бағдарламалық жасақтамамен бірге қайтарылады.

Басқа ақпарат

Активтерді рұқсат етілмеген жоюды анықтау үшін қабылданған таңдаулы тексерістер рұқсат етілмеген жазып алу құрылғыларын, қаруды және т.б. анықтау және оларды өткізуді болдыртпау үшін орындалуы мүмкін. Осындай таңдаулы тексерістер тиісті заңнама мен нұсқаулықтарға сәйкес орындалуы тиіс. Таңдаулы тексерістер орындалғанын адамдарға хабарлау қажет. Тексерістер заң және нормативтік талаптарға сәйкес келетін рұқсат алынып орындалуы тиіс.

11.2.6 Жабдықтар мен активтердің орынжайдан тыс қауіпсіздігі

Басқару шаралары

Ұйым ғимаратының қасында түрлі қауіптерді есепке алатын қашықтықтағы активтерге қатысты қауіпсіздік қолданылуы тиіс.

Іске асыру жөніндегі нұсқау

Кез келген ақпараттық сақтау мен технологиялық жабдықты ұйым ғимаратының қасында пайдалануға басшылық рұқсат етуі тиіс. Бұл ұйым ие болған жабдықтарға және ұйым атынан қолданылатын жеке жабдыққа қатысты болады.

Қашықтықтағы жабдықты қорғау үшін келесі ұсыныстарды қарастыру қажет:

a) ұйым аумағынан тыс алынған жабдықтар мен деректер қоғамдық жерлерде қараусыз қалдырылмауы тиіс;

b) жабдықты қорғауға арналған дайындаушылардың нұсқаулықтары кез келген жағдайда тексерілуі тиіс, мысалы, күшті электрмагнит өріс әсерінен қорғау;

c) үйдегі жұмыс, қашықтықта және уақытша жұмыс орындары сияқты ұйымнан тыс жұмыс орындары үшін басқару құралдарына қауіп дәрежесін бағалау және тиісті басқару құралдары арқылы белгіленуі тиіс. Мысалы, құжаттарды сақтауға арналған құлыпты шкафтар, үстелдің анық саясаты, компьютерлерге арналған қолжетімділікті басқару құралдары мен офиспен қауіпсіз байланыс (сондай-ақ, [15][16][17][18][19] қараңыз);

d) ғимараттан тыс жабдық түрлі адамдар немесе үшінші тарап арасында қолданылған кезде, жабдыққа жауапты адамдардың аты-жөндерін және ұйымдардың атауларын анықтауға мүмкіндік беретін тіркеу сақталуы тиіс.

Қауіптер, мысалы, бұзылулар, ұрлау немесе сырттан тыңдау орналасулар арасында елеулі өзгере алады және тиісті басқару құралдарын белгілеген кезде есепке алынуы тиіс.

Басқа ақпарат

Ақпараттық сақтау және технологиялық жабдық дербес компьютерлердің, организаторлардың, ұялы телефондардың, смарт-карталардың, қағаздың немесе үй жұмысы немесе қалыпты жұмыс орнынан тасымалдау үшін қажетті басқа түрлердің барлық формаларын қамтиды.

Мобильді жабдықты қорғаудың басқа аспектілері туралы көбірек ақпаратты 6.2 тармағында табуға болады.

Қызметкерлерге қашықтықтан жұмыс істеу қауіптерін түсіндіру немесе олардың портативтік IT жабдықтарын пайдалануын шектеу арқылы қауіптерді болдырмауға болады.

11.2.7 Жабдықты қауіпсіз басқару немесе қайта пайдалану

Басқару шаралары

Кез келген осал деректер немесе лицензияланған бағдарламалық жасақтама келесі үкімге дейін немесе қайта пайдаланғанға дейін жойылғанына немесе сенімді түрде қайта жазылғанына кепіл беру үшін деректер тасымалдаушыларын қамтитын барлық жабдық тексерілуі тиіс.

Іске асыру жөніндегі нұсқау

Үкім шығарғанға дейін немесе қайта пайдаланғанға дейін деректер тасымалдаушыларының болуына кепіл беру үшін жабдық тексерілуі тиіс.

Құпия немесе авторлық құқықпен қорғалған ақпаратты қамтитын деректер тасымалдаушылары нақты бұзылуы тиіс немесе ақпарат түпнұсқалық ақпаратты қалпына келтірілмейтін қылатын техника арқылы бұзылуы, жойылуы немесе қайта жазылуы тиіс.

Басқа ақпарат

Деректер тасымалдаушыларын қамтитын бұзылған жабдық қауіп дәрежесін бағалаудың осы тармақтарды жөндеуге жіберу немесе олардан бас тартудың орнына, нақты жою қажеттілігін анықтауын талап ете алады. Ақпарат бейберекет үкім немесе жабдықты қайта пайдалану салдарынан таратылуы мүмкін.

Сонымен қатар, дисктің өшірілуін қамтамасыз ету үшін, келесі жағдайларда жабдықты жойған немесе қайта ашқан кезде, толық дискті шифрлау құпия ақпараттың ашылу қаупін азайтады:

a) шифрлау процесінің қуаттылығы жеткілікті және ол дискті толығымен қамтиды (осал кеңістікті, алмасу файлдарын және т.б. қоса алғанда);

b) дөрекі күш шабуылына қарсыласу үшін шифрлау кілттері жеткілікті түрде ұзын;

c) шифрлау кілттері өз бетінше құпия түрде сақталады (мысалы, бір дискіде ешқашан сақталмайды).

Шифрлауға қатысты қосымша ақпаратты 10-тарауда қараңыз.

Деректер тасымалдаушыларын сенімді түрде қайта жазу әдістері деректер тасымалдаушыларының технологиясына сәйкес ерекшеленеді.

Аспаптарды қайта жазу деректер тасымалдаушыларының технологиясына қолданылатынына куә болу үшін ол қарастырылуы тиіс.

11.2.8 Қараусыз қалдырылған тұтынушы жабдығы

Басқару шаралары

Тұтынушылар қараусыз қалдырылған жабдықтың тиісті қорғанысы бар екендігіне кепіл берулері тиіс.

Іске асыру жөніндегі нұсқау

Барлық тұтынушылар қараусыз қалдырылған жабдықтың қауіпсіздік талаптары мен қорғау процедуралары туралы, сондай-ақ, олардың осындай қорғанысты жүзеге асыру жөніндегі міндеттерін білуге тиіс. Тұтынушылар:

a) егер белсенді сессиялар тиісті бұғаттау механизмімен, мысалы, қорғалған скринсейвер құпиясөзбен қамтамасыз етіле алмаса, белсенді сессияларды жұмысты аяқтаған кезде аяқтауға;

b) қажеттілік аяқталған кезде, қосымшалар немесе желі қызметтерінен шығуға;

c) қолданылмаған уақытта, пернелерді бұғаттау немесе ұқсас бақылау арқылы, мысалы, қолжетімділік құпиясөзі арқылы рұқсат етілмеген қолданыстан компьютерлер немесе мобильді құрылғыларды қорғауға тиіс.

11.2.9 Таза үстел мен таза экран саясаты

Басқару шаралары

Қағаздар мен алмалы-салмалы деректер тасымалдаушылары үшін таза үстел және ақпаратты өңдеу құралдары үшін таза экран саясаты қабылдануы тиіс.

Іске асыру жөніндегі нұсқау

Таза үстел және таза экран саясаты ұйымның ақпараттық жіктелуін (8.2 қараңыз), заң және шарт талаптарын (18.1 қараңыз) және тиісті қауіптері мен мәдени аспектілерін есепке алуы тиіс. Келесі ұсыныстарды қарастыру қажет:

a) сезгіш немесе маңызды бизнес-ақпарат, мысалы, қағаздағы немесе электрондық дерек тасымалдаушыларындағы, құлыпта сақталуы тиіс (сейф немесе кабинетте немесе қауіпсіз жиһаздың басқа түрлерінде), әсіресе, офис бос болған кезде;

b) жұмыс жүргізілмеген кезде, компьютерден немесе терминалдан шығуды орындап, құпиясөз, белгі немесе ұқсас тұтынушылық сәйкестендіру механизмі басқаратын экран немесе пернелік қармау механизмімен қорғау қажет, егер құрылғы қолданылмаса, оны құлып, құпиясөздер немесе басқа басқару құралдары арқылы қорғау қажет;

c) фотокөшіру құрылғылары мен басқа көшіру технологияларын (мысалы, сканер, сандық фотоаппараттар) рұқсат етілмеген пайдалануды болдыртпау қажет;

d) сезгіш немесе құпия деректерді қамтитын ақпарат принтерлерден дереу өшірілуі тиіс.

Басқа ақпарат

Таза үстел және таза экран саясаты жұмыс уақытында және жұмыс аяқталған кезде рұқсат етілмеген қолжетімділік, ақпараттың жоғалуы мен бұзылуы қауіптерін төмендетеді. Сейфтер немесе қауіпсіз сақтау орындарының басқа түрлері, сондай-ақ, ақпаратты өрт, жер сілкінісі, су тасқыны немесе жарылыс сияқты апаттардан қорғай алады.

PIN-код функциялы принтерлерді пайдаланғанды қарастырған жөн, осылайша, ұйымдастырушылар принтердің қасында тұрып, басып шығарылған қағаздарды алатын бірден-бір адам бола алады.

12 Операциялық қауіпсіздік

12.1 Эксплуатациялық процедуралар мен міндеттер

Мақсаты: ақпаратты өңдеу құралдарының дұрыс және қауіпсіз операцияларын қамтамасыз ету.

12.1.1 Тіркелген жұмыс процестері

Басқару шаралары

Жұмыс процестері тіркеліп, олар қажет болған барлық тұтынушылар үшін қолжетімді болуы тиіс.

Іске асыру жөніндегі нұсқау

Тіркелген процедуралар компьютерді іске қосу және жұмысты аяқтау процедуралары, резервтік көшірме, жабдыққа қызмет көрсету, ақпаратты өңдеу, компьютер бөлмесі және корреспонденцияны өңдеу және қауіпсіздік сияқты ақпаратты өңдеу құралдары мен коммуникацияларға байланысты эксплуатациялық әрекеттерге дайын болуға тиіс.

Жұмыс процестері келесілерді қоса алғандағы эксплуатациялық нұсқаулықтарды белгілеуге тиіс:

a) жүйелерді қондыру және оның конфигурациясы;

b) ақпаратты автоматтандырылған және қолмен өңдеу;

c) резервтік көшірме (12.3 қараңыз);

d) басқа жүйелермен өзара тәуелділікті, жұмысты ерте бастау және жұмысты аяқтаудың соңғы сағатын қоса алғандағы талаптарды жоспарлау;

e) дұрыс емес пайдалану немесе жұмысты орындаған кезде пайда болуы мүмкін басқа ерекше жағдайларға арналған, соның ішінде, жүйелік утилиталарды пайдалануды шектеуге арналған нұсқаулықтар (9.4.4 қараңыз);

f) сыртқы сүйемелдеуді қоса алғандағы сүйемелдеу байланыстарымен күтпеген эксплуатациялық немесе техникалық қиыншылықтар жағдайында байланысады;

g) арнаулы кеңсе қағазын пайдалану немесе сәтсіз жұмыс орындарындағы өнімнен қауіпсіз құтылу процедураларын қоса алғандағы құпия өнімді басқару сияқты ерекше өндіріс пен деректерді өңдеуге арналған нұсқаулықтар (8.3 және 11.2.7 қараңыз);

h) жүйелік бас тарту жағдайында жүйелік қайта іске қосу мен қалпына келтіру процедуралары;

i) бақылау журналы мен тіркеу туралы жүйелік ақпаратты басқару (12.4 қараңыз);

j) бақылау процедуралары.

Жұмыс процестері мен жүйелік әрекеттердің тіркелген процедураларын ресми құжаттар мен басшылық рұқсат еткен өзгерістер ретінде қарастыру қажет. Техникалық түрде орындала алатын жерде бірдей процедуралар, аспаптар мен утилиталарды пайдаланып, ақпараттық жүйелерді жүйелі түрде басқару қажет.

12.1.2 Өзгерістерді басқару

Басқару шаралары

Ұйымның, бизнес-процестердің, ақпаратты өңдеу құралдарының және ақпараттық қауіпсіздікке қатысты жүйелердің өзгерістерін басқару қажет.

Енгізу нұсқаулығы

Келесі ұсыныстарды қарастыру қажет:

a) елеулі өзгерістерді тіркеу және жазып алу;

b) өзгерістерді жоспарлау және сынау;

c) қауіпсіздіктің ақпараттық әсерін қоса алғандағы осындай өзгерістердің потенциалды әсерлерін бағалау;

d) ұсынылған өзгерістерді ресми мақұлдау процедурасы;

e) ақпараттық қауіпсіздік талаптарының болмауын тексеру;

f) өзгерістер турады мәлімдемелер барлық тиісті адамдарға жіберіледі;

g) шегіну процедуралары, соның ішінде, сәтсіз өзгерістер мен күтпеген оқиғаларды тоқтату және кейін қалпына келтіру процедуралары мен міндеттер;

h) барлық инциденттерді шешу үшін қажетті өзгерістерді тез және бақылап енгізуге мүмкіндік беру үшін төтенше өзгерту процесін ұсыну (16.1 қараңыз).

Барлық өзгерістерді қанағаттанарлық бақылау үшін ресми басқару функциялары мен процедуралары болуы тиіс. Өзгерістер енгізілген кезде, барлық өзекті ақпаратты қамтитын бақылау журналы сақталуы тиіс.

Басқа ақпарат

Ақпаратты өңдеу құралдары мен жүйелердің өзгерістерін бақыламау – қауіпсіздік немесе жүйе сәтсіздіктерінің жиі кездесетін себебі. Жұмыс ортасын өзгерту, әсіресе, жіберу сатысынан жұмыс сатысына, мәлімдемелердің сенімділігіне әсер ете алады (14.2.2 қараңыз).

12.1.3 Толық басқару

Басқару шаралары

Ресурстарды пайдаланутексеріліп, бапталуы тиіс. Қажетті жүйелік жұмысты қамтамасыз ету үшін келешек толық басқару жоспары әзірленуі тиіс.

Іске асыру жөніндегі нұсқау

Мүдделі жүйенің іскерлік маңыздылығын есепке ала отырып, басқару талаптары белгіленуі тиіс. Жүйелік баптау мен бақылау жүйелердің қолжетімділігі мен тиімділігін жақсарту үшін қолданылуы тиіс. Келешек басқару талаптарының жоспары жаңа іскерлік және жүйелік талаптарды және ұйымның ақпаратын өңдеу мүмкіндіктеріндегі қолданылатын және жобаланған үрдістерді есепке алуы тиіс.

Сатып алу тапсырысы ұзақ орындалатын немесе бағасы қымбат кез келген ресурстарға көңіл аударған жөн; сондықтан, менеджерлер түйінді жүйе ресурстарын

пайдалануды бақылаулары тиіс. Олар әсіресе ақпараттық жүйелер немесе бизнес-қосымшаларды басқару аспаптарына қатысты пайдаланудағы үрдістерді белгілеуі тиіс.

Жүйелер немесе қызметтерге төнетін қауіптерді болжай алатын және тиісті шараларды жоспарлай алатын жетекші мамандарға тәуелді потенциалды бөгеттерді анықтау және оларды болдыртпау үшін менеджерлер осы ақпаратты қолдануы тиіс.

Қабілеттілікті арттыру немесе талапты төмендету арқылы жеткілікті қабілеттілікті қамтамасыз етуге болады. Басқарушы толық талап мысалдары:

a) ескірген деректерді өшіру (диск кеңістігі);

b) мәлімдемелер, жүйелер, деректер базалары немесе қоршаған ортаны жазып алу;

c) сериялы өндіріс пен кестені оңтайландыру;

d) қолданбалы логика немесе деректер базасының сұрақтарын оңтайландыру;

e) бизнес маңызды емес болған жағдайда, ақпаратты өткізу желілерін болдыртпау немесе шектеу (мысалы, видеоның жайылып кетуі).

Тіркелген толық басқару жоспарын деректерге үздіксіз қолжетімділігі бар жүйелер үшін қарастыру қажет.

Басқа ақпарат

Осы бақылау, сондай-ақ, адам ресурстарының қабілеттеріне, офистер мен құралдарға қатысты.

12.1.4 Даму, сынау және жұмыс орталарын бөлу

Басқару шаралары

Жұмыс ортасына рұқсат етілмеген қолжетімділік немесе оны өзгерту қауіптерін азайту үшін даму, сынау және жұмыс орталары бөлінуі тиіс.

Іске асыру жөніндегі нұсқау

Эксплуатациялық мәселелерді болдыртау үшін қажетті жұмыс, сынақ және даму орталары арасындағы бөлініс деңгейі белгіленіп, енгізілуі тиіс.

Келесі ұсыныстарды қарастыру қажет:

a) әзірлемеден пайдалануға дейінгі бағдарламалық жасақтаманы жіберу ережелері белгіленіп, тіркелуі тиіс;

b) даму және эксплуатациялық бағдарламалық жасақтама түрлі жүйелерде немесе компьютерлік процессорларда және түрлі салаларда немесе анықтамалықтарда басқарылуы тиіс;

c) эксплуатациялық жүйелер мен мәлімдемелерді өзгерту эксплуатациялық жүйелерге қатысты қолданылғанға дейін сынақ барысында немесе қоршаған ортада тексерілуі тиіс;

d) ерекше жағдайлардан басқа, сынау эксплуатациялық жүйелерде жүргізілмеуі тиіс;

e) компилятор, редактор мен басқа әзірлеу құралдары немесе жүйелік бағдарламалар эксплуатациялық жүйелер үшін қолжетімді болмауы тиіс;

f) тұтынушылар эксплуатациялық және тексеру жүйелері үшін түрлі тұтынушы профильдерін қолдануы тиіс, ал мәзір қате қаупін азайту үшін тиісті сәйкестендіргіш мәлімдемелерді көрсетуі тиіс;

g) егер балама басқару құралдары сынау жүйесі үшін қамтамасыз етілмесе, осал деректер сынаудың жүйелік қоршаған ортасына көшірілмеуі тиіс (14.3 қараңыз).

Басқа ақпарат

Даму және сынақ әрекеттері күрделі қиыншылықтар тудыра алады, мысалы, файлдардың немесе қоршаған орта жүйесінің тиімсіз түрленуі немесе жүйенің істен шығуы. Елеулі сынақты орындау және әзірлеушінің жұмыс ортасына сәйкес емес қолжетімділігін болдыртпау мүмкіндігі бар белгілі және тұрақты қоршаған ортаны сүйемелдеу қажеттілігі бар.

Егер дамыту және сынақтарды өткізу жөніндегі қызметкерлердің эксплуатациялық жүйе мен оның ақпаратына қолжетімділігі болса, олар рұқсат етілмеген және

тексерілмеген кодексті енгізуге немесе жұмыс деректерін өзгертуге қабілетті болады. Кейбір жүйелерде айлакерлік жасау немесе күрделі эксплуатациялық қиыншылықтар тудыра алатын тексерілмеген немесе зиянды кодты енгізу үшін осы қабілет дұрыс емес қолданыла алады.

Дамыту және сынақтарды өткізу жөніндегі персонал, сондай-ақ, эксплуатациялық ақпараттың құпиялылығына қауіп төндіреді.

Даму және сынақ әрекеттері бір есептегіш қоршаған ортасын бөлген жағдайда, олар бағдарламалық жасақтаманың немесе ақпараттың абайсыз өзгерістерін тудыра алады. Эксплуатациялық бағдарламалық жасақтаманы немесе коммерциялық ақпаратты кездейсоқ өзгерту немесе оларға рұқсат етілмеген қолжетімділік қауіптерін азайту үшін даму, сынау және жұмыс орталарын бөлу маңызды (сынақ деректерін қорғау үшін 14.3 қараңыз).

12.2 Зиянды бағдарламалық жасақтамадан қорғау

Мақсаты: ақпарат пен ақпаратты өңдеу құралдарының зиянды бағдарламалық жасақтамадан қорғалуын қамтамасыз ету.

12.2.1 Зиянды бағдарламалық жасақтамаға қарсы басқару құралдары

Басқару шаралары

Зиянды бағдарламалық жасақтамадан қорғау үшін анықтау, болдыртпау және қалпына келтіруді басқару құралдары тиісті тұтынушы хабардарлығымен бірге жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқау

Зиянды бағдарламалық жасақтамадан қорғау зиянды бағдарламалық жасақтаманы анықтауға және қалпына келтіруші бағдарламалық жасақтамаға, ақпараттық қауіпсіздік хабардарлығына және тиісті жүйелік қолжетімділікке және өзгерістерді басқару құралдарына негізделуі тиіс. Келесі нұсқауды қарастыру қажет:

a) рұқсат етілмеген бағдарламалық жасақтаманы пайдалануға тыйым салатын ресми саясатты белгілеу (12.6.2 және 14.2 қараңыз);

b) рұқсат етілмеген бағдарламалық жасақтаманы пайдалануды болдыртпайтын немесе анықтайтын басқаруды енгізу (мысалы, қауіпсіздік тексерісінен өткен тұлғалар тізімі бойынша жұмыс істейтін қосымша);

c) белгілі немесе күдікті зиянды веб-сайттарды пайдалануды болдыртпайтын немесе анықтайтын басқару құралдарын жүзеге асыру (мысалы, қара тізімге енгізу);

d) қандай қорғау шаралары қолданылуға тиіс екендігін белгілеп, сыртқы желілерден немесе сыртқы желілер арқылы немесе кез келген басқа құралдан файлдарды және бағдарламалық жасақтаманы алуға байланысты қауіптерден қорғауға арналған ресми саясатты белгілеу;

e) зиянды бағдарламалық жасақтама пайдалануы мүмкін осал жерлерді қысқарту, мысалы, осалдықты техникалық басқару арқылы (12.6 қараңыз);

f) бағдарламалық жасақтама мен маңызды іскерлік процестерді сүйемелдейтін жүйелер деректерінің мазмұнына жүйелі түрде шолу жасау; кез келген бекітілмеген файлдардың немесе рұқсат етілмеген түзетулердің болуы ресми түрде зерттелуі тиіс;

g) компьютерлерді және деректерді ескертуші бақылау ретінде немесе қарапайым негізде қарау үшін анықтау және қалпына келтіру зиянды бағдарламалық жасақтаманы қондыру және жүйелі түрде жаңарту; сканерлеу келесілерді қамтиды:

1) желілер немесе деректер тасымалдаушыларының кез келген түрі арқылы алынған файлдарды пайдаланар алдында зиянды бағдарламалық жасақтамаға тексеру;

2) электрондық пошта қосымшалары мен жүктемелерді пайдаланар алдында зиянды бағдарламалық жасақтамаға тексеру; осы тексеріс түрлі орындарда орындалуы тиіс, мысалы, электрондық пошта серверлерінде, үстел компьютерлерінде және ұйым желісіне кірген кезде;

3) зиянды бағдарламалық жасақтамаларды анықтау үшін веб-парақшаларды тексеру;

h) жүйелерде зиянды бағдарламалық жасақтамалардан қорғаумен жұмысқа арналған процедуралар мен міндеттерді белгілеу, оларды пайдалануды үйрету, зиянды шабуылдардан кейін хабарлау және қалпына келтіру;

i) зиянды шабуылдардан кейін қалпына келтіру үшін бизнестің үздіксіздігін қамтамасыз етудің тиісті жоспарларын дайындау, соның ішінде, барлық қажетті деректер мен бағдарламалық жасақтаманың резервтік көшірмесі мен қалпына келтіру шаралары (12.3 қараңыз);

j) таратылым тізімдеріне жазылу немесе жаңа зиянды бағдарламалық жасақтама туралы ақпарат беретін веб-сайттарды растау сияқты ақпаратты жүйелі түрде жинау үшін процедураларды пайдалану;

k) зиянды бағдарламалық жасақтамаға қатысты ақпаратты тексеру үшін және ескертулер дәл және ақпаратқа толы екендігіне кепіл беру үшін процедураларды жүзеге асыру; менеджерлер жалған және нақты зиянды бағдарламалық жасақтамаларды бөліп айыру үшін білікті дереккөздер, мысалы, әйгілі журналдар, сайт өндіруге арналған бағдарламалық жасақтамаларды сенімді қорғау үшін қолданылатынына кепіл беруге тиіс; барлық тұтынушылар алдау мәселесі туралы және оларды алдау әрекеті болған кезде не жасау қажеттігін білулері қажет;

l) апаттық әсерлер аяқталуы мүмкін қоршаған ортаны оқшаулау.

Басқа ақпарат

Түрлі сатушылардан алынған ақпараттық орта арқылы зиянды бағдарламалық жасақтамаға қарсы екі немесе одан артық қорғайтын бағдарламалық жасақтамаларды пайдалану зияннан қорғау тиімділігін жақсарта алады.

Қалыпты зияннан қорғау құралдарын айналып өте алатын қызмет көрсету және төтенше процедуралар барысында зиянды бағдарламалық жасақтаманы енгізуден қорғау үшін мұқият болу қажет.

Белгілі жағдайларда зияннан қорғау операциялар шеңберінде толқулар тудыра алады.

Тек зиянды бағдарламалық жасақтаманы анықтау және жөндеу құралын зияннан қорғау ретінде пайдалану сәйкес келмейді және зиянды бағдарламалық жасақтаманы енгізуді болдыртпайтын жұмыс процестерімен сүйемелденуі тиіс.

12.3 Резервтік көшірме

Мақсаты: деректерді жоғалтудан қорғау.

12.3.1 Ақпараттық резервтік көшірме

Басқару шаралары

Ақпараттың, бағдарламалық жасақтаманың және жүйелік бейнелердің резервтік көшірмелері жасалып, келісілген резервтік саясатқа сәйкес жүйелі түрде тексерілуі тиіс.

Іске асыру жөніндегі нұсқау

Ұйымның ақпараттың, бағдарламалық жасақтаманың және жүйелердің резервтік көшірмелеріне арналған талаптарын белгілеу үшін резервтік саясат белгіленуі тиіс.

Резервтік көшірме саясаты қорғау және сақтау талаптарын белгілеуі тиіс.

Деректерді сақтау жүйесі істен шыққаннан кейін немесе апаттан кейін барлық маңызды ақпарат пен бағдарламалық жасақтамалар қалпына келтіре алатындығын қамтамасыз ету үшін тиісті резервтік қызметтер ұсынылуы тиіс.

Резервтік жоспарды жобалаған кезде келесі талаптар есепке алынуы тиіс:

a) резервтік көшірмелердің дәл және толық есептері мен тіркелген қалпына келтіру процедуралары құрылуы тиіс;

b) резервтік көшірмелердің дәрежесі (мысалы, толық немесе ерекше резервтік көшірме) мен жиілігі ұйымның іскерлік талаптарын, қамтылған ақпараттың қауіпсіздік талаптарын және ұйымның ұзақ қызметіне қатысты ақпараттың маңыздылығын көрсетеді;

c) басты орындағы бұзылудан кез келген зақымдануды болдыртпау үшін резервтік көшірмелер жеткілікті қашықтықтағы орында сақталуы тиіс;

d) резервтік ақпарат үшін басты орында қолданылатын стандарттармен үйлесетін нақты қорғаныс пен қоршаған ортаны қорғаудың (11-тарауды қараңыз) тиісті деңгейін беру қажет;

e) резервтік деректерді төтенше жағдайда қолдануға болатынын қамтамасыз ету үшін олар жүйелі түрде тексерілуі тиіс; бұл қалпына келтіру процедураларын сынаумен біріктіріліп, қалпына келтірудің талап етілетін уақытына тексерілуі тиіс. Сүйемелденген деректерді қалпына келтіру қабілетін сынау, резервтік көшірме немесе қалпына келтіру процесі деректерге өтелмейтін шығын әкелген немесе олардың жоғалуына әкелген жағдайда, түпнұсқалық деректерді қайта жазбай, арнаулы сынақ деректерінде орындалуы тиіс;

f) құпиялылық маңызды болған жағдайда, резервтік көшірмелер шифрлау арқылы қорғалуы тиіс.

Резервтік көшірмелердің толықтығын резервтік көшірмелер саясатына сәйкес қамтамасыз ету үшін эксплуатациялық процедуралар резервтік көшірмелердің орындалуын бақылап, жоспарланған резервтік көшірмелер қателерін жіберуі тиіс.

Бөлек жүйелер мен қызметтерге арналған резервтік шаралар бизнес ұздіксіздігін қамтамасыз ету жоспарының талаптарына сәйкес келуі үшін олар жүйелі түрде тексерілуі тиіс. Маңызды жүйелер мен қызметтер жағдайында, резервтік шаралар апат жағдайында толық жүйені қайтару үшін қажетті жүйелер, мәлімдемелер мен деректер туралы барлық ақпаратты қамтуы тиіс.

Тұрақты түрде сақталатын мұрағат көшірмелеріне арналған кез келген талапты есепке ала отырып, маңызды іскерлік ақпаратты сақтау мерзімі белгіленуі тиіс.

12.4 Тіркеу және бақылау

Мақсаты: оқиғаларды жазып алу және айғақтарды қамтамасыз ету.

12.4.1 Оқиғаларды тіркеу

Басқару шаралары

Тұтынушы әрекеттерін, ерекшеліктерді, қателерді және ақпараттық қауіпсіздік оқиғаларын жазып алатын оқиғалар журналы жүргізілуі, сақталуы және жүйелі түрде қарастырылуы тиіс.

Іске асыру жөніндегі нұсқау

Оқиғалар журналы келесі өзекті ақпаратты қамтуы тиіс:

a) тұтынушылардың сәйкестендіргіштері;

b) жүйелік әрекеттер;

c) түйінді оқиғалардың күні, уақыты мен егжей-тегжейлері, мысалы жүйеге кіру және жүйеден шығу;

d) құрылғы сәйкестігі немесе, мүмкін болса, оның орналасуы және жүйелік сәйкестендіргіш;

e) сәтті және рұқсат етілмеген жүйелік қолжетімділік әрекеттерінің есебі;

f) сәтті және рұқсат етілмеген деректер мен басқа ресурстарға қолжетімділік әрекеттерінің есептері;

g) жүйелік конфигарцияны өзгерту;

h) артықшылықтарды пайдалану;

i) жүйелік бағдарламалар мен мәлімдемелерді пайдалану;

j) қолжетімділік алу файлдары мен қолжетімділік түрі;

k) желі мекенжайлары мен хаттамалары;

l) қолжетімділікті басқару жүйесінің дабыл қағуы;

m) антивирустық жүйелер мен араласуды анықтау жүйелері сияқты қорғау жүйелерін активациялау және дезактивациялау;

n) тұтынушылардың мәлімдемелерде орындаған мәміле есептері.

Оқиғаларды тіркеу жинақ есепті құруға және қауіпсіздік жүйесінің дабылдарын тудыруға қабілетті автоматтандырылған мониторинг жүйелерінің негізін қалайды.

Басқа ақпарат

Оқиғалар журналы осал деректер мен жеке деректерді қамтуы мүмкін. Құпиялылықты қамтамасыз ету бойынша тиісті шаралар қабылдануы тиіс (18.1.4 қараңыз).

Егер мүмкін болса, жүйелік әкімшілерде өздерінің әрекеттерінің журналдарын жоюға немесе дезактивациялауға рұқсаты болмауы тиіс (12.4.3 қараңыз).

12.4.2 Тіркеу туралы ақпаратты қорғау

Басқару шаралары

Құралдарды тіркеу және тіркеу туралы ақпарат араласудан және рұқсат етілмеген қолжетімділіктен қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Ақпаратты және тіркелетін құралға байланысты эксплуатациялық қиыншылықтарды тіркеу үшін басқару құралдары рұқсат етілмеген өзгерістерден қорғалуы тиіс, соның ішінде:

a) тіркелген хабарландырулар типін өзгерту;

b) өзгертілген немесе өшірілген жүйелік журнал файлдары;

c) жазбаны жасаудан бас тартуға немесе бұрынғы тіркелген оқиғаларды қайта жазуға әкелетін жүйелік журнал артық файлының деректерінің сыйымдылығы.

Ұстап алу саясатының бөлігі ретінде мұрағаттау үшін немесе айғақтарды жинау және сақтау талаптарына (16.1.7 қараңыз) байланысты кейбір бақылау журналдары талап етілуі мүмкін.

Басқа ақпарат

Жүйелік тіркеулер жиі ақпараттың үлкен көлемін қамтиды, оның үлкен бөлігі қауіпсіздік жағдайын ақпараттық бақылау үшін бөгде болып табылады. Қауіпсіздік жағдайын бақылау мақсатында елеулі оқиғаларды анықтау үшін тиісті хабарландыру көшірмесі автоматтық түрде екінші тіркеуде басылады немесе жүйелердің немесе бақылау аспаптарының тиісті бағдарламаларын пайдалануды файлға сұрау салу үшін қарастырылуы тиіс.

Жүйелік тіркеулер қорғалуы тиіс, себебі, деректер өзгертіле немесе өшіріле алынған жағдайда, олардың болуы жалған қауіпсіздік күйін тудыра алады. Жүйелік әкімші немесе оператор бақылауынан тыс тіркеулерді көшіру тіркеулерді қорғау үшін қолданылуы мүмкін.

12.4.3 Әкімші және операторды тіркеу

Басқару шаралары

Жүйелік әкімші мен оператордың жүйедегі әрекеттері тіркеліп, тіркеулер қорғалуы және жүйелі түрде тексерілуі тиіс.

Іске асыру жөніндегі нұсқау

Тұтынушының есеп жазбасының артықшылықты иелері тікелей басқару арқылы ақпаратты өңдеу құралдарының жүйесіне кіруді басқара алады, сондықтан, артықшылықты тұтынушылар үшін жауапкершілікті сүйемелдеу үшін тіркеулерді қорғап, қарастыру қажет.

Басқа ақпарат

Жүйені және жүйелік әкімшілерді бақылаудан тыс басқарылатын араласуды анықтау жүйесі жүйелік әкімшілікті және желі әкімшілігінің әрекеттерін сәйкестікке тексеру үшін қолданылуы мүмкін.

12.4.4 Сағатты сәйкестендіру

Басқару шаралары

Ұйымдағы немесе қауіпсіздік доменіндегі жүйелердің өзекті ақпаратын өңдейтін барлық құралдардың сағаттары бірыңғай анықтамалық уақыт дереккөзіне сәйкес синхрондалуы тиіс.

Іске асыру жөніндегі нұсқау

Уақыт, синхрондау және дәлдікті ұсыну үшін сыртқы және ішкі талаптар тіркелуі тиіс. Осындай талаптар заң, реттеу, шарт талаптары, стандарт немесе ішкі бақылау талаптары бола алады. Ұйымда қолдану үшін стандартты анықтамалық сағат белгіленуі тиіс.

Ұйымның анықтамалық сағатты сыртқы дереккөзден алу тәсілі мен ішкі сағаттарды дұрыс синхрондау тіркеліп, жүзеге асырылуы тиіс.

Басқа ақпарат

Тергеу үшін немесе заң немесе тәртіп бұзу жағдайларында айғақ ретінде талап етілуі мүмкін бақылау журналдарының дәлдігін қамтамасыз ету үшін компьютерлік сағаттарды дұрыс баптау маңызды. Дәл емес бақылау журналдары осындай тергеулерге кедергі келтіріп, осындай айғақтарға қатысты күдік тудырады. Ұлттық атомдық сағаттардан уақытты радио жіберуге байланысты сағаттар жүйелерді тіркеу үшін негізгі сағат ретінде қолданыла алады. Уақыттың желілік хаттамасы барлық серверлерді негізгі сағатпен синхрондау үшін қолданыла алады.

12.5 Эксплуатациялық бағдарламалық жасақтаманы бақылау

Мақсаты: эксплуатациялық жүйелердің бүтіндігін қамтамасыз ету.

12.5.1 Эксплуатациялық жүйелерде бағдарламалық жасақтаманы қондыру

Басқару шаралары

Эксплуатациялық жүйелерде бағдарламалық жасақтаманы қондыруды басқару үшін процедуралар жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстар эксплуатациялық жүйелердегі бағдарламалық жасақтама өзгерістерін басқарады:

a) эксплуатациялық бағдарламалық жасақтаманы, бағдарламаның қосымшалары мен библиотекаларын жаңартуды тек тиісті басқарушылық рұқсатқа оқытылған әкімшілер орындауға тиіс (9.4.5 қараңыз);

b) эксплуатациялық жүйелер даму коды немесе компиляторларды емес, мақұлданған орындалатын бағдарламаны қамтуы тиіс;

c) операциялық жүйенің қосымшалары мен бағдарламалық жасақтамасы тек кең және сәтті сынақтан кейін ғана жүзеге асырылуы тиіс; сынақтар пайдалану қолайлығын, қауіпсіздікті, басқа жүйелерге әсерін және пайдалану оңайлығын қамтып, бөлек жүйелерде орындалуы тиіс (12.1.4 қараңыз); бағдарламалар дереккөздерінің барлық тиісті библиотекалары жаңартылуын білген жөн;

d) барлық жүзеге асырылған бағдарламалық жасақтамаларды, сондай-ақ, жүйелік құжаттаманы бақылау үшін конфигурацияны басқару жүйесі қолданылуы тиіс;

e) өзгерістер жүзеге асырылғанға дейін қайтару стратегиясы болуы тиіс;

f) бақылау журналы бағдарламаның эксплуатациялық библиотекаларының барлық жаңартуларынан тұруы тиіс;

g) қолданбалы бағдарламалық жасақтаманың бұрынғы нұсқалары күтпеген жағдайда қолданылатын шара ретінде сақталуы тиіс;

h) бағдарламалық жасақтаманың ескі нұсқалары барлық сұралған ақпарат пен параметрлермен, процедуралармен, конфигурация нақтылауларымен және сүйемелдеуші бағдарламалық жасақтамасымен бірге деректер сақталған мерзімге сәйкес сақталуы тиіс.

Эксплуатациялық жүйелерде қолданылатын сатушының жеткізетін бағдарламалық жасақтамасы жеткізуші сүйемелдеген деңгейде сақталуы тиіс. Ұзақ уақыт ішінде бағдарламалық жасақтама сатушылары бағдарламалық жасақтаманың ескі нұсқаларын сүйемелдеуді тоқтатады. Ұйым сүйемелденбеген бағдарламалық жасақтамаға сену қауіптерін қарастыруы тиіс.

Жаңа нұсқа шыққанға дейін жаңарту жөніндегі кез келген шешім нұсқа өзгерістері мен қауіпсіздігіне қатысты іскерлік талаптарды есепке алуы тиіс, мысалы, қауіпсіздіктің жаңа ақпараттық функционалдығын енгізу немесе осы нұсқаға қатысты ақпараттық қауіпсіздік мәселелерінің саны мен маңыздылығы. Бағдарламалық жасақтама бөліктері қауіпсіздіктің ақпараттық осал жерлерін жоюға немесе азайтуға көмектескен кезде, олар қолданылуы тиіс (12.6 қараңыз).

Жеткізушілерге нақты және логикалық қолжетімділікті тек сүйемелдеу мақсатында беру қажет. Жеткізуші әрекеттері тексерілуі тиіс (15.2.1 қараңыз).

Қауіпсіздіктің осал жерлерінің себебі бола алатын рұқсат етілмеген өзгертулерді болдыртпау үшін бағдарламалық жасақтама тексерілуге және басқарылуға тиісті сырттан жеткізілетін бағдарламалық жасақтама мен модульдерге сүйене алады.

12.6 Осалдықты техникалық басқару

Мақсаты: техникалық осал жерлерді пайдалануды болдыртпау.

12.6.1 Техникалық осал жерлерді басқару

Басқару шаралары

Ақпараттық жүйелер қолданатын техникалық осал жерлер туралы ақпарат уақытында алынып, осындай осал жерлердің ұйымға әсері бағаланып, оған байланысты қауіппен жұмыс істеу үшін тиісті шаралар қолданылуы тиіс.

Іске асыру жөніндегі нұсқау

Ағымдағы және толық активтер тізілімі (8-тарауды қараңыз) осалдықты тиімді техникалық басқару үшін алғышарт болып табылады. Белгілі ақпарат, соның ішінде, сатушының бағдарламалық жасақтамасы, нұсқа нөмірлері, ашудың қазіргі күйі (мысалы, қай бағдарламалық жасақтама қай жүйеде қондырылды) және бағдарламалық жасақтамаға жауапты адам, осалдықты техникалық басқаруды сүйемелдеуі тиіс.

Тиісті және уақтылы шаралар потенциалды техникалық осал жерлерді анықтауға жауап ретінде қабылдануы тиіс. Техникалық осал жерлер үшін тиімді басқарушылық процесті белгілеу үшін келесі нұсқау сақталуы тиіс:

a) ұйым осалдықты бақылау, осалдық қауіп дәрежесін бағалау, түзетулер енгізу, активті қадағалау және координация бойынша кез келген талап етілетін міндеттерді қоса алғандағы осалдықты техникалық басқаруға байланысты рөлдер мен міндеттерді белгілеуі тиіс;

b) тиісті техникалық осал жерлерді анықтау және олар туралы хабардарлықты сүйемелдеу үшін қолданылатын ақпараттық ресурстар бағдарламалық жасақтама мен

басқа технологиялар (активтер тізіліміне негізделген, 8.1.1 қараңыз) үшін белгіленуі тиіс; осы ақпараттық ресурстар тізімдегі өзгерістер негізінде немесе жаңа немесе пайдалы ресурстар табылған кезде жаңартылуы тиіс;

c) потенциалды сәйкес келетін техникалық осал жерлер туралы хабарландыруларға жауап беру үшін уақыт кестесі белгіленуі тиіс;

d) потенциалды техникалық осалдық белгіленген кезде, ұйым оған байланысты қауіптер мен қолданылатын әрекеттерді белгілеуі тиіс; осындай әрекет осал жүйелерге түзетулер енгізуді немесе басқа басқару құралдарын пайдалануды қамти алады;

e) техникалық осалдықтың қаншалықты дереу жойылу қажеттілігіне байланысты қолданылатын шаралар өзгерістерді басқаруға байланысты басқару құралдарына сәйкес (12.1.2 қараңыз) немесе қауіпсіздік инциденттеріне жауап беру процедураларын орындау арқылы (16.1.5 қараңыз) орындалуы тиіс;

f) егер аумақ заңды дереккөзден қолжетімді болса, аумақты қондыруға байланысты қауіптер бағалануы тиіс;

g) аумақтар тиімді екендігін және олар жол берілмейтін жағымсыз әсер етпейтінін қамтамасыз ету үшін олар қондырылғанға дейін тексерілуі және бағалануы тиіс; егер ешқандай аумақ қолжетімді болмаса, басқа басқару құралдарын қарастыру қажет:

1) осалдыққа қатысы бар қызметтер мен мүмкіндіктерді сөндіру;

2) қолжетімділікті басқару құралдарын бейімдеу немесе қосу, мысалы, желі шекараларындағы брандмауэрлер (13.1 қараңыз);

3) іс жүзіндегі шабуылдарды анықтау үшін ұлғайтылған бақылау;

4) осалдықты түсінуді арттыру;

h) барлық қолданылған процедуралар үшін бақылау журналы сақталуы тиіс;

i) осалдықты басқарудың техникалық процесінің тиімділігін қамтамасыз ету үшін ол жүйелі түрде тексерілуі және бағалануы тиіс;

j) аса қауіпті жүйлер ең алдымен өңделуі тиіс;

k) осалдық туралы деректерді инциденттерге жауап беру функциялары үшін хабарлау үшін тиімді техникалық басқару процесі басқарушылық инцидент әрекеттеріне бейімделуі тиіс;

l) осалдық анықталған, бірақ ешқандай қарсы шара жоқ жағдайда жұмыс істеу үшін процедураны белгілеу қажет. Бұл жағдайда ұйым белгілі осалдыққа қатысты қауіптерді бағалап, тиісті түзетуші әрекеттерді белгілеуі тиіс.

Басқа ақпарат

Осалдықты техникалық басқару өзгерістерді басқарудың ішкі функциясы ретінде қарастырылуы мүмкін және өз мақсатында өзгерістерді басқару процестері мен процедураларын қолдануы мүмкін (12.1.2 және 14.2.2 қараңыз).

Сатушылар патчтерді (жаңартуларды) тезірек шығаруы үшін елеулі қысым объектісі болып табылады. Сондықтан, аумақ мәселені шешпей, теріс жағымсыз әсерін тигізу мүмкіндігі бар. Сонымен қатар, кейбір жағдайларда патч қолданылғаннан кейін патчты оңай өшіру мүмкін емес.

Егер шығындарға немесе ресурстардың болуына байланысты аумақтарды сынау мүмкін емес болса, түзетулер енгізу кідірісі басқа тұтынушылар хабарлаған тәжірибеге негізделген қауіптерді бағалайды. [14] қолдану тиімді бола алады.

12.6.2 Бағдарламалық жасақтаманы орнатуды шектеу

Басқару шаралары

Тұтынушылардың бағдарламалық жасақтаманы қондыруын басқаратын ережелер белгіленіп, енгізілуі тиіс.

Іске асыру жөніндегі нұсқау

Ұйым бағдарламалық жасақтаманың типтері қондырыла алатын қатаң саясатты белгілеп, жүзеге асыруы тиіс.

Ең аз артықшылықтар принципі қолданылғаны жөн. Егер белгілі артықшылықтар берілсе, тұтынушылардың бағдарламалық жасақтаманы қондыру мүмкіндігі болуы мүмкін. Ұйым бағдарламалық жасақтаманың қай типтерін қондыруға рұқсат етілгенін (мысалы, бар бағдарламалық жасақтама жаңартулары мен қауіпсіздік аумақтары) және қай типтерін қондыруға тыйым салынғанын (мысалы, тек жеке қолданысқа арналған бағдарламалық жасақтама және потенциалды зиянды бола алатын, шығу тегі белгісіз немесе күдікті болатын бағдарламалық жасақтама) белгілеуі тиіс. Осы артықшылықтарды мүдделі тұтынушылардың рөлдерін есепке ала отырып ұсыну қажет.

Басқа ақпарат

Есептегіш құрылғыларда бағдарламалық жасақтаманы жүйелі түрде қондыру осал жерлердің пайда болуына, кейін ақпараттың жайылуына, бүтіндіктің жоғалуына немесе басқа ақпараттық қауіпсіздік инциденттеріне немесе зияткерлік меншік құқықтарының бұзылуына әкеле алады.

12.7 Ақпараттық жүйелер аудиті

Мақсаты: эксплуатациялық жүйелер бойынша бақылау әрекеттердің әсерін азайту.

12.7.1 Ақпараттық жүйелер аудитін басқару құралдары

Басқару шаралары

Бизнес-процестердің бұзылуын азайту үшін эксплуатациялық жүйелерді тексеруді қамтитын бақылау талаптыра мен әрекеттері мұқият жоспарланып, келісілуі тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстарды қарастыру қажет:

a) жүйелер мен деректерге қолжетімділікке арналған бақылау талаптары тиісті басқарумен келісілуі тиіс;

b) техникалық аудиторлық сынақтар көлемін келісіп, басқару қажет;

c) аудиторлық сынақтар бағдарламалық жасақтама мен деректерге тек оқу үшін қолжетімілікпен шектелуі тиіс;

d) аудит аяқталған кезде, өшірілуі тиіс жүйелік файлдардың оқшауланған көшірмелері үшін ғана тек оқу үшін қолжетімділіктен артық беріле алады;

e) арнайы немесе қосымша өңдеуге қойылатын талаптар белгіленіп, келісілуі тиіс;

f) жүйелік қолжетімділікті қолдана алатын аудиторлық сынақтарды жұмыс уақытынан тыс басқару қажет;

g) анықтамалық ізді жүргізу үшін барлық қолжетімділік тексеріліп, тіркелуі тиіс.

13 Коммуникациялар қауіпсіздігі

13.1 Желі қауіпсіздігін басқару

Мақсаты: ақпарат пен ақпаратты өңдеу құралдарын желілерде қорғау.

13.1.1 Желілік басқару құралдары

Бақылау

Ақпаратты жүйелер мен мәлімдемелерде қорғау үшін желілерді басқару қажет.

Іске асыру жөніндегі нұсқау

Желідегі ақпаратты және оған байланысты қызметтерді рұқсат етілмеген қолжетімділіктен қорғалуын қамтамасыз ету үшін басқару құралдары жүзеге асырылуы тиіс. Келесі тармақтарды қарастыру қажет:

a) желілік жабдықты басқаруға арналған міндеттер мен процедуралар белгіленуі тиіс;

b) желілерге эксплуатациялық жауапкершілік компьютерлік операциялардан бөлінуі тиіс (6.1.2 қараңыз);

c) жалпыға қолжетімді желілер немесе сымсыз желілер бойынша жіберілетін деректердің құпиялылығы мен бүтіндігін қорғау және оған байланысты жүйелер мен мәлімдемелерді қорғау үшін арнаулы басқару құралдары белгіленуі тиіс (10 және 13.2 тармақтарын қараңыз); сонымен қатар, желі қызметтері мен оған байланысты компьютерлердің қолжетімділігін сүйемелдеу үшін арнаулы басқару құралдары талап етіле алады;

d) ақпараттық қауіпсіздікке қатысты әрекеттерді жазып алу және анықтау үшін тиісті тіркеу және бақылау қолданылуы тиіс;

e) ұйымға қызмет көрсетуді оңтайландыру үшін және басқару құралдары ақпаратты өңдеу инфрақұрылымы арқылы жүйелі түрде қолданылатынын қамтамасыз ету үшін басқару әрекеттері үйлестірілуі тиіс;

f) желідегі жүйелер расталуы тиіс;

g) жүйелердің желімен байланысы шектеулі болуға тиіс.

Басқа ақпарат

Желі қауіпсіздігі туралы қосымша ақпарат [15], [16], [17], [18], [19].

13.1.2 Желі қызметтерінің қауіпсіздігі

Басқару шаралары

Барлық желі қызметтерінің қауіпсіздік механизмдері, сервистік қызмет көрсету және басқарушылық талаптары, осы қызметтердің ғимарат ішінде немесе одан тыс көрсетілетіні желі қызметтерінің келісімдерінде белгіленіп, қамтылады.

Іске асыру жөніндегі нұсқау

Желі қызметін жеткізушінің келісілген қызметтерді қауіпсіз тәсілмен басқару қабілеттілігі белгіленіп, жүйелі түрде тексерілуі тиіс, ал тексеру құқығы келісілген болуы тиіс.

Қауіпсіздік механизмдері, сервистік қызмет көрсету және басқарушылық талаптар сияқты ерекше қызметтер үшін қажетті қауіпсіздік шаралары белгіленуі тиіс. Ұйым желі қызметтерін жеткізушілердің осы шараларды жүзеге асыруын қамтамасыз етуі тиіс.

Басқа ақпарат

Желі қызметтері желіні, жеке желі қызметтерін ұсынуды қамтиды және қосылған желілерді және брандмауэр және араласуды анықтау жүйелері сияқты желі қаупісіздігіне арналған шешімдерді бағалайды. Осы қызметтер қарапайым басқарылмайтын өткізу желісінен бастап қосылған құнды күрделі ұсыныстарға дейін қамтиды.

Желі қызметтерінің қауіпсіздік механизмдері:

a) сәйкестендіру, шифрлау және байланысты желілік басқару құралдары сияқты желі қызметтерінің қауіпсіздігі үшін қолданылатын технологиялар;

b) қауіпсіздік пен желілік байланыс ережелеріне сәйкес желі қызметтерімен қамтамасыз етілген байланыс үшін талап етілетін техникалық параметрлер;

c) қажетті болған жағдайда, желі қызметтері немесе мәлімдемелерге қолжетімділікті шектеу үшін желі қызметін пайдалану процедуралары.

13.1.3 Желідегі бөліну

Басқару шаралары

Ақпараттық қызметтер, тұтынушылар мен ақпаратты жүйелер топтары желіде бөлек болулары тиіс.

Іске асыру жөніндегі нұсқау

Ірі желілердің қауіпсіздігін басқарудың бір әдісі оларды бөлек желі аумақтарына бөлуге тиіс. Сенімділік деңгейлеріне негізделген аумақтар (мысалы, ашық қолжетімділік аумағы, үстел аумағы, сервер аумағы), ұйым бірліктерінің бойындағы аумақтар (мысалы, адам ресурстары, қаржы, маркетинг) немесе кейбір тіркестер (мысалы, көптеген ұйым

бірліктерімен байланысатын сервер аумағы) таңдалуы мүмкін. Бөліну, сонымен қатар, физикалық түрлі желілерді пайдалану арқылы немесе түрлі логикалық желілер арқылы (мысалы, жеке виртуалдық желі) жүзеге асырылуы мүмкін.

Әр аумақ периметрі анық белгіленуі тиіс. Желі аумақтары арасында қолжетімділікке рұқсат беруге болады, бірақ желі аралық интерфейсті қолданып (мысалы, брандмауэр, маршрутизатор), периметрде оны басқару қажет. Желілердің домендерге бөліну критерийлері әр аумақтың қауіпсіздік талаптарын бағалауға негізделуі тиіс. Бағалау қолжетімділікті басқару саясатына (9.1.1 қараңыз), қолжетімділік талаптарына, өңделген ақпараттың құны мен жіктелуіне сәйкес болып, жарамды желі аралық ауысудың салыстырмалы бағасы мен бірігу әсерін есепке алуы тиіс.

Сымсыз желілер нашар анықталған желі периметріне байланысты арнаулы режимді талап етеді. Сезгіш қоршаған орта үшін сыртқы желілер сияқты барлық сымсыз қолжетімділікті қарастыру қажет, қолжетімділікті ішкі жүйелер үшін бергенге дейін басқару құралдарының желілік саясатына (13.1.1 қараңыз) сәйкес желі аралық интерфейс арқылы өткенге дейін оны ішкі желілерден бөлу қажет.

Сымсыз желі стандарттарына негізделген, заманауи деңгейіндегі сәйкестендіру, шифрлау және желінің қолжетімділігін басқарудың тұтынушылық технологиялары ұйымның ішкі желісімен тікелей байланысу үшін жеткілікті болуы мүмкін.

Басқа ақпарат

Желілер жиі ұйым шектерінен тыс жайылады, себебі іскерлік әріптестіктер өңдейтін және желі құралдарының байланысын немесе ақпарат алмасуын талап етеді. Осындай кеңейтулер желіні пайдаланатын ұйымның ақпараттық жүйелеріне рұқсат етілмеген қолжетімділік қаупін ұлғайта алады, олардың кейбірі сезгіштігі немесе маңыздылығына байланысты басқа желі тұтынушыларынан қорғалуды талап етеді.

13.2 Ақпаратты жіберу

Мақсаты: ұйым ішінде және кез келген сыртқы кәсіпорынға жіберілетін ақпараттың қауіпсіздігін сүйемелдеу.

13.2.1 Ақпаратты жіберу саясаты және процедуралар

Басқару шаралары

Ресми жіберу саясаты, процедуралар мен басқару құралдары ақпаратты коммуникация құралдарының барлық типтері арқылы жіберуді қорғау үшін бар болуға тиіс.

Іске асыру жөніндегі нұсқау

Ақпаратты жіберуге арналған коммуникация құралдарын пайдаланып жүзеге асырылатын процедуралар мен басқару құралдары келесі тармақтарды қарастыруы қажет:

a) жіберілген ақпаратты ұстап қалудан, көшіруден, түрлендіруден, дұрыс емес бағыттаудан және бұзудан қорғау үшін әзірленген процедуралар;

b) электрондық байланыс құралдары арқылы жіберілуі мүмкін зиянды бағдарламалық жасақтаманы анықтау және қорғау процедуралары (12.2.1 қараңыз);

c) қосымша түрінде орналасқан, жіберілген сезгіш электрондық ақпаратты қорғау процедуралары;

d) коммуникация құралдарын тиісті қолданысын жалпы сипаттайтын саясат немесе ұсыныстар (8.1.3 қараңыз);

e) персонал, үшінші тарап пен кез келген басқа тұтынушы міндеттерінің ұйымға қауіп төндірмеуі, мысалы, жала тағу, құғынға ұшырау, спам жіберу, рұқсат етілмеген сатып алулар және т.б.;

f) шифрлау әдістерін пайдалану, мысалы, ақпараттың құпиялылығын, бүтіндігін және шынайылығын қорғау (10-тарауды қараңыз);

g) тиісті ұлттық және жергілікті заңнама мен нұсқауларға сәйкес барлық іскерлік хат алысу үшін ұсыныстар, соның ішінде, хабарландырулар;

h) коммуникация құралдарын пайдалануға байланысты басқару құралдары мен шектеулер, мысалы, электрондық поштаны сыртқы пошта мекенжайларына автоматтық түрде жіберу;

i) персоналға құпия ақпаратты көрсетпеу үшін тиісті сақтандыру шараларын қолдану;

j) автоматты түрде жауап қайтарғыш туралы құпия ақпаратты қамтитын хабарландыруларды жібермеу, себебі, коммуналдық жүйелерде немесе мекенжайды дұрыс емес теру нәтижесінде сақталатын хабарландыруларды бөгде адамдар қайталай алады;

k) персоналға фототелеграф аппараттарын немесе қызметтерін пайдалану мәселелері туралы хабарлау, соның ішінде:

1) хабарландыруларды қалпына келтіру үшін хабарландырулардың кіріктірілген мұрағаттарына рұқсат етілмеген қолжетімділік;

2) хабарландыруларды белгілі күнде жіберу үшін машиналарды қасақана немесе абайсыз бағдарламалау;

3) құжаттар мен хабарландыруларды дұрыс емес жіберу.

Сонымен қатар, персоналға қоғамдық жерлерде немесе қауіпті байланыс желілері бойынша, ашық офистерде және жиналысқа арналған жерлерде құпия әңгімелер жүргізбеуге айтқан жөн.

Ақпаратты жіберу қызметтері кез келген тиісті заңды талаптарды орындауға тиіс (18.1 қараңыз).

Басқа ақпарат

Ақпаратты жіберу электрондық пошта, дауыстық хабарлама, факсимиле және видео хабарламаны қоса алғандағы коммуникация құралдарының көптеген түрлі типтері арқылы жүзеге асырылуы мүмкін.

Бағдарламалық жасақтаманы жіберу Интернеттен жүктеу және стандартты өнімдерді сататын сатушылардан сатып алуды қоса алғандағы түрлі орталар арқылы жүзеге асырылуы мүмкін.

13.2.2 Ақпаратты жіберу жөніндегі келісімдер

Басқару шаралары

Келісімдер бизнес-ақпаратты ұйым мен үшінші тарап арасында қауіпсіз жіберуді қамтуы тиіс.

Іске асыру жөніндегі нұсқау

Ақпаратты жіберу туралы келісімдер келесілерді қамтуы тиіс:

a) жіберу және алу туралы хабарлау және оларды басқару бойынша басқару функциялары;

b) қадағалануды және міндеттерден бас тартпауды қамтамасыз ететін процедуралар;

c) буып-түю және жіберуге арналған минимал техникалық стандарттар;

d) шартты депозиттеу туралы келісімдер;

e) курьердің сәйкестендіру стандарттары;

f) деректерді жоғалту сияқты ақпараттық қауіпсіздік инциденттері жағдайындағы міндеттер мен міндеттемелер;

g) затбелгілер дереу түсінікті болатынын және ақпарат тиісінше қорғалуын қамтамасыз ететін сезгіш немесе маңызды ақпарат үшін келісілген маркалау жүйесін пайдалану (8.2 қараңыз);

h) ақпарат пен бағдарламалық жасақтаманы жазу және оқуға арналған техникалық стандарттар;

i) сезгіш тармақтарды қорғау үшін талап етілетін кез келген арнаулы басқару құралдары, мысалы, криптография (10-тарауды қараңыз);

j) жолдағы ақпаратты алу үшін тұжырымдама тізбегін сүйемелдеу;

k) қолжетімділікті басқарудың рұқсат етілген деңгейлері.

Саясат, процедуралар мен стандарттар ақпарат пен нақты ортаны жолда қорғайтындай белгіленіп, сақталуы тиіс (8.3.3 қараңыз).

Кез келген келісімнің ақпараттық қауіпсіздік мазмұны қамтылған бизнес-ақпараттың сезгіштігін белгілеуі тиіс.

Басқа ақпарат

Келісімдер электрондық немесе қолма-қол бола алады және ресми келісімшарт түрінде болуы мүмкін. Құпия ақпарат үшін осындай ақпаратты жіберу үшін қолданылатын белгілі механизмдер барлық ұйымдар мен келісім типтері үшін жүйелі болуы тиіс.

13.2.3 Хабарламаларды электрондық жіберу

Басқару шаралары

Хабарламаларды электрондық жіберуде қамтылған ақпарат тиісінше қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Хабарламаларды электрондық жіберуге арналған ақпараттық қауіпсіздік:

a) ұйымда қабылданған жіктеу жүйесімен шамалас хабарламаларды рұқсат етілмеген қолжетімділіктен, түрлендіруден немесе қызмет көрсетуге бас тартудан қорғау;

b) хабарламаны дұрыс пайдалану және тасымалдауды қамтамасыз ету;

c) қызмет етудің сенімділігі мен қолжетімділігі;

d) заңды талаптар, мысалы, электрондық қолдарға қойылатын талаптар;

e) дереу хат алмасу, әлеуметтік желі немесе файлдарды бірге пайдалану сияқты сыртқы әлеуметтік қызметтерді пайдалануды мақұлдау;

f) жалпыға қолжетімді желілерден сәйкестендіруді басқарудың күшті қолжетімділік деңгейлері.

Басқа ақпарат

Іскерлік байланыста маңызды болып табылатын хабарламаларды электрондық жіберудің көптеген түрлері бар, мысалы, электрондық пошта, электрондық деректер алмасу және әлеуметтік желі.

13.2.4 Құпиялылық немесе жарияламау туралы келісімдер

Басқару шаралары

Ұйымның ақпаратты қорғау қажеттілігін белгілейтін құпиялылық талаптары немесе жарияламау туралы келісімдер белгіленіп, жүйелі түрде қарастырылуы және құжатталуы тиіс.

Іске асыру жөніндегі нұсқау

Құпиялылық немесе жарияламау туралы келісімдер заңды терминдерді қолданатын құпия ақпаратты қорғауға арналған талапты қанағаттандыруы тиіс. Құпиялылық немесе жарияламау туралы келісімдер үшінші тараптар немесе ұйым қызметкерлеріне қолданыла алады. Элементтер басқа тарап типін, оның рұқсат етілген қолжетімділігін немесе құпия ақпаратты өңдеу деңгейін есепке алып таңдалады немесе енгізіледі. Құпиялылық немесе жарияламау туралы келісімдер талаптарын белгілеу үшін келесі элементтерді қарастыру қажет:

a) қорғалатын ақпаратты белгілеу (мысалы, құпия ақпарат);

b) келісімнің болжалды әрекет ету мерзімі, соның ішінде, ақпарат құпия болып қалатын жағдайлар;

c) келісім бұзылған кездегі қажетті әрекеттер;

d) рұқсат етілмеген ақпаратты ашуды болдыртпау үшін қол қойғандардың міндеттері мен әрекеттері;

e) ақпарат, коммерциялық құпия мен зияткерлік меншік және олардың құпия ақпаратты қорғауға қатысы;

f) құпия ақпаратты рұқсат етілген қолдану және қол қойғандардың ақпаратты пайдалану құқықтары;

g) құпия ақпаратты қамтитын әрекеттерді тексеру және бақылау құқығы;

h) құпия ақпаратты рұқсат етілмеген ашу немесе оның жайылуы туралы хабарлау процесі;

i) келісім мерзімі өткенде қайтарылатын немесе бұзылатын ақпаратты алу шарттары;

j) келісімді бұзған кездегі болжалды әрекеттер.

Ұйымның ақпараттық қауіпсіздік талаптарына негізделген басқа элементтер құпиялылық немесе жарияламау туралы келісімдер үшін қажет бола алады.

Құпиялылық немесе жарияламау туралы келісімдер барлық әрекеттегі заңдар және олар қолданылатын құзырет нұсқаулықтарына сәйкес болулары тиіс (18.1 қараңыз).

Құпиялылық немесе жарияламау туралы келісімдер талаптары кезеңдік түрде және осы талаптарға әсер ететін өзгерістер енгізілген кезде қарастырылады.

Басқа ақпарат

Құпиялылық немесе жарияламау туралы келісімдер ұйым ақпаратын қорғайды және қол қойғандарға ақпаратты жауапты және рұқсат етілген тәсіл арқылы қорғау, пайдалану және ашу міндеттері туралы хабарлайды.

Ұйымда түрлі жағдайларда құпиялылық немесе жарияламау туралы келісімдердің түрлі типтерін пайдалану қажеттілігі туындауы мүмкін.

14 Жүйелік сатып алулар, даму және қызмет көрсету

14.1 Ақпараттық жүйелердің қауіпсіздік талаптары

Мақсаты: ақпараттық қауіпсіздіктің ақпараттық жүйелерді пайдаланудың барлық кезеңі ішінде ажырамас бөлігі болатынына кепіл беру. Бұл, сонымен қатар, жалпыға қолжетімді желілер бойынша қызметтер көрсететін ақпараттық жүйелер үшін талаптарды қамтиды.

14.1.1 Ақпараттық қауіпсіздік талаптарын талдау және спецификация

Басқару шаралары

Ақпараттық қауіпсіздікке қатысты талаптар жаңа ақпараттық жүйелер үшін талаптарда және бар ақпараттық жүйелерді жақсартуда қамтылуы тиіс.

Іске асыру жөніндегі нұсқау

Ақпараттық қауіпсіздік талаптары саясат пен нұсқаулықтарды сақтау талаптары, қауіпті үлгілеу, инциденттерге шолу жасау немесе осалдық шектерін пайдалану сияқты түрлі әдістерді пайдалану арқылы белгіленуі тиіс. Сәйкестендіру нәтижелері тіркеліп, оларды барлық мүдделі тараптар қарастыруы қажет.

Ақпараттық қауіпсіздік талаптары мен басқару құралдары қамтылған ақпараттың іскерлік құндылығы (8.2 қараңыз) мен тиісті қауіпсіздік болмаған жағдайда пайда болуы мүмкін болжалды теріс іскерлік әсерді көрсетеді.

Ақпараттық қауіпсіздік талаптары мен оларға байланысты процестерді сәйкестендіру және басқару ақпараттық жүйелер жобаларының ерте сатыларында бірігуі тиіс. Ақпараттық қауіпсіздік талаптарын ерте қарастыру, мысалы, жобалау сатысында, тиімдірек және ұтымдырақ шешімдерге әкеледі.

Ақпараттық қауіпсіздік талаптары, сондай-ақ, келесілерді қарастырады:

a) сәйкестендірудің тұтынушы талаптарын алу үшін талап етілетін тұтынушы тұлғасы үшін қажетті сенімділік деңгейі;

b) іскер тұтынушылар, артықшылықты немесе техникалық тұтынушылар үшін қамтамасыз етуші қолжетімділік пен рұқсат беру процестері;

c) тұтынушылар мен операторларға олардың міндеттері мен жауапкершілігі туралы хабарлау;

d) қамтылған активтерді қорғау қажеттіліктері, әсіресе, қолжетімділік, құпиялылық, бүтіндікке қатысты;

e) операциялық тіркеу және бақылау, міндеттерден бас тартпау сияқты бизнес-процестерден туындаған талаптар;

f) қауіпсіздікті қамтамасыз етудің басқа шараларымен мандатқа табысталған талаптар, мысалға, тіркеу және бақылау интерфейстері немесе мәліметтердің шығып кетуін анықтау жүйесі.

Жалпыға қолжетімді желілер бойынша қызмет көрсететін немесе мәмілелерді жүзеге асыратын мәлімдемелер үшін 14.1.2 және 14.1.3 арнаулы басқару талаптарын қарастыру қажет.

Егер өнім сатып алынса, ресми сынау және сатып алу процесі тіркелуі тиіс. Жеткізушімен жасалған келісімшарттар белгілі қауіпсіздік талаптарын сақтауға тиіс. Ұсынылған өнімде қауіпсіздік белгіленген талапты қанағаттандырмаған кезде, енгізілген және басқару құралдарына байланысты қауіп өнімді сатып алғанға дейін қарастыралады.

Қорытынды бағдарламалық жасақтамаға/жүйенің қызметтер жинағына сәйкес келетін өнімнің қауіпсіздік конфигурациясы үшін қолжетімді нұсқау бағаланып, жүзеге асырылуы тиіс.

Басқа ақпарат

[11] және [27] ақпараттық қауіпсіздік талаптарына сәйкес келу үшін басқару талаптарын белгілеуге арналған қауіптерді басқару процестерін пайдалану туралы ақпарат береді.

14.1.2 Жалпыға қолжетімді желілерде қосымша сервистерін қамтамасыз ету

Басқару шаралары

Жалпыға қолжетімді желілер бойынша жіберілетін, қосымшалар сервистерінде қамтылған ақпарат айлакерлік қызметтен, келісімшарт дауларынан және рұқсат етілмеген ашу мен түрлендіруден қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Жалпыға қолжетімді желілер бойынша жіберілетін қосымшалар сервистері үшін ақпараттық қауіпсіздік талаптары:

a) әр тарап бір-бірін сәйкестендіру үшін талап ететін сенімділік деңгейі, мысалы, сәйкестендіру арқылы;

b) түйінді транзакциялық құжаттар мазмұнын кім мақұлдай алатынына, оларды кім жариялай алатынына немесе оларға кім қол қоя алатынына байланысты рұқсат беру процестері;

c) әріптестердің қызметтерді ұсыну немесе пайдалану бойынша рұқсаттары туралы хабардар болуын қамтамасыз ету;

d) түйінді құжаттардың құпиялылығы, бүтіндігі, шынайылығына арналған сәйкестік талаптары мен келісімшарттардан бас тартпау, мысалы, ұсыныс және процестерге байланысты келісімшарт;

e) түйінді құжаттардың бүтіндігінде сенімділік деңгейі;

f) кез келген құпия ақпаратты қорғау талаптары;

g) кез келген тапсырыс мәмілелері, төлем ақпараты, жеткізу мекенжайы мен түбіртекті растаудың құпиялылығы мен бүтіндігі;

h) клиент ұсынған төлем ақпаратын тексеруге сәйкес келетін тексеріс дәрежесі;

i) айлакерлікке қарсы шаралар қолдану үшін тиісті төлем формасын таңдау;

j) тапсырыс ақпаратының құпиялылығы мен бүтіндігін сақтауға арналған қорғау деңгейі;

k) мәміле туралы ақпаратты жоғалту немесе көшіруді болдыртпау;

l) кез келген мәмілелерге байланысты жауапкершілік;

m) сақтандыру талаптары.

Көптеген жоғарыда аталған талаптар заңды талаптарға сәйкестігін (18-тарау, соның ішінде, криптография үшін 18.1.5 қараңыз) есепке ала отырып, шифрлау басқару құралдарын (10-тарауды қараңыз) қолдану арқылы шешіле алады.

Басқа ақпарат

Жалпыға қолжетімді желілер арқылы қолжетімді мәлімдемелер айлакерлік әрекеттер, келісімшарт даулары немесе ақпаратты жаю сияқты желі қауіптеріне ұшырайды. Сондықтан, қауіп дәрежесін толық бағалау және басқару құралдарын тиісінше таңдау міндетті болып табылады. Басқару құралдары сәйкестендіру және қамтамасыз ету деректерін жіберуге арналған шифрлау әдістерін қамтиды.

Қосымшалар сервистері қауіпсіз сәйкестендіру әдістерін қолдана алады, мысалы, ашық кілт криптографиясы және сандық қолдар (10-тарауды қараңыз). Сонымен қатар, осындай қызметтер қажет болған жерде сенімді үшінші тараптар қолданыла алады.

14.1.3 Қосымша сервистерінің мәмілелерін қорғау

Басқару шаралары

Хабарламаны толық емес жіберу, дұрыс емес бағыттау, рұқсат етілмеген өзгерту, рұқсат етілмеген көшіру және қайта қарауды болдыртпау үшін қосымша сервистерінің мәмілелерінде қамтылған ақпарат қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Қосымша сервистерінің мәмілелеріне арналған ақпараттық қауіпсіздік талаптары:

a) мәмілеге қатысатын әр тараптың электрондық қолын пайдалану;

b) мәміленің барлық аспектілері:

1) барлық тараптардың тұтынушыны сәйкестендіру туралы құпия ақпараты шын және тексерілген;

2) мәміле құпия болып қалады;

3) барлық қатысушы тараптарға байланысты жеке деректер сақталған;

c) барлық қатысушы тараптар арасында коммуникациялық жол шифрланған;

d) барлық қатысушы тараптар арасында байланысу үшін қолданылатын хаттамалар қамтамасыз етілген;

e) транзакция егжей-тегжейлерін сақтау кез келген жалпыға қолжетімді ортадан тыс, мысалы, ұйымдастырушылық интранеттегі сақтау платформасы, орналасқанын және интернеттен тікелей қолжетімді деректер тасымалдаушыларында сақталмағанын қамтамасыз ету;

f) сенімді басшылық қолданылаты жерде (мысалы, сандық қолдар немесе сандық куәліктерді сүйемелдеу мақсатында), қауіпсіздік біріктіріліп, куәліктерді/қолдарды басқарудың барлық үздіксіз процесі барысында қамтамасыз етіледі.

Басқа ақпарат

Басқару құралдарының қауіпсіздік дәрежесі әр қатысушы сервис мәмілесіне байланысты қауіп деңгейіне шамалар болуға тиіс.

Мәмілелер жасалған, аяқталған немесе сақталған құзыреттегі заңды және нормативтік талаптарды орындауға тиіс.

14.2 Даму және сүйемелдеу процестеріндегі қауіпсіздік

Мақсаты: ақпараттық қауіпсіздіктің ақпараттық жүйелердің өміршең циклінің шегінде әзірленуін және жүзеге асырылуын қамтамасыз ету.

14.2.1 Қауіпсіз даму стратегиясы

Басқару шаралары

Бағдарламалық жасақтама мен жүйелерді дамыту ережелері белгіленіп, ұйымдағы оқиғаларға қатысты болуы тиіс.

Іске асыру жөніндегі нұсқау

Қауіпсіз даму қауіпсіз қызмет көрсету, архитектура, бағдарламалық жасақтама мен жүйені құруға арналған талап болып табылады.

Қауіпсіз даму стратегиясының шеңберінде келесі аспектілерді қарастырады:

a) жобалау ортасының қауіпсіздігі;

b) бағдарламалық жасақтаманы әзірлеудің өміршең циклінде қауіпсіздік нұсқаулары:

1) бағдарламалық жасақтаманы әзірлеу әдіснамасындағы қауіпсіздік;

2) әр бағдарламалау тілі үшін қауіпсіз кодтау ұсынымдарын пайдалану;

c) жобалау сатысындағы қауіпсіздік талаптары;

d) жоба сатыларында бақылау-өткізу қауіпсіздік тармақтары;

e) қауіпсіз сақтау орындары;

f) нұсқаларды бақылаудағы қауіпсіздік;

g) қажетті қолданбалы қауіпсіздік білімі;

h) әзірлеушілердің осал жерлерді болдыртпау, табу және бекіту қабілеттілігі.

Қауіпсіз бағдарламалық әдістер жаңа әзірлемелер үшін де, қайта қолданылатын кодтау сценарийлерінде де қолданылуға тиіс. Қауіпсіз кодтау стандарттарын қарастырып, олардың пайдалануға өзектілігін қарастыру қажет.

Әзірлеушілер оларды пайдалануға және сынауға оқытылып, олардың қолданысын кодтау шолуы тексереді.

Егер дамыту сыртта өндірілсе, ұйым үшінші тараптың қауіпсіз дамуға арналған осы ережелерді орындайтынына кепіл алуға тиіс (14.2.7 қараңыз).

Басқа ақпарат

Даму офистік қосымшалар, кодтарды жазу, браузерлер мен деректер базалары сияқты қосымшаларда орын алуы мүмкін.

14.2.2 Өзгерістерді жүйелік бақылау процедуралары

Басқару шаралары

Дамудың өміршең цикл шеңберінде жүйе өзгерістерін өзгерістерді ресми бақылау процедуралары арқылы басқару қажет.

Іске асыру жөніндегі нұсқау

Ерте жобалау сатыларынан кейінгі қызмет ету сатыларына дейін жүйе, қосымшалар мен өнімдердің бүтіндігіне кепіл беру үшін өзгерістерді ресми бақылау процедуралары тіркеліп, жүзеге асырылуы тиіс.

Жаңа жүйелерді және бар жүйелерге елеулі өзгерістерді енгізу ресми құжаттау, спецификация, сынау, сапаны бақылау және басқарылатын енгізу процестерінен кейін өткізу қажет.

Осы процесс қауіп дәрежесін бағалау, өзгерістер әсерін талдау және қауіпсіздікті қамтамасыз етудің қажетті шараларының спецификацияларын қамтуы тиіс. Осы процесс бар қауіпсіздік пен бақылау процедураларына қауіп төнбейтінін және сүйемелдеу бағдарламалаушыларына олардың жұмысына қажетті бөліктерге ғана қолжетімділік берілетінін және кез келген өзгеріс ресми келісілгенін және мақұлданғанын қамтамасыз етуі тиіс.

Барлық іске асатын жерлерде өзгерістерді пайдалану және эксплуатациялық бақылау процедуралары біріктірілуі тиіс (12.1.2 қараңыз). Өзгерістерді бақылау процедуралары:

a) келісілген рұқсат беру деңгейлерінің есебін сүйемелдеу;

b) кепіл беруші өзгерістерді тіркелген тұтынушылардың ұсынуы;

c) өзгерістер басқару және бүтіндік процедураларының деңгейін түсірмейтінін қамтамасыз ету үшін оларды қарастыру;

d) түзетуді талап ететін барлық бағдарламалық жасақтаманы, ақпаратты, деректер базасын және аппаратуралық құралдарды белгілеу;

e) қауіпсіздіктің белгілі осал жерлерінің ықтималдығын азайту үшін маңызды кодекс қауіпсіздігін сәйкестендіру және тексеру;

f) жұмыс алдында толық ұсыныстар үшін ресми мақұлдау алу;

g) кепіл беруші тіркелген тұтынушылар өзгерістерді енгізгенге дейін қабылдайды;

h) әр өзгеріс аяқталған кезде жүйелік құжат жинағы жаңартылуын және ескі құжаттарды мұрағаттайтынын немесе жоятынын қамтамасыз ету;

i) бағдарламалық жасақтаманың барлық жаңартулары үшін нұсқаларды бақылау;

j) өзгерістерге барлық сұраулар бақылау журналын жүргізу;

k) операциялық құжаттама (12.1.1 қараңыз) мен тұтынушылық процедуралардың тиісті болып қалу үшін қажеттілігіне орай өзгертілгенін қамтамасыз ету;

l) өзгерістерді енгізу уақтылы болуын және қамтылған бизнес-процестерді бұзбайтынын қамтамасыз ету.

Басқа ақпарат

Өзгертілетін бағдарламалық жасақтама жұмыс ортасына және керісінше әсер ете алады.

Жақсы тәжірибе өндіріс пен жобалау ортасынан (12.1.4 қараңыз) бөлек қоршаған ортада жаңа бағдарламалық жасақтаманы сынауды қамтиды. Бұл жаңа бағдарламалық жасақтаманы басқару құралын және мақсаттын сынау үшін қолданылатын эксплуатациялық ақпаратты қосымша қорғауды қамтамасыз етеді. Бұл аумақтар, жаңарту пакеттері мен басқа жаңартуларды қамтуы тиіс.

Автоматтық түрде жаңару қарастырылатын жерде, жүйенің бүтіндігі пен қолжетімділігі қаупі жаңартуларды тез пайдалану тиімділігіне қарсы қарастырылады. Автоматтандырылған жаңартулар маңызды жүйелерде қолданылмайды, себебі кейбір жаңартулар маңызды қосымшаларды істен шығарады.

14.2.3 Мәмілелерге техникалық шолу операциялық платформадан кейін өзгереді

Басқару шаралары

Операциялық платформалар өзгертілген кезде, маңызды іскерлік мәлімдемелер ұйым операциялары немесе қауіпсіздікке жағымсыз әсердің болмауын қамтамасыз ету үшін қарастырылуы және тексерілуі тиіс.

Іске асыру жөніндегі нұсқау

Осы процесс қамтиды:

a) платформаның операциялық өзгерістері қолданбалы бақылау және бүтіндік процедураларының деңгейін түсірмейтінін қамтамасыз ету үшін оларға шолу жасау;

b) енгізу алдында тиісті сынақтар мен шолулар болуына мүмкіндік беру үшін платформаның операциялық өзгерістері туралы хабардың уақытында ұсынылуын қамтамасыз ету;

c) тиісті өзгерістерді бизнес үздіксіздігін қамтамасыз ету жоспарларына енгізу (17-тарауды қараңыз).

Басқа ақпарат

Операциялық платформалар операциялық жүйелер, деректер базасы мен аралық бағдарламалық жасақтама платформаларын қамтиды. Бақылау, сондай-ақ, мәлімдемелерді өзгертуге қолданылуы тиіс.

14.2.4 Бағдарлама пакеттерін өзгертуді шектеу

Басқару шаралары

Бағдарлама пакеттерін түрлендіруді болдыртпай, қажетті өзгерістермен шектеу қажет және барлық өзгерістерді қатал түрде басқару қажет.

Іске асыру жөніндегі нұсқау

Сатушылар жеткізген бағдарлама пакеттері мүмкіндігіне орай түрленусіз қолданылуы тиіс. Бағдарлама пакеті өзгертілуге тиісті болған кезде, келесі талаптарды қарастыру қажет:

a) кіріктірілген және бүтіндік процестеріне қауіп төндіретін басқару құралдары қаупі;

b) сатып алушының растауын алу қажеттілігі;

c) сатушыдан стандартты бағдарлама жаңарту ретінде қажетті өзгертулерді алу мүмкіндігі;

d) ұйым өзгерістер нәтижесінде бағдарламалық жасақтамаға келешек қызмет көрсетуге жауапты болған жағдайдағы әсер;

e) қолданыста басқа бағдарламалық жасақтамамен үйлесуі.

Егер өзгерістер қажет болса, түпнұсқалық бағдарламалық жасақтама сақталып, өзгертулер белгіленетін көшірмеге қатысты болады. Бағдарламалық жасақтама жаңартуының басқарушылық процесі ең өзекті мақұлданған аумақтардына кепіл беру үшін жүзеге асырылады, ал қолданбалы жаңартулар барлық рұқсат етілген бағдарламалық жасақтама үшін орнатылады (12.6.1 қараңыз). Барлық өзгерістер бағдарламалық жасақтаманың келешек түрленулеріне қайта қолданылуын қамтамасыз ету үшін толығымен тексерілуі және тіркелуі тиіс. Қажеттілігіне орай, түрленулерді тәуелсіз бағалау тұлғасы тексеріп, бекітуі тиіс.

14.2.5 Қауіпсіз әзірлеу жүйелік принциптері

Басқару шаралары

Техникалық қауіпсіз жүйелерге арналған принциптер белгіленіп, құжатталып, сақталып, ақпараттық жүйені енгізуге қатысты болуы тиіс.

Іске асыру жөніндегі нұсқау

Қауіпсіздікті әзірлеу принциптеріне негізделген ақпараттық жүйе әзірлемесінің қауіпсіз тәртіптері белгіленіп, құжатталып, ақпараттық жүйені әзірлеудің ішкі әрекеттеріне қатысты болуы тиіс. Қауіпсіздік ақпараттық қауіпсіздік қажеттілігін қолжетімділік қажеттілігімен шамалас қылып, барлық архитектура қабаттары үшін (бизнес, деректер, қосымшалар мен технология) әзірленуі тиіс. Жаңа технология қауіпсіздік қауіптеріне талданып, ал дизайн белгілі шабуыл үлгілеріне қарсы қарастырылуы тиіс.

Осы принциптер мен белгіленген техникалық тәртіптер әзірлеу процесінің шеңберінде кеңейтілген қауіпсіздік стандарттарына тиімді көмектесетініне кепіл беру үшін жүйелі түрде қарастырылуы тиіс. Олар, сонымен қатар, кез келген жаңа потенциалды қауіптермен күресуге қатысты және технологиялардағы жетістіктерге қатысты өзекті болуын қамтамасыз ету үшін жүйелі түрде қарастырылуы тиіс.

Белгіленген әзірлеме қауіпсіздігі принциптері қолданысына орай шетте өндірілген ақпараттық жүйелерге ұйым мен жеткізуші арасындағы келісімшарттар мен басқа келісімдер арқылы қолданылуы тиіс. Ұйым жеткізушілердің инженерлік қауіпсіздік принциптерінің қаталдығы ұйым принциптеріне сайма-сай екендігін растауға тиіс.

Басқа ақпарат

Қосымшаларды әзірлеу процедуралары кіру және шығу интерфейстері бар қосымшаларды дамытуда қауіпсіз техниканы қолдануы тиіс. Қауіпсіз техника тұтынушылық сәйкестендірі әдістері туралы түсінік беріп, сессияны бақылайды және деректер дұрыстығын растайды.

14.2.6 Қауіпсіз жобалау ортасы

Басқару шаралары

Ұйым барлық пайдалану кезеңінде жүйелік даму мен интеграция талпыныстарын жобалаудың қауіпсіз орталарын белгілеуі және тиісінше қорғауы тиіс.

Іске асыру жөніндегі нұсқау

Қауіпсіз жобалау ортасы жүйелік даму мен интеграцияға байланысты адамдар, процестер мен технологияны қамтиды.

Ұйым бөлек даму талпыныстарына байланысты қауіптерді бағалап, келесілерді қарастыру арқылы жүйелік даму әрекеттері үшін қауіпсіз жобалау орталарын белгілеуі тиіс:

a) жүйе өңдейтін, сақтайтын және жіберетін деректер сезгіштігі;

b) қолданылатын сыртқы және ішкі талаптар, мысалы, нұсқаулықтар немесе саясат;

c) ұйым жүйені дамыту үшін жүзеге асырған қауіпсіздікті қамтамасыз ету шаралары;

d) қоршаған ортада жұмыс істейтін персоналдың кредит қабелеттілігі (7.1.1 қараңыз);

e) жүйелік дамуға байланысты аутсорсинг дәрежесі;

f) түрлі жобалау орталары арасына бөліну қажеттілігі;

g) жобалау ортасына қолжетімділікті бақылау;

h) қоршаған орта мен сақталған кодекстің өзгерісін бақылау;

i) резервтік көшірмелерді қауіпсіз қашық жерлерде сақтау;

j) деректердің қоршаған ортадан және қоршаған ортаға дейін жылжуын бақылау.

Қорғау деңгейі белгілі жобалау ортасы үшін анықталған кезде, ұйымдар тиісті процестерді қауіпсіз дамыту процедураларында тіркеп, оларды қажет болған барлық адамдарға ұсынуға тиіс.

14.2.7 Шетте өндірілген даму

Басқару шаралары

Ұйым шетте өндірілген жүйелік даму қызметін бақылауға тиіс.

Іске асыру жөніндегі нұсқау

Жүйелік даму шетте өндірілген кезде, ұйымның сыртқы жеткізілім жүйесі арқылы келесілерді қарастыру қажет:

a) шетте өндірілген дамуға байланысты шараларды, кодтық меншік пен зияткерлік меншік құқықтарын лицензиялау (18.1.2 қараңыз);

b) қауіпсіз дизайн, кодтау және әдістерді тексеру үшін шарт талаптары (14.2.1 қараңыз);

c) сыртқы әзірлеушіге мақұлданған қауіп үлгісін ұсыну;

d) соңғы нәтижені сапа мен дәлдікке сынау;

e) қауіпсіздік пен жеке деректердің минимал жол берілетін сапа деңгейлерін белгілеу үшін қауіпсіздік шектерінің қолданылу айғақтарын ұсыну;

f) жеткізілімнің болмауына және қасақана және абайсыз зиянды мазмұнына қарсы шараларды қабылдау үшін жеткілікті сынақтар қолданылғанын дәлелдеу;

g) белгілі осал жерлерге қарсы шаралар қабылдау үшін жеткілікті сынақ қолданылғанын дәлелдеу;

h) шартты депозиттеу шаралары, мысалы, бастапқы код қолжетімсіз болған кезде;

i) даму процестері мен басқару құралдарын шарттық тексеру құқығы;

j) қоршаған ортаны құрудың тиімді құжаттамасы бұрын соңғы нәтижені құрды;

k) ұйым қолданылатын заңдарға және бақылау тиімділігін тексеруге сәйкестігіне жауапты болып қалады.

Басқа ақпарат

Жеткізуші қатынастары туралы қосымша ақпарат [21], [22], [23] берілген.

14.2.8 Жүйе қауіпсіздігін сынау

Басқару шаралары

Қауіпсіздік қызметін сынау дамыту барысында орындалуы тиіс.

Іске асыру жөніндегі нұсқау

Жаңа және жаңартылған жүйелер толық әрекеттер кестесін дайындауды қоса алғандағы дамыту процестері барысында толық сынау және тексеруді талап етеді және

кірулер мен болжалды өнімді тексереді. Ішкі оқиғалар үшін осындай сынақтарды ең алғаш рет әзірлеушілер тобы орындайды. Жүйенің болжалды жұмысын растау үшін тәуелсіз қабылдау сынақтары қабылдануы тиіс (ішкі де, шетте өндірілген де оқиғалар үшін) (14.1.1 және 14.1.9 қараңыз). Сынау дәрежесі жүйенің маңыздылығына сайма-сай болуы тиіс.

14.2.9 Жүйелік қабылдау сынақ

Басқару шаралары

Қабылдау сынақ бағдарламалары мен оған байланысты критерийлер жаңа ақпараттық жүйелер, түрлендірулер мен жаңа нұсқалар үшін белгіленуі тиіс.

Іске асыру жөніндегі нұсқау

Жүйелік қабылдау сынақ ақпараттық қауіпсіздік талаптарын сынауды (14.1.1 және 14.1.2 қараңыз) және жүйелік даму әдістерін (14.2.1 қараңыз) қамтуы тиіс. Сынақ, сонымен қатар, алынған құрауышты және интеграцияланған жүйелерде өткізіледі. Ұйымдар кодтық талдамалық аспаптар немесе осалдық сканерлері сияқты автоматтандырылған аспаптарды күшейте алады және қауіпсіздікті түзету ақауларды байланыстырғанын тексеруі тиіс.

Сынақ жүйенің ұйым ортасына осалдық енгізбейтінін және сынақтар сенімді екендігін қамтамасыз ету үшін іс жүзіндегі жағдайларда орындалуы тиіс.

14.3 Сынақтар деректері

Мақсаты: сынақ үшін қолданылатын деректерді қорғау.

14.3.1 Сынақтар деректерін қорғау

Басқару шаралары

Сынақтар деректерін мұқият іріктеп, қорғау және басқару қажет.

Іске асыру жөніндегі нұсқау

Жеке деректер мен мақсаттарды сынауға арналған кез келген басқа құпия ақпаратты қамтитын жұмыс деректерін пайдаланбаған жөн. Егер жеке деректер немесе басқа құпия ақпарат мақсаттарды сынау үшін қолданылса, барлық сезгіш деректер мен мазмұны өшіру немесе түрлендіру арқылы қорғалуы тиіс ([26] қараңыз).

Мақсаттарды сынау үшін қолданылатын жұмыс деректерін қорғау үшін:

a) эксплуатациялық қолданбалы жүйелерге қатысты қолжетімділікті басқару процедуралары, сондай-ақ, сынақ қолданбалы жүйелерге қолданылуы тиіс;

b) эксплуатациялық ақпарат сынақ шарттарына көшірілген әр кезде, бөлек рұқсат болуы тиіс;

c) сынақ аяқталғаннан кейін эксплуатациялық ақпарат сынақ шарттарынан дереу өшірілуі тиіс;

d) бақылау журналын қамтамасыз ету үшін эксплуатациялық ақпаратты көшіру және пайдалану тіркелуі тиіс.

Басқа ақпарат

Жүйе мен қабылдау-тапсыру сынақтары жұмыс деректеріне максимал жақын сынақ деректерінің елеулі көлемін талап етеді.

15 Жеткізушілермен қатынастар

15.1 Жеткізушілермен қатынастағы ақпараттық қауіпсіздік

Мақсаты: Жеткізушілерге қолжетімді ұйым активтерін қорғау.

15.1.1 Жеткізушілермен қатынастарға арналған ақпараттық қауіпсіздік саясаты

Басқару шаралары

Жеткізушінің ұйым активтеріне қолжетімділігіне байланысты қауіптерді азайтуға арналған ақпараттық қауіпсіздік талаптары жеткізушімен келісіліп, құжатталуы тиіс.

Қолдану жөніндегі нұсқау

Ұйым жеткізушінің ұйым ақпаратына қолжетімділігімен белгілі тәсілмен жұмыс істеу үшін ақпараттық қауіпсіздікті қамтамасыз ету шараларын міндетті ретінде анықтауға және белгілеуге тиіс. Осы қауіпсіздікті қамтамасыз ету шаралары ұйым орындайтын процестер мен процедураларға, сонымен қатар, ұйым жеткізушіден талап ететін процестер мен процедураларға қатысты болады:

a) ұйым өз ақпаратына қолжетімділік беретін ИТ қызметтері, логистика қызметтері, қаржы қызметтері, ИТ инфрақұрылымының құрауыштары сияқты жеткізушілер типін белгілеу және құжаттау;

b) жеткізушілермен қатынастарды басқарудың стандартталған процесі мен кезеңі;

c) жеткізушілердің түрлі типтеріне қолжетімді болатын ақпараттық қолжетімділік типін белгілеу, сондай-ақ, қолжетімділікті бақылау және басқару;

d) іскерлік талаптар мен ұйым талаптарына және оның қауіп профиліне негізделген жеткізушінің жеке келісімдеріне негіз болатын әр ақпарат түрі мен әр қолжетімділік түріне қойылатын минимал ақпараттық қауіпсіздік талаптары;

e) өнімді үшінші тараптың қарауын және тексеруін қоса алғандағы әр жеткізуші типі мен әр қолжетімділік түрі үшін белгіленген ақпараттық қауіпсіздік талаптарының сақталуын бақылау процестері мен процедуралары;

f) үшінші тарап ұсынатын ақпараттың бүтіндігі немесе өңделуін қамтамасыз ету үшін аяқталуды басқару шараларының дәлдігі;

g) жеткізушілерге ұйым ақпаратын қорғау үшін қолданылатын міндеттер түрі;

h) жеткізуші қолжетімділігіне байланысты инциденттер мен күтпеген жағдайлармен жұмыс істеу, соның ішінде, ұйым мен жеткізуші міндеттері;

i) ақпараттың әр тарап үшін қолжетімділігі мен өңделуін қамтамасыз ету үшін жүйенің тұрақтығы мен қалпына келу қабілеттілігі;

j) қолданылатын саясат, процестер мен процедураларға қатысты сатып алуға тартылған ұйым персоналына арналған кіріспе;

k) жеткізуші типі мен жеткізушінің ұйым жүйелері мен ақпаратына қолжетімділік деңгейіне негізделген міндет ережелері мен жұмыс режиміне сәйкес келетін жеткізуші персоналымен әрекеттесетін ұйым персоналына арналған кіріспе;

l) ақпараттық қауіпсіздік талаптары мен қауіпсіздікті қамтамасыз ету шаралары екі тарап та қол қоятын келісімде құжатталатын шарттар;

m) көшірілуге тиіс ақпараттың, ақпаратты өңдеу құралдарының және т.б. қажетті өтуді басқару және барлық көшіру кезеңінде ақпараттық қауіпсіздік сақталатынын қамтамасыз ету.

Қосымша ақпарат

Келісімдер түрлі ұйымдар мен жеткізушілердің түрлі типтері арасында ерекшелене алады. Сондықтан, қолданылатын ақпараттың барлық қауіпсіздік қауіптері мен талаптарын қамтуда мұқият болу қажет. Жеткізушілермен жасалған келісімдер, сондай-ақ, басқа тараптарды да қамтуы мүмкін (мысалы, қосалқы жеткізуші).

15.1.3 Ақпараттық-коммуникациялық технологияларды жеткізу жүйесі

Басқару шаралары

Жеткізушілермен жасалған келісімдер ақпараттық-коммуникациялық технологиялар қызметтеріне және өнімді жеткізу жүйесіне байланысты ақпараттық қауіпсіздік қауіптеріне қойылатын талаптарды қамтуы тиіс.

Қолдану жөніндегі нұсқау

Жеткізушімен жасалатын келісімге жеткізу жүйесінің қауіпсіздігіне қатысты келесі тақырыптарды қарастыру қажет:

a) ақпараттық-коммуникациялық технология өніміне немесе сервистік сатып алуға жеткізушімен қатынастарға арналған жалпы ақпараттың қауіпсіздік талаптарына қосымша ретінде қолдану үшін ақпараттық қауіпсіздік талаптарын белгілеу;

b) егер жеткізушілердің қосалқы келісімшарты телекоммуникациялық технологиялар бойынша ақпарат бөліктері туралы болса, барлық жеткізілім тізбегі бойынша ақпарат қауіпсіздігінің талаптарын таратуды талап ететін ақпаратты және коммуникациялық қызметтер үшін;

c) егер өнімдер басқа жеткізушілерден сатып алынған құрауыштарды қамтыса, жеткізушілердің барлық жеткізілім жүйесі бойынша тиісті қауіпсіздік әдістерді таратуын талап ететін ақпараттық-коммуникациялық технологиялар өнімдері үшін;

d) ақпараттық-коммуникациялық технологиялар өнімдері бекітуге ұсынған бақылау процесі мен жарамды әдістерді жүзеге асыру және қызметтер белгіленген қауіпсіздік талаптарын сақтайды;

e) егер басты жеткізуші өнім немесе сервистік құрауыштарға қатысты аспектілерді басқа жеткізушілер үшін қолданса, ұйым шекарасынан тыс құрылған кезде, функционалдық үшін маңызды өнім немесе сервистік құрауыштарды сәйкестендіру бойынша процесті мұқият жүзеге асыру қажет;

f) маңызды құрауыштар мен олардың пайда болуы барлық жеткізілім жүйесі бойынша қадағалана алатынын қамтамасыз ету;

g) жеткізілген ақпараттық-коммуникациялық технологиялар өнімдері қандай да болмасын күтпеген немесе жағымсыз ерекшеліктерсіз қызмет етуін қамтамасыз ету;

h) жеткізілім жүйесі және ұйым мен жеткізушілер арасындағы кез келген потенциалды мәселелер мен компромистерге қатысты ақпарат алмасу ережелерін белгілеу;

i) ақпараттық-коммуникациялық технологиялар құрауышын пайдаланған кезде белгілі процестер мен қолжетімділікті жүзеге асыру. Осы тармақ жеткізушілер салдарынан қолжетімсіз болған құрауыштар қауіптерін басқаруды қамтиды.

Басқа ақпарат

Ақпараттық-коммуникациялық технологиялар жеткізілім жүйесінің қауіптерін белгілі басқару әдістері жоғары жалпы ақпараттың қауіпсіздік тәжірибелеріне, сапа, жобаны басқару және жүйелік әзірлеу әдістеріне негізделеді, бірақ оларды ауыстырмайды.

Ақпараттық-коммуникациялық технологиялар жеткізілім жүйесі мен өнімдерге және көрсетілген қызметтерге әсер ететін кез келген мәселелерді түсіну үшін ұйымдар жеткізушілермен бірігіп жұмыс істегені жөн. Ұйымдар ақпараттық-коммуникациялық технологиялар жеткізілім жүйесі туралы ақпараттық қауіпсіздік әдістеріне әсер ете алады, сонымен қатар, жеткізушілермен жасалған келісімдерде ақпараттық-коммуникациялық технологияларды жеткізу жүйесінде басқа жеткізушілер алдында қойылатын мәселелерді анық белгілейді.

Ақпараттық-коммуникациялық технологияларды жеткізу жүйесі бұлтты есептеулер бойынша қызметтерді қамтиды.

15.2 Жеткізушінің қызмет көрсетуін басқару

Мақсаты: жеткізуші келісіміне сәйкес келісілген ақпараттық қауіпсіздік деңгейін қамтамасыз ету және қызметтерді көрсету.

15.2.1 Жеткізуші қызметтерін бақылау және шолу жасау

Басқару шаралары

Ұйымдар жеткізушінің қызмет көрсетуін жүйелі түрде бақылауға, қарастыруға және тексеруге тиіс.

Іске асыру жөніндегі нұсқау

Жеткізуші қызметтерін бақылау келісімнің қауіпсіздік ережелері мен шарттарының сақталғанын және ақпараттық қауіпсіздік инциденттері мен мәселелері тиісінше басқарылатынын қамтамасыз етуге тиіс.

Бұл ұйым мен жеткізуші арасындағы сервистік басқарушылық қатынастар процесін қамтуы тиіс:

a) келісімдердің сақталуын тексеру үшін шолуды орындаудың сервистік деңгейлері;

b) жеткізуші ұсынған сервистік есептерді тексеру және келісімдерге сәйкес жүйелі прогресс кездесулерін белгілеу;

c) тәуелсіз аудитор есептеріне шолу жасаумен бірге жеткізушілер аудиттерін жүргізу және белгілі мәселелер бойынша жоспарлы есеп беру;

d) ақпараттық қауіпсіздік инциденттері туралы ақпаратты ұсыну және келісімдер мен сүйемелдеу және процедуралар бойынша кез келген ұсыныстарға сәйкес ақпаратты қарастыру;

e) жеткізушінің бақылау журналын және көрсетілген қызметке байланысты ақпараттық қауіпсіздік оқиғалары, эксплуатациялық мәселелер, сәтсіздіктер, қателер мен бұзуларды қадағалау есептері;

f) кез келген белгілі мәселелерді шешу және басқару;

g) жеткізушінің өзінің жеке жеткізушілерімен қатынастарына шолу туралы ақпараттық қауіпсіздік аспектілері;

h) жеткізушінің келісілген сервистік үздіксіздік деңгейлері негізгі сервистік сәтсіздіктер немесе апаттардан кейін сақталатынына кепіл беру үшін әзірленген жоспарлармен бірге жеткілікті сервистік қабілеттілікті сақтайтынын қамтамасыз ету (17-тарауды қараңыз).

Жеткізушімен орнатылған қатынастарға жауапкешілік тағайындалған адамға немесе сервистік басшылыққа жүктеледі. Сонымен қатар, ұйым жеткізушілердің келісім талаптарын сақтауды қарастыруға міндеттерді жүктегенін қамтамасыз етуге тиіс. Келісім талаптары, соның ішінде, ақпараттық қауіпсіздік талаптарына сәйкес келетінін қамтамасыз ету үшін жеткілікті техникалық дағдылар мен ресурстар қолжетімді болуы тиіс. Тиісті шаралар қызмет көрсетуде жетіспеушілік байқалғанда қабылдануға тиіс.

Ұйым сезгіш немесе маңызды ақпарат үшін барлық қауіпсіздік аспектілерінің толық бақылауды сақтауға тиіс. Ұйым өзгерістерді басқару, осал жерлерді сәйкестендіру және ақпараттық қауіпсіздік инциденттері туралы есептер сияқты қауіпсіздік әрекеттерінде айқындықты сақтауға тиіс.

15.2.2 Жеткізуші қызметтерінің өзгеруін басқару

Басқару шаралары

Бар ақпараттық қауіпсіздік саясатын, процедуралар мен басқару құралдарын сүйемелдеу және жақсартуды қоса алғанда жеткізушілер қызмет көрсетуіндегі өзгерістерді бизнес-ақпараттың, жүйелер мен қамтылған процестердің маңыздылығын және қауіптерді қайта бағалауды есепке ала отырып басқару қажет.

Іске асыру жөніндегі нұсқау

Келесі аспектілер есепке алынуы тиіс:

a) жеткізушімен жасалған келісім өзгерістері;

b) ұйым келесілерді жүзеге асыру үшін енгізген өзгертулер:

1) әрекеттегі ұсынылған қызметтерді жақсарту;

2) кез келген жаңа мәлімдемелер мен жүйелерді дамыту;

3) ұйым саясаттары мен процедураларын түрлендіру немесе жаңарту;

4) ақпараттық қауіпсіздік инциденттерін шешу және қауіпсіздікті жақсартуға арналған жаңа немесе өзгертілген басқару құралдары;

c) келесілерді жүзеге асыру үшін жеткізуші қызметтеріндегі өзгерістер:

1) желілерді өзгерту және жақсарту;

2) жаңа технологияларды пайдалану;

3) жаңа өнімдерді немесе жаңа нұсқаларды қабылдау;

4) жаңа әзірленген аспаптар және қоршаған орта аспаптары;

5) қызмет көрсету құралдарының нақты орналасуының өзгеруі;

6) жеткізушінің өзгеруі;

7) басқа жеткізушімен мердігерлік шарт жасау.

16 Ақпараттық қауіпсіздік инцидентін басқару

16.1 Ақпараттық қауіпсіздік инциденттерін және жақсартуларды басқару

Мақсаты: қауіпсіздік оқиғаларын және осал жерлерді талқылауды қоса алғандағы ақпараттық қауіпсіздік инциденттерін басқаруға арналған жүйелі және тиімді тәсілді қамтамасыз ету.

16.1.1 Міндеттер мен процедуралар

Басқару шаралары

Ақпараттық қауіпсіздік инциденттеріне тез, тиімді және ұйымдастырылған жауапты қамтамасыз ету үшін басқарушылық функциялар мен процедуралар белгіленуі тиіс.

Іске асыру жөніндегі нұсқау

Ақпараттық қауіпсіздік инциденттерін басқаруға қатысты басқарушылық функциялар мен процедураларға арналған келесі ұсыныстарды қарастыру қажет:

a) келесі процедуралар дамытылып, ұйымға тиісінше хабарланғандығын қамтамасыз ету үшін басқарушылық функциялар белгіленуі тиіс:

1) инциденттерге жауап беруді және дайындалуды жоспарлау процедуралары;

2) ақпараттық қауіпсіздік оқиғалары мен инциденттерін бақылау, анықтау, талдау және олар жайлы хабарлау процедуралары;

3) инциденттің басқарушылық әрекеттерін тіркеу процедуралары;

4) сот сараптама деректерін өңдеу процедуралары;

5) ақпараттық қауіпсіздік оқиғалары туралы бағалау және шешім қабылдау және ақпараттық қауіпсіздіктің осал жерлерін бағалау процедуралары;

6) инциденттен кейінгі жайылу, басқарылатын қалпына келуді қоса алғандағы жауап беру процедуралары және ішкі және сыртқы персоналмен немесе ұйымдармен байланысу;

b) белгіленген тәртіптер келесілерді қамтамасыз етуі тиіс:

1) құзыретті персонал ұйымдағы ақпараттық қауіпсіздік инциденттеріне қатысты мәселелермен жұмыс жасайды;

2) қауіпсіздік инциденттерін және хабарламаларды анықтау үшін байланыс нүктесін белгілеу;

3) ақпараттық қауіпсіздік инциденттеріне байланысты мәселелерге қатысты билік, сыртқы мүдделі топтар немесе форумдармен тиісті байланыстар сақталады;

c) есеп беру процедуралары:

1) хабарлама әрекетін сүйемелдеу және хабарламаны құрған адамға ақпараттық қауіпсіздік оқиғасы жағдайында барлық қажетті әрекеттерді есте сақтауға көмектесу үшін ақпараттық қауіпсіздік оқиғаларына арналған хабарламаларды дайындау;

2) ақпараттық қауіпсіздік оқиғасы жағдайында қабылданатын процедура, мысалы, істен шығуға байланысты сәйкессіздік немесе бұзылу типі және байланыс бекетіне дереу хабарлау және тек үйлестірілген әрекеттерді қабылдау сияқты барлық мәліметтерді ескерту;

3) қауіпсіздік ережелерін бұзу туралы хабарлайтын қызметкерлермен байланысу үшін белгіленген ресми тәртіптік процеске сілтеме;

4) ақпараттық қауіпсіздік оқиғалары туралы хабарлайтын адамдар мәселені шешкеннен кейін нәтижелер туралы ескертілгендігін қамтамасыз ету үшін тиісті кері байланысты өңдеу.

Ақпараттық қауіпсіздік инцидентін басқару мақсаттары басқармамен келісілген болып, ақпараттық қауіпсіздік инциденттерін басқаруға жауапты адамдар ақпараттық қауіпсіздік инциденттерін өңдеуге арналған ұйым басымдылықтарын түсінгендігін қамтамасыз ету қажет.

Іске асыру жөніндегі нұсқау

Ақпараттық қауіпсіздік инциденттері ұйымдастырушылық және ұлттық шекаралардан аса алады. Осындай инциденттерге жауап беру үшін жауапты үйлестіру және осы инцидент туралы сыртқы ұйымдармен бөлісу қажеттілігі ұлғаяды.

Ақпараттық қауіпсіздік инцидентін басқаруға арналған толық нұсқау [20] берілген.

16.1.2 Ақпараттық қауіпсіздік оқиғалары туралы хабарлау

Басқару шаралары

Ақпараттық қауіпсіздік оқиғалары туралы тиісті басқару каналдары арқылы дереу хабарлау қажет.

Іске асыру жөніндегі нұсқау

Барлық қызметкерлер мен мердігерлер өздерінің ақпараттық қауіпсіздік оқиғалары туралы дереу хабарлау міндеттері жайлы білуге тиіс. Олар ақпараттық қауіпсіздік оқиғалары туралы хабарлау процедурасы және оқиғалар хабарланатын байланысу бекеті туралы білуге тиіс.

Ақпараттық қауіпсіздік оқиғасы туралы келесі жағдайларда хабарлайды:

a) қауіпсіздікті тиімсіз бақылау;

b) ақпараттық бүтіндік, құпиялылық немесе болжалды қолжетімділікті бұзу;

c) адам қателері;

d) саясат немесе ұсынымдарды бұзу;

e) нақты қорғаныс шараларын бұзу;

f) басқарылмайтын жүйелік өзгерістер;

g) бағдарламалық жасақтама немесе аппараттық құралдардың істен шығуы;

h) қолжетімділіктің бұзылуы.

Басқа ақпарат

Істен шығу немесе басқа нормадан тыс жүйелік әрекеттер қауіпсіздікке бағытталған шабуыл немесе қауіпсіздік ережелерін іс жүзінде бұзу көрсеткіші бола алады, сондықтан, әрдайым ақпараттық қауіпсіздік оқиғасы ретінде хабарлануға тиіс.

16.1.3 Ақпараттық қауіпсіздіктің осал жерлері туралы хабарлау

Басқару шаралары

Ұйымның ақпараттық жүйелері мен қызметтерін пайдаланатын қызметкерлер мен мердігерлер жүйелер мен қызметтердегі күдікті ақпараттық қауіпсіздіктің осал жерлері туралы хабарлауға міндетті.

Іске асыру жөніндегі нұсқау

Барлық қызметкерлер мен мердігерлер ақпараттық қауіпсіздік инциденттерін болдыртпау үшін осы мәселелер туралы байланысу бекетіне дереу хабарлауға тиіс. Хабарлау механизмі максимал түрде оңай және қолжетімді болуға тиіс.

Басқа ақпарат

Қызметкерлер мен мердігерлер күдікті осал жерлерді өз бетінше дәлелдемеуге тиіс. Осал жерлерді сынау жүйені потенциалды дұрыс емес қолдану ретінде түсіндіріліп, ақпараттық жүйе немесе қызмет көрсетуге шығын келтіре алады және сынақты өткізген адамға заңды жауапкершілік жүктей алады.

16.1.4 Ақпараттық қауіпсіздік оқиғаларын бағалау және шешім қабылдау

Басқару шаралары

Ақпараттық қауіпсіздік оқиғалары ақпараттық қауіпсіздік инциденттері ретінде жіктелген жағдайда бағалануы тиіс және шешілуі тиіс.

Іске асыру жөніндегі нұсқау

Байланысу бекеті келісілген ақпараттық қауіпсіздік оқиғасы мен инциденттерді жіктеу шкаласын пайдаланып, әр ақпараттық қауіпсіздік оқиғасын бағалайды және оқиғаның ақпараттық қауіпсіздік инциденті ретінде жіктелуін шешеді. Инцидентті жіктеу және басымдалықтарын белгілеу инцидент әсері мен дәрежесін анықтауға көмектеседі.

Ұйымда қауіпсіздік инциденттеріне жауап берудің ақпараттық тобы (бұдан әрі – ISIRT) бар болған жағдайда, баға мен шешім растау немесе қайта бағалау үшін ISIRT тобына жіберілуі мүмкін.

Келешек сілтеме жасау және тексеру мақсатында бағалау және шешім қабылдау нәтижелері толық тіркелуі тиіс.

16.1.5 Ақпараттық қауіпсіздік инциденттеріне жауап беру

Басқару шаралары

Ақпараттық қауіпсіздік инциденттеріне тіркелген процедураларға сәйкес жауап беру қажет.

Іске асыру жөніндегі нұсқау

Ақпараттық қауіпсіздік инциденттеріне тағайындалған байланысу бекеті және ұйымның немесе үшінші тараптардың басқа тиісті адамдары жауап береді (16.1.1 қараңыз).

Жауап келесіні қамтиды:

a) дереу айғақтарды жинау;

b) талапқа сәйкес (16.1.7 қараңыз) қауіпсіздікті сот сараптамасының ақпараттық талдауын жүргізу;

c) талапқа сәйкес жаю;

d) жауаптың барлық қамтылған әрекеттері кейінгі талдау үшін тиісінше тіркелгендігін қамтамасыз ету;

e) бар ақпараттық қауіпсіздік инциденті немесе кез келген тиісті мәліметтерді басқа ішкі және сыртқы адамдар немесе ұйымдарға хабарлау;

f) инцидентті тудырған ақпараттық қауіпсіздік осалдықтарымен байланысу;

g) іс аяқталғаннан кейін істі ресми жабу және есеп құру.

Инцидент көзін анықтау үшін постинцидентті талдау қажеттілігіне орай орындалуға тиіс.

Басқа ақпарат

Инциденттерге жауап берудің бірінші мақсаты – «қалыпты қауіпсіздік деңгейін» жаңартып, кейін қажетті қалпына келтіруді бастау.

16.1.6 Ақпараттық қауіпсіздік инциденттерінен білім алу

Басқару шаралары

Ақпараттық қауіпсіздік инциденттерін талдау және шешуден алынған білім келешек инциденттер ықтималдығын немесе әсерін азайту үшін қолданылуға тиіс.

Іске асыру жөніндегі нұсқау

Ақпараттық қауіпсіздік инциденттерінің типтері, көлемдері мен шығындарына мөлшерлік түрде анықталып, тексерілу мүмкіндігін беретін механизм болуға тиіс.

Ақпараттық қауіпсіздік инциденттерін бағалаудан алынған ақпарат қалпына келу деңгейін анықтау немесе инциденттерге орасан зор әсер ету үшін қолданылуы тиіс.

Басқа ақпарат

Ақпараттық қауіпсіздік инциденттерін бағалау келешекте жиілік, зақымдану мен шығындарды шектеу үшін кеңейтілген немесе қосымша басқару құралдары қажеттілігіне көрсете алады немесе қауіпсіздік саясатын қарастырған кезде есепке алына алады (5.1.2 қараңыз).

Құпия аспектілерін қорғау мақсатында іс жүзіндегі ақпараттық қауіпсіздік инциденттері туралы күлкілі оқиғалар осындай инциденттерге қалай жауап беру қажет және оларды келешекте қалай болдыртау қажет мысалдары ретінде тұтынушылық хабардарлыққа оқытуда (7.2.2 қараңыз) қолданыла алады.

16.1.7 Айғақтарды жинау

Басқару шаралары

Ұйым айғақ бола алатын ақпаратты сәйкестендіру, жинау, сатып алу және сақтау процедураларын белгілеп, қолдануға тиіс.

Іске асыру жөніндегі нұсқау

Тәртіптік шаралар және сот қуынымақсатында ішкі тәсілдер айғақтармен жұмыс істеп әзірленуі тиіс.

Жалпы, осы айғақ жинау процедуралары түрлі деректер, құрылғылар типіне және құрылғылар статусына, мысалы, іске қосылған немесе сөндірілген, сәйкес айғақтарды сәйкестендіру, жинау, сатып алу және сақтау процестерін қамтамасыз етуге тиіс. Процедуралар келесілерді есепке алуға тиіс:

a) тұжырым тізбегі;

b) айғақтардың қауіпсіздігі;

c) персонал қауіпсіздігі;

d) персоналдың рөлдері мен міндеттері;

e) персонал құзыреті;

f) құжаттама;

g) брифинг.

Сақталған айғақтардың құндылығын арттыру үшін қолжетімді жағдайларда персоналды сертификаттау немесе басқа тиісті біліктілік құралдары табылуға тиіс.

Сот сараптамасының деректері ұйым немесе ведомство ішілік шекаралардан аса алады. Бұл жағдайларда ұйымның қажетті ақпаратты сот сараптамасының деректері ретінде жинау құқығын қамтамасыз ету қажет. Түрлі құзырет талаптары тиісті құзырет арқылы қолжетімділік мүмкіндіктерін ұлғайтады.

Басқа ақпарат

Сәйкестендіру потенциалды айғақтарды іздеу, мойындау және құжаттауды қамтитын процесс болып табылады. Жинау – потенциалды айғақтард қамти алатын нақты тармақтарды жинау процесі. Сатып алу – белгілі жинақ шеңберінде деректер көшірмесін жасау процесі. Сақтау – потенциалды айғақтардың бүтіндігі мен түпнұсқалығын қорғауға арналған процесс.

Ақпараттық қауіпсіздік оқиғасы алғаш рет анықталған кезде, оқиғаның сот қуынымына әкелетіні белгісіз. Сондықтан, инцидент маңыздылығы түсінгенге дейін қажетті айғақтардың қасақана немесе кездейсоқ бұзылу қаупі бар. Кез келген қарастырылған сот қуынымында адвокат немесе полицияны тартып, талап етілетін айғақтарға қатысты кеңес алған жөн.

[24] сандық айғақтарды сәйкестендіру, жинау, сатып алу және сақтауға арналған ұсынымдарды белгілейді.

17 Бизнес үздіксіздігін басқарудың ақпараттық қауіпсіздік аспектілері

17.1 Ақпараттық қауіпсіздіктің үздіксіздігі

Мақсаты: ақпараттық қауіпсіздіктің үздіксіздігі ұйымның бизнес үздіксіздігін басқару жүйелерінде қамтылуға тиіс.

17.1.1 Ақпараттық қауіпсіздіктің үздіксіздігін жоспарлау

Басқару шаралары

Ұйым жағымсыз жағдайларда, мысалы, дағдарыс немесе апаттар кезінде, ақпараттық қауіпсіздіктің үздіксіздігін басқаруға және ақпараттық қауіпсіздікке арналған өз талаптарын белгілеуге тиіс.

Іске асыру жөніндегі нұсқау

Ұйым ақпараттық қауіпсіздік үздіксіздігінің бизнес үздіксіздігін басқару процесінің шеңберінде немесе апаттық қалпына келтіруді басқару процесінің шеңберінде болуын анықтауға тиіс. Бизнес үздіксіздігі мен апаттық қалпына келтіруді жоспарлаған кезде, ақпараттық қауіпсіздік талаптары белгіленуі тиіс.

Ресми бизнес үздіксіздігі мен апаттық қалпына келтіруді жоспарлау болмаған жағдайда, ақпараттық қауіпсіздікті басқару ақпараттық қауіпсіздік талаптары қалыпты пайдалану жағдайларымен салыстырғанда жағымсыз жағдайларда бірдей болып қалатынын шешуге тиіс. Балама ретінде, ұйым жағымсыз жағдайларға қолданылатын ақпараттық қауіпсіздік талаптарын белгілеу үшін ақпараттық қауіпсіздік аспектілеріне әсерін талдау қажет.

Басқа ақпарат

Ақпараттық қауіпсіздікке тигізетін әсерді «қосымша» іскерлік талдау бойынша уақыт пен күш салуды азайту үшін талдауға әсер ететін бизнес үздіксіздігін қалыпты басқару немесе апаттық қалпына келтіруді басқару шеңберінде ақпараттық қауіпсіздік аспектілерін алған жөн. Бұл ақпараттық қауіпсіздік үздіксіздігі талаптарының бизнес үздіксіздігін басқаруда немесе апаттық қалпына келтіруді басқару процестерінде анық тұжырымдалғанын білдіреді.

Бизнес үздіксіздігін басқару туралы ақпарат [14], [9] және [8] берілген.

17.1.2 Ақпараттық қауіпсіздік үздіксіздігін жүзеге асыру

Басқару шаралары

Ұйым жағымсыз жағдай барысында ақпараттық қауіпсіздік үздіксіздігінің қажетті деңгейін қамтамасыз ету үшін басқару процестерін, процедураларын және құралдарын белгілеп, тіркеуге, жүзеге асыруға және сүйемелдеуге тиіс.

Іске асыру жөніндегі нұсқау

Ұйым келесілерге кепіл беруге тиіс:

a) қажетті білік, тәжірибе мен құзыретті пайдаланып, бұзғыш әрекеттерге дайындалу, оларды жұмсарту және оларға жауап беру үшін тиісті басқару құрылымы бар;

b) инцидентті басқару және ақпараттық қауіпсіздікті сүйемелдеу үшін қажетті жауапкершілігі, билігі және құзыреті бар инциденттерге жауап беру персоналы тағайындалады;

c) ұйым бұзғыш оқиғаны қалай басқаратыны және басқарма мақұлдаған қауіпсіздік үздіксіздігінің ақпараттық мақсаттарына негізделген алдын ала белгіленген деңгейде ақпараттық қауіпсіздікті қалай сүйемелдейтінін нақтылап, тіркелген қалпына келтіру жоспарлары, жауаптары мен процедуралары дамытылып, мақұлданған (17.1.1 қараңыз).

Ақпараттық қауіпсіздік үздіксіздігінің талаптарына сәйкес ұйым келесілерді белгілеуге, тіркеуге, жүзеге асыруға және сүйемелдеуге тиіс:

a) бизнес үздіксіздігі немесе апаттық қалпына келтіру процестері, процедурлары мен сүйемелдеу жүйелерінің және аспаптарының шеңберінде ақпараттық қауіпсіздікті қамтамасыз ету шаралары;

b) жағымсыз жағдай барысында бар ақпараттық қауіпсіздікті басқару құралдарын сүйемелдеу үшін процестер, процедуралар мен енгізулер өзгертіледі;

c) жағымсыз жағдай барысында сақтала алмайтын ақпараттық қауіпсіздікті басқару құралдарына арналған өтеуші басқару құралдары.

Басқа ақпарат

Бизнес үздіксіздігі немесе апаттық қалпына келтіру шеңберінде белгілі процестер мен процедуралар белгілене алады. Оларды сүйемелдеуге арналған осы процестер мен процедуралар шеңберінде немесе арнаулы ақпараттық жүйелер шеңберінде өңделген ақпарат қорғалуы тиіс. Сондықтан, ұйым бизнес үздіксіздігі немесе апаттық қалпына келтіру процестері мен процедураларын белгілеп, жүзеге асырып және сүйемелдеп, ақпараттық қауіпсіздік бойынша мамандарды тартуға тиіс.

Жүзеге асырылуға тиіс ақпараттық қауіпсіздікті қамтамасыз ету шаралары жағымсыз жағдай барысында жұмысын жалғастыруға тиіс. Егер қауіпсіздікті қамтамасыз ету шаралары ақпаратты қамтамасыз етуді жалғастыруға қабілетсіз болса, ақпараттық қауіпсіздіктің рұқсат етілген деңгейін сүйемелдеу үшін басқа басқару құралдары белгіленуге, жүзеге асырылуға және сақталуға тиіс.

17.1.3 Ақпараттық қауіпсіздік үздіксіздігін тексеру, қарастыру және бағалау

Басқару шаралары

Ақпараттық қауіпсіздік үздіксіздігін басқару құралдары жағымсыз жағдайларда жарамды және тиімді болуын қамтамасыз ету үшін ұйым белгіленген және жүзеге асырылған басқару құралдарын тексеруге тиіс.

Іске асыру жөніндегі нұсқау

Пайдалану немесе үздіксіздікке қатысты ұйымдастырушылық, техникалық, процедуралық пен процестік өзгерістер ақпараттық қауіпсіздік үздіксіздігі талаптарын да өзгерте алады. Осы жағдайларда ақпараттық қауіпсіздікке арналған процестер, процедуралар мен басқару құралдарының үздіксіздігі осы өзгертілген талаптарға қарсы қарастырылуға тиіс.

Ұйымдар өзінің ақпараттық қауіпсіздік үздіксіздігін басқаруды тексеруге тиіс:

a) олар ақпараттық қауіпсіздік үздіксіздік мақсаттарымен үйлесуін қамтамасыз ету үшін ақпараттық қауіпсіздік үздіксіздік процестерінің функционалдығын, процедуралары мен басқары құралдарын зерттеу және сынау;

b) олардың жұмысы ақпараттық қауіпсіздік үздіксіздік мақсаттарымен үйлесуін қамтамасыз ету үшін ақпараттық қауіпсіздік үздіксіздік процестерін, процедуралары мен басқару құралдарын басқару үшін білім мен белгіленген тәртіпті тексеру және сынау;

c) ақпараттық жүйелер, ақпараттық қауіпсіздік процестері, процедуралар мен басқару құралдары немесе бизнес үздіксіздігін басқару/апаттық қалпына келтіру процестері мен шешімдері басқарушылық түрде өзгерген кезде, ақпараттық қауіпсіздік үздіксіздігінің заңдылығы мен тиімділігін қарастыру өлшемді болады.

Басқа ақпарат

Ақпараттық қауіпсіздік үздіксіздігін басқару құралдарын тексеру жалпы ақпаратты сынау және тексеруден ерекшеленеді және өзгерістерден сынаудан тыс орындалуы тиіс. Мүмкіндігіне орай, ақпараттық қауіпсіздік үздіксіздігін басқару құралдарын ұйым бизнесінің үздіксіздігі немесе апаттық қалпына келтіруді сынаумен бірге біріктірген жөн.

17.2 Артықшылық

Мақсаты: ақпаратты өңдеу құралдарының қолжетімділігін қамтамасыз ету.

17.2.1 Ақпаратты өңдеу құралдарының қолжетімділігі

Басқару шаралары

Ақпаратты өңдеу құралдары қолжетімділік талаптарына сәйкес келу үшін жеткілікті артықшылықпен жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқау

Ұйымдар ақпараттық жүйелердің қолжетімділігіне арналған іскерлік талаптарды белгілеуі тиіс. Жүйелердің бар архитектурасын қолдану арқылы қолжетімділікті қамтамасыз ету мүмкін емес болған жағдайда, артықшылық құрауыштарды немесе архитектураны қарастыру қажет.

Бір құрауыштан тағайындалған басқа құрауышқа дейін бас тартуға төзімділікті қамтамасыз ету үшін артық ақпараттық жүйелерді тексеру қажет.

Басқа ақпарат

Жұмыстан шығарушаларды енгізу ақпараттық жүйелерді жобалау қарастырылуға тиіс ақпарат пен ақпараттық жүйелердің бүтіндігі немесе құпиялылығыс үшін қауіптерді тудыра алады.

18 Сәйкестік

18.1 Заңды және шарт талаптарына сәйкестік

Мақсаты: ақпараттық қауіпсіздік пен кез келген баса қауіпсіздік талаптарына қатысты заңда белгіленген заңды, реттеуіш немесе шарт міндеттерін бұзуды болдыртпау.

18.1.1 Қолданылатын заңнама мен шарт талаптарын сәйкестендіру

Басқару шаралары

Заңда белгіленген барлық тиісті заңды, реттеуіш, шартты талаптарға сәйкес келу үшін оларды белгілеу, тіркеу және әр ақпараттық жүйе мен ұйым үшін жетілдірілуі тиіс.

Іске асыру жөніндегі нұсқау

Белгілі басқару құралдары мен осы талаптарға сәйкес келетін жеке жауапкершілік те белгіленуі және тіркелуі тиіс.

Менеджерлер олардың бизнес типіне қойылатын талаптарға сәйкес келу үшін олардың ұйымдарына қолданылатын барлық заңнаманы белгілеуі тиіс. Егер ұйым өзінің істерін басқа елдерде жүргізсе, менеджерлер барлық тиісті елдерде сақталуын қарастыруға тиіс.

18.1.2 Зияткерлік меншік құқықтары

Басқару шаралары

Зияткерлік меншік құқықтарына және бағдарламалық өнімдердің құрауыштарын пайдалануға байланысты заңды, реттеуіш және шарт талаптарына сәйкестікті қамтамасыз ету үшін тиісті процедуралар жүзеге асырылуы тиіс.

Іске асыру жөніндегі нұсқау

Келесі ұсыныстар зияткерлік меншік деп саналатын кез келген материалды қорғайды:

a) ақпараттық өнімдер мен бағдарламалық жасақтаманы заңды түрде пайдалануды белгілейтін зияткерлік меншік құқықтарын сақтау саясатын жариялау;

b) авторлық құқық бұзылмағанын қамтамасыз ету үшін бағдарламалық жасақтаманы тек әйгілі және құрметті көздер арқылы сатып алу;

c) зияткерлік меншік құқықтарын қорғау саясатын түсінуді сүйемелдеу және оларды бұзатын персоналға қарсы тәртіптік шараларды қабылдау туралы мәлімдемелер ұсыну;

d) активтің барлық тиісті тізілімдерін жүргізу және зияткерлік меншік құқықтарын қорғау үшін барлық активтерді талаптармен сәйкестендіру;

e) сүйемелдеуші айғақтар және негізгі дисктер, нұсқаулар және т.б. лицензияларының меншік құқығының айғақтары;

f) лицензия шеңберінде рұқсат етілген тұтынушылардың максимал саны аспағанын қамтамасыз ету үшін басқару шаралары енгізу;

g) тек қондырылған бағдарламалық жасақтама мен лицензияланған өнімдер бойынша шолу жасау;

h) лицензияның тиісті шарттарын сүйемелдеу үшін саясатты қамтамасыз ету;

i) бағдарламалық жасақтаманы басқаларға беру немесе оны жою үшін саясатты қамтамасыз ету;

j) бағдарламалық жасақтама мен ақпаратқа арналған қағидалар мен шарттар жалпыға қолжетімді желіле арқылы алынды;

k) авторлық құқық туралы заңда рұқсат етілген жағдайлардан басқа, коммерциялық жазбалардан (фильм, аудио) басқа пішімге ауыстыру, оларды көшірмеу немесе шығарып алу;

l) авторлық құқық туралы заңда рұқсат етілген жағдайлардан басқа, кітап, мақала, баяндама немесе басқа құжаттарды толық немесе бөлшектеп көшірмеу.

Басқа ақпарат

Зияткерлік меншік құқықтары бағдарламалық жасақтама немесе құжаттың авторлық құқықтарын, дизайнерлік құқықтарды, сауда маркаларды, бастапқы кодтың патенті мен лицензияларын қамтиды.

Меншікті құрайтын бағдарламалық өнімдер әдетте лицензияның қолданылу мерзімін және шарттарын белгілейтін лицензиялық келісімге сәйкес жеткізіледі, мысалы, белгіленген машиналарға өнімдерді қолдануды шектеу немесе резервтік көшірмелерді құру арқылы көшіруді шектеу. Зияткерлік меншік құқықтарының маңыздылығы мен оларды түсіну ұйым дамытқан бағдарламалық жасақтама үшін штатқа хабарлануы тиіс.

Заңды, реттеуіш және шарт талаптары меншікті құрайтын материалды көшіруге арналған шектеулерді белгілей алады. Соның ішінде олар тек лицензиялатын немесе әзірлеушімен ұйымда қамтамасыз етілетін ұйымда дамытылған материал ғана қолданыла алатынын талап ете алады. Авторлық құқықты бұзу айыппұл мен қылмыстық сот ісін қамтуы мүмкін сот қуынымына әкеле алады.

18.1.3 Есептерді қорғау

Басқару шаралары

Есептер заңды, реттеуіш, шарт және іскерлік талаптарға сәйкес жоғалудан, бұзылудан, бұрмалаудан, рұқсат етілмеген қолжетімділіктен және рұқсат етілмеген шығарудан қорғалуы тиіс.

Іске асыру жөніндегі нұсқау

Белгілі ұйым есептерін, ұйымның жіктеу жүйесіне негізделген олардың тиісті жіктелуін қорғауды қарастыру қажет. Есептер санаттарға бөлінуі тиіс, мысалы, бухгалтерлік есептер, деректер базасының есептері, транзакция журналдары, бақылау журналдары және пайдалану процедуралары, олардың әрқайсысы үшін жүргізу кезеңдері мен рұқсат етілген деректер тасымалдаушылары белгіленуі тиіс, мысалы, қағаз, микрофиш, магнит, оптикалық. Кез келген байланысты шифр кілттері мен шифрланған мұрағаттар немесе сандық қолдарға байланысты бағдарламалар (10-тармақты қараңыз) уақыт аралығындағы есептерді декодтауға мүмкіндік беру үшін сақталуы тиіс, есептер де сақталғаны жөн.

Есептерді сақтау үшін қолданылатын деректердің нашарлау мүмкіндігіне назар аудару қажет. Сақтау және өңдеу процедуралары дайындаушының ұсынымдарына сәйкес жүзеге асырылуы тиіс.

Деректердің электрондық тасымалдаушылары таңдалған жағдайда, келешек технологиялық өзгерістерге байланысты жоғалудан қорғау үшін жүргізу кезеңінің ішінде деерктерге қолжетімділік алу үшін процедуралар белгіленуі тиіс.

Қажетті деректер орындалатын талаптарға сәйкес жарамды кезеңде және пішімде қалпына келтіруін қамтамасыз ету үшін деректерді сақтау жүйелері таңдалуы тиіс.

Сақтау және өңдеу жүйесі ұлттық немесе аймақтық заңнамада белгіленген есептер мен оларды жүргізу кезеңін сәйкестендіруді қамтамасыз етуі тиіс. Осы жүйе, олар ұйымға қажет болмаған жағдайда, есептерді сол кезеңнен кейін тиісті бұзуға рұқсат етуге тиіс.

Осы қорғау мақсаттарына қол жеткізу үшін келесі қадамдар ұйымда сақталуы тиіс:

a) есептер мен ақпаратты сақтау, өңдеу және жоюға арналған ұсынымдар белгіленуі тиіс;

b) есептер мен олар сақталуға тиіс уақыт аралығын белгілеп, жүргізу кестесі құрылуы тиіс;

c) түйінді ақпарат дереккөздерінің құрал-саймандары сақталуы тиіс.

Басқа ақпарат

Заңды, реттеуіш немеса шарт талаптарына сәйкес келу үшін және бар іскерлік белсенділікті сүйемелдеу үшін кейбір есептер сенімді түрде сақталуы тиіс. Мысалы, потенциалды азаматтық процесс немесе қылмыстық әрекетке қарсы қорғанысты қамтамасыз ету үшін немесе акционерлерге, үшінші тараптарға және аудиторларға ұйымның қаржы жағдайын растау үшін ұйымның белгіленген заңды немесе реттеуіш қағидалар шеңберінде жұмыс істейтінін растау үшін ьалап етілетін есептер. Мемлекеттік құқық немесе реттеу ақпараттық жүргізуге арналған уақыт аралығын немесе деректер мазмұнын белгілеуі мүмкін.

Ұйым есептерін басқару туралы қосымша ақпарат [5] берілген.

18.1.4 Жеке өмір және жеке деректерді қорғау

Басқару шаралары

Жеке өмір және жеке деректерді қорғау тиісті заңнама мен реттеуде талап етілетіндей қамтамасыз етілуі тиіс.

Іске асыру жөніндегі нұсқау

Жеке өмір және жеке деректерді қорғауға арналған ұйым саясаты дамытылып, жүргізілуі тиіс. Осы саясат жеке деректерді өңдеуде мүдделі барлық тұлғаларға хабарлануы тиіс.

Осы саясат пен адамдардың жеке өмірі мен жеке деректерді қорғауға қатысты барлық тиісті заңнама мен нұсқаулықтарға сәйкестік тиісті басқарушылық құрылым мен бақылауды талап етеді. Менеджерлер, тұтынушылар мен қызметтерді жеткізушілерге олардың жеке жауапкершілігі мен орындалуға тиіс нақты процедуралар туралы түсінік беруге тиісті жеке өмір төрешілі сияқты жауапты адамды тағайындау арқылы қол жеткізу қажет. Жеке деректерді өңдеу жауапкершілігі және жеке өмір принциптерін түсінуді қамтамасыз ету тиісті заңнама мен нұсқаулықтарға сәйкес болуы тиіс. Жеке деректерді қорғау үшін тиісті техникалық және ұйымдастырушылық шаралар жүзеге асырылуы тиіс.

Басқа ақпарат

[25] ақпараттық-коммуникациялық технологиялар жүйелерінің шеңберінде жеке деректерді қорғау үшін жоғары деңгей негізі бола алады. Көптеген елдер жеке деректерді жинау, өңдеу және жіберуді бақылайтын заңдарды енгізді (әдетте осы ақпарат арқылы танила алатын өмір сүретін адамдар туралы ақпарат). Тисті ұлттық заңнамаға тәуелді осындай басқару құралдары жеке деректерді жинайтын, өңдейтін және тарататын адамдарға міндеттер жүктей алады және жеке деректерді басқа елдерге беруді шектей алады.

18.1.5 Шифрлау басқару құралдарын реттеу

Басқару шаралары

Шифрлау басқару құралдары барлық тиісті келісімдер, заңдар мен нұсқаулықтарға сәйкес қолданылуы тиіс.

Іске асыру жөніндегі нұсқау

Тиісті келісімдер, заңдар мен қаулыларға сәйкес келу үшін келесі тармақтарды қарастыру қажет:

a) шифрлау функцияларын орындау үшін компьютерлік техника мен бағдарламалық жасақтаманы импорттау немесе экспорттауды шектеу;

b) компьютерлік техника мен оларға шифрлау функцияларын қосу үшін әзірленген бағдарламалық жасақтаманы импорттау немесе экспорттауды шектеу;

c) шифрлауды қолдануды шектеу;

d) мазмұнның құпиялылығын қамтамасыз ету үшін аппараттық құралдар немесе бағдарламалық жасақтама арқылы шифрланған ақпаратқа ел билігінің қолжетімділігінің міндетті немесе бақыланатын әдістері.

Тиісті заң мен нұсқаулықтарға сәйкестікті қамтамасыз ету үшін заң кеңесін алу қажет. Шифрлау ақпарат немесе шифрлау басқару құралдары ведомство ішілік шекаралар өткенге дейін заң кеңесін алу қажет.

18.2 Ақпараттық қауіпсіздік шолулары

Мақсаты: ақпараттық қауіпсіздік ұйым саясаты мен процедураларына сәйкес жүзеге асырылатынын және басқарылатынын қамтамасыз ету.

18.2.1 Ақпараттық қауіпсіздікке тәуелсіз шолу

Басқару шаралары

Басшылыққа алынатын ақпараттық қауіпсіздікке арналған ұйым тәсілі мен оны енгізу (яғни, бақылау мақсаттары, басқару құралдары, ақпараттық қауіпсіздік саясаты, процестері мен процедуралары) жоспарланған аралықтарда тәуелсіз немесе елеулі өзгерістер енгізілген кезде қарастырылуы тиіс.

Іске асыру жөніндегі нұсқау

Басшылық тәуелсіз шолуды бастауы тиіс. Осындай тәуелсіз шолу ұйымның басшылыққа алынатын ақпараттық қауіпсіздігіне тәсілінің жарамдылығын, сәйкестігін және тиімділігін қамтамасыз ету үшін қажет. Шолу бақылау мақсаттары мен саясатты қоса алғандағы қауіпсіздік тәсілдерін бағалау және өзгерту қажеттілігін қамтуы тиіс.

Осындай шолуды қарастырылатын салаға тәуелсіз адамдар орындауға тиіс, мысалы, осындай шолуларға мамандырылған ішкі аудит қызметі, тәуелсіз менеджер немесе үшінші тарап ұйымы. Осы шолуларды орындайтын адамдардың тиісті дағдылары мен тәжірибесі болуы тиіс.

Тәуелсіз шолу нәтижелерін тіркеп, шолуды бастаған басшылыққа хабарлау қажет. Осы есептер сақталуы тиіс.

Егер тәуелсіз шолу басшылыққа алынатын ақпараттық қауіпсіздікке арналған ұйым тәсілі және оны енгізу сәйкес келмейді деп белгілесе, мысалы, тіркелген мақсаттар талаптарға сәйкес келмейді немесе ақпараттық қауіпсіздік саясатында белгіленген ақпараттық қауіпсіздік бағытымен үйлеспейді (5.1.1 қараңыз), басшылық түзетуші әрекеттерді қарастыруы тиіс.

Басқа ақпарат

[12], «Қауіпсіздікті басқару жүйелерін ақпараттық тексеруге арналған ұсынымдар» және [13], «Қауіпсіздікті қамтамасыз етудің ақпараттық шаралары туралы аудиторларға арналған ұсынымдар» тәуелсіз шолуды орындау туралы түсінік береді.

18.2.2 Қауіпсіздік саясаты мен стандарттарға сәйкестік

Басқару шаралары

Менеджерлер тиісті қауіпсіздік саясаты, стандарттар мен кез келген басқа қауіпсіздік талаптарына сәйкес олардың жауапкершілік саласының шеңберінде ақпаратты өңдеу процедураларын сақтауды жүйелі түрде қарастыруы тиіс.

Іске асыру жөніндегі нұсқау

Саясатта, стандарттарда және басқа қолданылатын нұсқаулықтарда белгіленген ақпараттық қауіпсіздік талаптары сәйкес келетінін қамтамасыщ ету үшін менеджерлер ақпаратты қалай қарастыру қажеттігін белгілеуі тиіс. Тиімді жүйелі шолу үшін автоматтық өлшеу және аспаптар туралы хабарлауды қарастыру қажет.

Егер шолу барысында қандай да болмасын бұзушылық анықталса, менеджерлер:

a) бұзу себебін анықтауға;

b) сақтауға қол жеткізу үшін әрекеттер қажеттілігін бағалауға;

c) тиісті түзетуші әрекетті жүзеге асыуға;

d) оның тиімділігін тексеру және кез келген дефицит немесе осал жерлерді анықтау үшін қабылданған салдарларды жою бойынша шараларды қарастыруға тиіс.

Менеджерлер орындаған шолулар мен түзетуші әрекеттердің нәтижелері тіркелуі тиіс, осы есептер сақталуы тиіс. Менеджерлер нәтижелер туралы олардың жауапкершілік саласы шеңберіндегі тәуелсіз шолуларды орындайтын адамдарға (18.2.1 қараңыз) хабарлауы тиіс.

Басқа ақпарат

Жүйелік пайдалануды эксплуатациялық бақылау 12.4 берілген.

18.2.3 Сақтауға техникалық шолу

Басқару шаралары

Ұйымның ақпараттық қауіпсіздік саясаты мен стандарттарға сәйкес келу үшін ақпараттық жүйелер жүйелі түрде қарастырылуы тиіс.

Іске асыру жөніндегі нұсқау

Кейән техникалық маман түсіндіретін техникалық есептерді жасайтын автоматтандырылған аспаптар арқылы техникалық сақтау қарастырлуы тиіс. Балама түрде қолмен шолуды тәжірибелі жүйелік инженер орындай алады (қажет болса, тиісті бағдарламалық құралдармен сүйемелденген).

Егер ену сынақтары немесе осалдықты бағалау қолданылса, алдын ала ескерту жүзеге асырылуы тиіс. Әрекеттер жүйенің қауіпсіздік компромисіне әкеле алады. Осындай сынақтар жоспарланып, тіркелуі және қайталануы тиіс.

Кез келген техникалық шолуды құзыретті, сенімді тұлғалар немесе осындай адамдардың бақылауымен орындау қажет.

Басқа ақпарат

Техникалық шолулар аппараттық және бағдарламалық жасақтаманы басқару құралдары дұрыс жүзеге асырылуын қамтамасыз ету үшін эксплуатациялық жүйелерді сараптауды қамтиды. Шолудың осы типі техникалық сараптамалық білімі бар маманды талап етеді.

Осы шолулар, сондай-ақ, ену сынақтары мен осалдықты бағалауға қатысты болады, оларды осы мақсатта шартталған тәуелсіз сарапшылар орындай алады. Бұл жүйедегі осал жерлерді анықтауда және осы осал жерлерге байланысты рұқсат етілмеген қолжетімділікті болдыртпаудағы басқару құралдарының тиімділігін анықтау үшін пайдалы бола алады.

Енуді сынау және осалдықты бағалау мемлекет белгілеген уақытта жүйе кескінін қамтамасыз етеді. Кескін ену әрекеттері кезінде іс жүзінде тексерілген бөліктермен шектеледі. Енуді сынау және осалдықты бағалау қауіп дәрежесін бағалау орнын баса алмайды.

[13] техникалық шолуларға қатысты белгілі нұсқауды қамтамсыз етеді.

Библиография

[1] ISO/IEC, Directives, Part 2 (Директивалар, 2-бөлім)

[2] ISO/IEC 11770-1, *Information technology - Security techniques - Key management - Part 1: Framework (Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Кілт менеджменті. 1-бөлім. Құрылым)*

[3] ISO/IEC 11770-2, *Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques (Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Кілт менеджменті. 2-бөлім. Симметриялық әдістерді қолданатын механизмдер)*

[4] ISO/IEC 11770-3, *Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques (Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Кілт менеджменті. 3-бөлім. Асимметриялық әдістерді қолданатын механизмдер)*

[5] ISO 15489-1, *Information and documentation - Records management - Part 1. General (Ақпарат және құжаттама. Жазбаларды басқару. 1-бөлім. Жалпы талаптар)*

[6] ISO/IEC 20000-1, *Information technology - Service management - Part 1: Service management system requirements (Ақпараттық технология. Қызметтер менеджменті. 1-бөлім. Қызметтер менеджменті жүйесіне қойылатын талаптар)*

[7] ISO/IEC 20000-2, *Information technology - Service management - Part 2: Guidance on the application of service management systems (Ақпараттық технология. Қызметтер менеджменті. 1-бөлім. Қызметтер менеджменті жүйелерін пайдалану жөніндегі нұсқау)*

[8] ISO 22301, *Societal security - Business continuity management systems - Requirements (Әлеуметтік қауіпсіздік. Бизнес үздіксіздігінің менеджмент жүйесі. Талаптар)*

[9] ISO 22313, *Societal security - Business continuity management systems - Guidance (Әлеуметтік қауіпсіздік. Бизнес тұрақтылығының менеджмент жүйесі. Нұсқау)*

[10] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements (Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар)*

[11] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік қауіптерінің менеджменті)*

[12] ISO/IEC 27007, *Information technology - Security techniques - Guidelines for information security management systems auditing (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік жүйелерінің менеджменті жүйелері аудиті жөніндегі басшылыққа алынатын нұсқаулар)*

[13] ISO/IEC TR 27008, *Information technology - Security techniques - Guidelines for auditors on information security controls (Ақпараттық технологиялар. Қорғауды қамтамасыз ету әдістері. Басқару органдарын бағалау жөніндегі аудиторларға арналған басшылыққа алынатын нұсқаулар)*

[14] ISO/IEC 27031, *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық-коммуникациялық технологиялардың бизнесті жүргізуге дайындығы жөніндегі басшылыққа алынатын нұсқаулар)*

[15] ISO/IEC 27033-1, I*nformation technology - Security techniques - Network security - Part 1: Overview and concepts (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Желі қауіпсіздігі. 1-бөлім. Шолу және тұжырымдамалар)*

[16] ISO/IEC 27033-2, *Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Желіні қорғау. 2-бөлім. Желіні қорғауды жобалау және енгізу жөніндегі басшылыққа алынатын нұсқаулар)*

[17] ISO/IEC 27033-3, *Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Желі қауіпсіздігі. 3-бөлім. Эталондық желі сценарийлері. Қауіптер, жобалау әдістері және басқару мәселелері)*

[18] ISO/IEC 27033-4, *Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Желі қауіпсіздігі. 4-бөлім. Қауіпсіздік шлюздерін қолдану арқылы желілер арасындағы қауіпсіздікті қамтамасыз етуге арналған коммуникациялар)*

[19] ISO/IEC 27033-5, *Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs) (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық желі қауіпсіздігі. 5-бөлім. Виртуалдық жеке желілерді қолдану арқылы желілер арасындағы қауіпсіздікті қамтамасыз етуге арналған коммуникациялар)*

[20] ISO/IEC 27035, *Information technology - Security techniques - Information security incident management (Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдісі. Ақпараттық қауіпсіздік жүйесінде кездейсоқ жағдайларды басқару)*

[21] ISO/IEC 27036-1, *Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Жеткізушілермен байланысу ақпаратын қорғау. 1-бөлім. Шолу және тұжырымдама)*

[22] ISO/IEC 27036-2, *Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Жеткізушілермен байланысу ақпаратын қорғау. 2-бөлім. Талаптар)*

[23] ISO/IEC 27036-3, *Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Жеткізушілермен байланысу ақпаратын қорғау. 3-бөлім. Ақпараттық және коммуникациялық технологиялардың жеткізілім тізбектерін қорғау жөніндегі басшылыққа алынатын нұсқаулар)*

[24] ISO/IEC 27037, *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сандық деректерді сәйкестендіру, жинау, сатып алу және сақтау жөніндегі басшылыққа алынатын нұсқаулар)*

[25] ISO/IEC 29100, *Information technology - Security techniques - Privacy framework (Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Құпиялылық схемасы)*

[26] ISO/IEC 29101, *Information technology - Security techniques - Privacy architecture framework (Ақпараттық технологиялар. Қорғанысты қамтамасыз ету технологиясы. Құпиялылықты қамтамасыз етуге арналған архитектура)*

[27] ISO 31000, *Risk management - Principles and guidelines (Қауіптер менеджменті. Принциптер мен басшылыққа алынатын нұсқаулар)*

В.А қосымшасы
(ақпараттық)

В.А.1 кестесі – Стандарттардың сілтемелік халықаралық, аймақтық стандарттарға, шетел мемлекеттерінің стандарттарына сәйкестігі туралы мәліметтер

Халықаралық, аймақтық стандарттардың, шетел мемлекеттік стандартының белгіленуі және атауы	Сәйкестік дәрежесі	Ұлттық стандарт, мемлекет аралық стандарттың белгіленуі және атауы
ISO/IEC 27000:2012 Information technology - Security techniques - Information security management systems - Overview and vocabulary	IDT	ҚР СТ ISO/IEC 27000-2013 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік менеджмент жүйелері. Жалпы шолу және сөздік
ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements	IDT	ҚР СТ ISO/IEC 27001-201_* Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік менеджмент жүйелері. Талаптар.

* Жариялануға тиіс.

ӘОЖ 534.322.3.08.006.354 **МСЖ 35.040**

Түйін сөздер: ақпараттық технологиялар, ақпараттық қауіпсіздікті қорғау әдістері, бағдарламалық жасақтама, қауіптер, осалдық, құпиялылық, жауапкершілік, патч, аутентификация, мобильді құрылғылар, бағдарлама, активтер, деректер, сәйкестендіру, қолжетімділік құқықтары, криптография, шифр, қауіптіліктер, резервтік көшірме, сынау, инцидент, артықшылық, шифрлау басқару құралдары

НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

Методы и средства обеспечения безопасности

СВОД ПРАВИЛ ПО СРЕДСТВАМ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ

СТ РК ISO/IEC 27002-2015

(ISO/IEC 27002:2013 «Information technology — Security techniques — Code of practice for information security controls», IDT)

Издание официальное

**Комитет технического регулирования и метрологии
Министерства по инвестициям и развитию Республики Казахстан
(Госстандарт)**

Астана

Предисловие

1 ПОДГОТОВЛЕН И ВНЕСЕН Республиканским государственным предприятием «Казахстанский институт стандартизации и сертификации»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан от 24 ноября 2015 г. № 236-од

3 Настоящий стандарт идентичен международному стандарту ISO/IEC 27002:2013/ Cor.1:2014 «Information technology — Security techniques — Code of practice for information security controls» (Информационная технология - Методы обеспечения безопасности - Свод правил по средствам управления защитой информации), с учетом технической поправки.

Международный стандарт ISO/IEC 27002 подготовлен ОТК 1 ISO/IEC ОТК 1, *Информационные технологии,* Подкомитет ПК 27, *Методы защиты информационной безопасности.*

Перевод с английского языка (en)

Официальные экземпляры международных стандартов, на основе которых подготовлен (разработан) настоящий стандарт, и на которые даны ссылки, имеются в Едином государственном фонде нормативных технических документов

Сведения о соответствии стандартов (межгосударственных) ссылочным международным стандартам приведены в дополнительном приложении В.А.

В разделе «Нормативные ссылки» и тексте стандарта ссылочные международные стандарты актуализированы

Степень соответствия – идентичная, IDT

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2020 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Нормативные документы по стандартизации», а текст изменений и поправок – в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты»

Введение

1 Справочная информация и контекст

Настоящий стандарт разработан для организаций с целью использования в качестве документа, с помощью которого можно выбрать способы управления процессами внедрения системы менеджмента информационной безопасностью (далее - СМИБ), которая основана на ISO/IEC 27001. Также, настоящий стандарт может использоваться организациями, которые внедряют общепринятые средства управления информационной безопасностью. Настоящий стандарт предназначается для использования в руководствах по менеджменту информационной безопасности, связанной с промышленной и организационной сферой. Следует принять во внимание особый риск в сфере информационной безопасности.

Организации всех типов и масштабов (включая общественный и публичный сектора, коммерческие и некоммерческие организации) собирают, обрабатывают, хранят и передают информацию в различных форматах, таких как электронный, физический и вербальный (например, во время разговора или презентации).

Значимость информации невозможно описать словами, числами или изображениями: знания, концепции идеи и брэнды являются примерами видов информации. Информация, связанные с ней процессы, системы, сети и персональные данные, используемые в ходе операции, работа с ней и ее защита являются средствами, которые важны для бизнеса организации. Следовательно, следует осуществлять защиту информации.

Подобные средства подвергаются осознанной и случайной опасности, а соответствующие процессы, системы, сети и люди обладают врожденными слабостями. Изменения, которые происходят в деловых процессах или системах, а также внешние изменения (такие как новые законы или регламенты) могут подвергать все новой угрозе безопасности. Принимая во внимание большое количество опасностей, которые могут нанести вред организации, следует также учитывать угрозу безопасности информации. Эффективная защита информации снижает подобные риски, защищая тем самым организацию от угрозы безопасности информации и снижая влияние на вышеуказанные средства.

Безопасность информации осуществляется с помощью внедрения соответствующей группы средств управления, включая различные политики, процессы, процедуры, организационные структуры, функции программного обеспечения и функции техники. Настоящие средства управления следует установить, внедрить, отслеживать, проверять и улучшать по мере необходимости. Это позволит обеспечить соответствие деловых целей и целей безопасности организации. СМИБ типа, указанного в ISO/IEC 27001, проводит всеобъемлющий, согласованный обзор рисков системы безопасности информации, чтобы внедрить систему менеджмента безопасности информации, которая будет основана на соответствующей системе менеджмента.

Большое количество информационных систем не было разработано для защиты информации в том виде, как это изложено в ISO/IEC 27001 и настоящем стандарте. Защита, достигаемая с помощью технических средств, ограничена, поэтому ее следует поддерживать соответствующим управлением и процедурами. Чтобы понять, какой вид менеджмента подходит, следует все тщательно спланировать и уделить большое внимание деталям. Успешно внедренная СМИБ требует, помимо прочего, поддержки со стороны всех сотрудников организации. Также, может потребоваться участие заинтересованных сторон, поставщиков или других сторон. Может потребоваться совет специалиста другой стороны.

В общих чертах, эффективная защита информации обеспечивает безопасность и тщательную защиту от вреда, способствуя успешному ведению бизнеса.

2 Требования безопасности информации

Важно, чтобы организация могла определить требования безопасности. Существует 3 главных источника требований безопасности:

a. оценка рисков организации, учитывая стратегию и цели организации. С помощью оценки рисков определяется угроза средствам (активам), оценивается уязвимость, схожесть случаев и потенциальное влияние;

b. законные, законодательные и контрактные требования, которые должны удовлетворить организация, ее торговые партнеры, партнеры по контракту и поставщики услуг. Также, следует учесть социо-культурную среду;

c. группа принципов, целей и деловых требований, прилагаемые к работе с информацией, ее обработкой, хранением, распространением и архивированием. Все эти процессы разработаны организацией в помощь к осуществлению своей деятельности.

Ресурсы, используемые для внедрения систем менеджмента, должны быть способны противостоять тому вреду бизнесу, который возникает при отсутствии таковых систем менеджмента. Результаты оценки риска помогут определить соответствующие действия по управлению и выделению приоритетов по управлению рисками безопасности и внедрению систем менеджмента, которые отбираются для защиты от подобных рисков.

ISO/IEC 27005 содержит руководство по управлению информационными рисками, включая советы по оценке риска, по работе с рисками, допустимым степеням риска, по информированию о рисках. по отслеживаю рисков и обзору рисков.

3 Выбор систем менеджмента

Системы менеджмента могут быть выбраны из настоящего стандарта или из других групп управления. Также, могут быть разработаны новые системы менеджмента, чтобы соответствовать особым требованиям.

Выбор системы менеджмента зависит от решения организации, которое основано на таких критериях как приемлемость риска, воздействие на риск и общий подход управления риском. Также, решение организации должно быть принято с учетом действующего национального и международного законодательства и регламентов. Выбор системы менеджмента зависит от вида работы с системой, чтобы обеспечить защиту в глубину.

Некоторые виды управления, определенные в настоящем стандарте, могут рассматриваться в качестве руководящих принципов для управления безопасностью системы и использоваться большинством организаций. Системы менеджмента более детально изложены ниже в настоящем стандарте вместе с использованием руководства. Больше информации относительно выбора системы менеджмента и работы с рисками можно найти в ISO/IEC 27005.

4 Разработка собственных руководств

Настоящий стандарт может рассматриваться в качестве основы для разработки руководство для организации. Могут применяться не все средства управления и руководства, изложенные в настоящем своде правил. Также, могут потребоваться дополнительные средства управления и руководства, не включенные в настоящий стандарт. Если разрабатываемые документы содержат дополнительные руководства или

средства управления, то включение перекрестных ссылок может быть весьма целесообразным, чтобы способствовать соответствию, которое будет проверяться аудиторами и партнерами по бизнесу.

5 Рассуждения о жизненном цикле

Информация обладает естественным жизненным циклом: создание и происхождение посредством хранения, обработки, использования и передачи до конечного разрушения или ухудшения. Ценность средств может быть разной в течение жизненного цикла (например, несанкционированное разглашение или кража финансовых счетов компании после их публикации не так критична). Однако, информационная безопасность на некоторых стадиях носит весьма важный характер.

Информационные системы обладают жизненным циклом, в котором можно наблюдать как информация воспринимается, определяется, задумывается, разрабатывается, испытывается, внедряется, используется, сохраняется и устраняется из пользования. Информационная безопасность чрезвычайно важна на каждой стадии. Новые разработки систем и изменения к существующим системам предоставляют возможности организациям по обновлению и улучшению управления системой безопасности, принимая во внимание случаи и текущие и заметные риски информационной безопасности.

6 Стандарты, содержащие аналогичную информацию

В то время как настоящий стандарт содержит руководства по множеству систем менеджмента информационной безопасностью, которые уже применяются во многих организациях, то оставшиеся стандарты серии ISO/IEC 27000 содержат дополнительные советы или требования к другим аспектам информационной безопасности.

Серия ISO/IEC 27000 содержит общее введение в СМИБ и в настоящую серию стандартов. ISO/IEC 27000 содержит глоссарий, которые содержат термины в стандартах серии ISO/IEC 27000, и описывает область определения и цели каждого стандарта настоящей серии.

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

Методы и средства обеспечения безопасности

СВОД ПРАВИЛ ПО СРЕДСТВАМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Дата введения 2017–01–01

1 Область применения

Настоящий стандарт содержит руководство для организационных стандартов по информационной безопасности и управлению информационной безопасностью, включая отбор, внедрение и управления системами управления, принимая во внимание организационную среду информационного риска.

Настоящий стандарт разработан для организаций с целью:

a) выбора системы менеджмента в процессе внедрения СМИБ, на основе [10]

b) внедрения общепринятых систем управления информационной безопасностью;

c) разработки собственных руководств по управления информационной безопасностью.

2 Нормативные ссылки

Для применения настоящего стандарта (документа) необходимы, следующие ссылочные документы. Для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения)

ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary (Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Общий обзор и словарь)

3 Термины и определения

В настоящем стандарте применяются (используются) термины по ISO/IEC 27000.

4 Структура настоящего стандарта

Настоящий стандарт содержит 14 Разделов о системах управления безопасностью. В них насчитывается 35 главных категорий безопасности и 114 систем управления.

4.1 Разделы

Каждый раздел, содержащий определения систем управления безопасностью, содержит одну или более главных категорий безопасности.

Порядок разделов в настоящем стандарте не показывает значимость того или иного раздела. В зависимости от обстоятельств различные системы менеджмента безопасностью могут носить важный характер. Каждая организация, применяющая настоящий стандарт, должна определить системы менеджмента, их важность и их применения к отдельным деловым процессам. Также, порядок в списке, представленном в настоящем стандарте, сформирован не из-за приоритетности.

4.2 Категории систем управления

Каждая категория системы менеджмента безопасности содержит:

a) цель системы управления, в которой показывается, что следует достичь;

b) одна или более систем управления, которая применяется для достижения цели системы безопасности.

Описание системы безопасности разработано следующим образом:

Система менеджмента

Определение особой спецификации системы управления, которая соответствует цели системы управления

Руководство по внедрению систем управления

Содержит более детальную информацию, которая необходима для внедрения системы управления и соответствия цели системы управления. Руководство может не подходить или быть достаточным во всех ситуациях. Также, руководство может не способствовать выполнению особых организационных требований систем управления.

Другая информация

Содержит информацию, которую следует рассмотреть. Например, соображения о законности и ссылки к другим стандартам. Если настоящая часть отсутствует, значит не содержится подобной информации.

5 Политика безопасности информации

5.1 Управление направлением для информационной безопасности

Цель: Обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса и соответствующими законами и нормами.

5.1.1 Документирование политики информационной безопасности

Мера и средство контроля и управления

Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации и соответствующих сторонних организаций.

Рекомендация по реализации

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью.

Документ, в котором излагается политика, должен содержать положения относительно:

a) бизнес-стратегия;

b) регламенты, законы и контракты;

c) текущая и предполагаемая опасность среде информационной безопасности.

Политика информационной безопасности должна содержать положении о следующем:

a) определение информационной безопасности, целей и принципов, которые управляют всеми действиями, которые имеют отношение к информационной безопасности;

b) распределение основной и особой ответственности различным людям для управления информационной безопасностью;

c) процессы, которые способствуют работе с отклонениями и случаями исключения.

На более низком уровне политика информационной безопасности должна поддерживаться политикой топиков. С ее помощью можно способствовать внедрению систем управления информационной безопасностью. Настоящие топики разработаны таким образом, чтобы отвечать всем требованиями определенной целевой группы в рамках организации или отвечать за другие определенные топики.

Примерами подобных топиков являются:

a) управление за доступом (см. Раздел 9);

b) классификация информации (и работа с ней) (см. 8.2);

c) физическая безопасность и безопасность среды (см. Раздел 11);

d) топики, ориентированные на конечного пользователя:

1) доступное использование активов (см. 8.1.3);

2) чистый рабочий стол и экран (см. 11.2.9);

3) передача информации (см. 13.2.1);

4) мобильные устройства и телеобработка (см. 6.2);

5) ограничения по установке программного обеспечения и использования (см. 12.6.2);

e) откат системы (см. 12.3);

f) передача информации (см. 13.2);

g) защита от хакерской программы (см. 12.2);

h) управление технической уязвимостью (см. 12.6.1);

i) системы управления криптографией (см. Раздел 10);

j) защита коммуникаций (см. Раздел 13);

k) конфиденциальность и защита персональной определяемой информации (см. 18.1.4);

l) связь с поставщиком (см. Раздел 15).

Данная политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в актуальной, доступной и понятной форме. Например, в контексте «осведомленности об информационной безопасности, образования и обучающих программ» (см. 7.2.2).

Другая информация

Необходимость во внешней политики информационной безопасности различаются во всех организациях. Внутренняя политика особенно полезна в больших и сложных организациях, где определение и одобрение ожидаемых уровней систем управления отделяются от простого внедрения систем управления или от ситуаций, когда политика применяется в отношении людей или функций организации. Политика информационной безопасности может составлять часть документа по общей политике или группу отдельных документов, которые имеют общее между собой.

Некоторые организации используют другие термины для подобных документов. Например, «Стандарты», «Директивы» или «Правила».

5.1.2 Пересмотр политики информационной безопасности

Мера и средство контроля и управления

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Рекомендация по реализации

Политика информационной безопасности должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку политики безопасности. Пересмотр заключается в оценке возможностей по улучшению политики информационной безопасности организации и подхода к управлению информационной безопасностью в ответ на изменения организационной среды, обстоятельств бизнеса, правовых условий или технической среды.

При пересмотре политики информационной безопасности следует учитывать результаты пересмотров методов управления.

Должно быть получено одобрение пересмотренной политики управления.

6 Организационные аспекты информационной безопасности

6.1 Задачи, решаемые внутри организации

Цель: Осуществлять управление информационной безопасностью в рамках организации.

Мера и средство контроля и управления

Все обязанности по управлению информационной безопасностью должны быть четко определены.

Рекомендация по реализации

Распределение обязанностей по управлению информационной безопасностью следует осуществлять в соответствии с политикой информационной безопасности (см. 5.1.1). Следует четко определять обязанности по защите отдельных активов и по выполнению конкретных процессов, связанных с информационной безопасностью. Такие обязанности следует дополнять, при необходимости, более детальными руководствами для конкретных мест эксплуатации и средств обработки информации. Конкретные обязанности в отношении защиты активов и осуществления специфических процессов, связанных с безопасностью, например планирование непрерывности бизнеса, должны быть четко определены.

Лица, на которые возложена обязанность по обеспечению безопасности, могут делегировать задачи, связанные с безопасностью, другим лицам. Тем не менее, они остаются ответственными за выполнение делегированных задач.

Круг обязанностей каждого руководителя должен быть четко определен, в частности:

a) активы и процессы (процедуры) безопасности, связанные с каждой конкретной системой, должны быть четко определены;

b) необходимо назначить ответственных за каждый актив или процедуру безопасности, и подробно описать их обязанности в соответствующих документах (см. 8.1.2);

c) уровни полномочий должны быть четко определены и документально оформлены;

d) возможность выполнять обязательства в области информационной безопасности. Назначенные сотрудники должны быть конкурентоспособными в настоящей области и обладать возможностью соответствовать развитию;

e) координация и обзор аспектов информационной безопасности должны быть определены и указаны в документации.

Другая информация

Во многих организациях назначается менеджер по информационной безопасности, на которого возлагается общая ответственность за разработку и реализацию безопасности и за поддержку определения мер и средств контроля и управления.

Однако обязанности в отношении поиска ресурсов и реализации мер и средств контроля и управления часто вменяются отдельным менеджерам. Общепринятой практикой является назначение владельца для каждого актива, который несет ответственность за его повседневную защиту.

6.1.2 Отделение обязанностей

Система менеджмента

Противоречащие обязанности и области ответственности должны быть отделены, чтобы снизить возможности несанкционированного или непреднамеренного изменения или неправильного использования активов организации.

Рекомендации по реализации

Меры должны быть приняты, чтобы ни один человек не мог получить доступ, изменять или использовать активы без разрешения или обнаружения. Инициирование события следует отделить от его разрешения. Возможность сговора следует учитывать при проектировании элементов управления.

Небольшие организации могут найти разделение обязанностей слишком сложными, но принцип должен применяться по мере возможности и целесообразности. Даже, если сложно отделить, другие системы управления, такие как мониторинг деятельности, аудит и надзор управления должны быть рассмотрены.

Другая информация

Отделение обязанностей является способом снижения риска случайного или намеренного неправильного использования активов организации.

6.1.3 Контакт с различными инстанциями

Мера и средство контроля и управления

Должны поддерживаться соответствующие контакты с различными инстанциями.

Рекомендация по реализации

В организациях должны применяться процедуры, определяющие, когда и с какими инстанциями (например, правоохранительными, пожарными и надзорными органами) необходимо вступить в контакт, и каким образом следует своевременно сообщать о выявленных инцидентах информационной безопасности, если есть подозрение о возможности нарушения закона.

Дополнительная информация

Организациям, подвергающимся атаке через Интернет, может потребоваться привлечение внешней третьей стороны (например, провайдера Интернет-услуг или телекоммуникационного оператора) для принятия мер против источника атаки.

При осуществлении таких контактов может потребоваться поддержка процесса менеджмента инцидентов информационной безопасности (см. Раздел 16) или процесса планирования непрерывности бизнеса и действий в чрезвычайных ситуациях (см. Раздел 17). Также следует поддерживать контакты с регулирующими органами для прогнозирования и подготовки к предстоящим изменениям в законах или нормах, которые должны соблюдаться организацией. Контакты с другими инстанциями включают контакты с коммунальными службами, скорой помощью и службами охраны труда, например с пожарными органами (в связи с непрерывностью бизнеса), провайдерами телекоммуникационных услуг (в связи с трассировкой линий связи и их доступностью), службами водоснабжения (в связи со средствами охлаждения оборудования).

6.1.4 Мера и средство контроля и управления

Должны поддерживаться соответствующие контакты со специализированными профессиональными группами или участниками форумов по безопасности, а также с профессиональными ассоциациями.

Рекомендация по реализации

Членство в специализированных группах или форумах следует рассматривать как средство для:

a) повышения знания о «передовом опыте» и достижений информационной безопасности на современном уровне;

b) обеспечения уверенности в том, что понимание проблем информационной безопасности является современным и полным;

c) получения раннего оповещения в виде предупреждений, информационных сообщений и патчей;

d) возможности получения консультаций специалистов по вопросам информационной безопасности;

e) совместного использования и обмена информацией о новых технологиях, продуктах, угрозах или уязвимостях;

f) обеспечения адекватных точек контакта для обсуждения инцидентов информационной безопасности (см. Раздел 16).

Дополнительная информация

Могут быть установлены соглашения на совместное использование информации с целью улучшения сотрудничества и координации по вопросам безопасности. В таких соглашениях должны быть определены требования в отношении защиты чувствительной информации.

6.1.5 Информационная безопасность при управлении проектом

Системы управления

Информационная безопасность должна быть учтена при управлении проектом вне зависимости от типа проекта.

Рекомендации по реализации

Информационная безопасность должна быть интегрирована в метод управления проектом организации для обеспечения того, что риски информационной безопасности выявляются и решаются в рамках проекта. Это относится в основном к любому проекту, независимо от его характера. Например, проект для базового бизнес-процесса, IT, управления зданиями и другими вспомогательными процессами. Методы управления проектами в использовании должны требовать следующее:

a) цели информационной безопасности включаются в цели проекта;

b) проводится оценка риска информационной безопасности на ранней стадии проекта, чтобы определить необходимые системы управления;

c) информационная безопасность является частью всех фаз применяемой методологии проекта.

Последствия информационной безопасности должны быть рассмотрены и регулярно пересматриваются во всех проектах. Ответственность за информационную безопасность должна быть определена и выделены особые сотрудники, определенные в методах управления проектами.

6.2 Мобильные устройства и телеобработка

Цель: Обеспечивать безопасность телеобработки и использования мобильных устройств.

6.2.1 Политика в отношении мобильных устройств

Системы управления

Политики и поддерживающие меры безопасности должны быть приняты, чтобы управлять рисками в связи с работой мобильных устройств.

Рекомендации по реализации

При использовании мобильных устройств, особое внимание следует уделить для обеспечения того, чтобы информация о бизнесе не пострадала. Политика мобильных устройств должна принимать во внимание риски работы с мобильными устройствами в незащищенной среде.

Политика мобильных устройств должна обращать свое внимание на следующее:

a) регистрацию мобильного устройства;
b) требованиям для физической защиты;
c) ограничение по установке программного обеспечения;
d) требования к версиям программного обеспечения мобильных устройств и применяемым патчам;
e) ограничения связи с информационными услугами;
f) управление за доступом;
g) криптографические техники;
h) защиту от хакерских программ;
i) удаленное отключение, разрушение или блокировку информации;
j) откат системы;
k) использование веб-услуг и веб-приложений.

Следует соблюдать осторожность при использовании мобильных устройств в общественных местах, конференц-залах и других незащищенных местах. Защита должна быть способна избежать несанкционированного доступа или разглашения информации, хранящейся и обрабатываемой на этих устройствах. Например, с использованием криптографических методов (см. Раздел 10) и реализации использование секретной информации аутентификации (см. 9.2.4).

Мобильные устройства также должны быть физически защищены от кражи, особенно когда они потеряны. Например, в автомобилях и других видах транспорта, гостиничных номерах, конференц-центрах и местах встречи. Определенная процедура, учитывающая юридические, страховые и другие требования безопасности в организации, должна быть установлена в случае кражи или потери мобильных устройств. Устройства, обладающие важной или критической бизнес-информацией, не должны быть оставлены без присмотра. По возможности следует держать их в безопасности или использовать специальные замки для обеспечения безопасности устройства.

Обучение должно быть проведено для персонала, использующего мобильные устройства, чтобы повысить их осведомленность о дополнительных рисках, связанных с этим способом работать и системах управления, которые должны быть использованы.

Если политика мобильных устройств позволяет использовать в частной собственности мобильные устройства, то политика и связанные с ней меры безопасности должны также учитывать:

Другая политика

Соединения по беспроводным мобильным устройствам являются типами соединений связи. Однако, они обладают некоторыми различиями, которые следует учесть при определении систем управления. Различия выглядят следующим образом:

a) некоторые протоколы безопасности недостаточны и обладают некоторыми слабыми местами;
b) информация, хранящаяся на мобильных устройствах, не может быть возвращена из-за пропускной способности сети или отсутствия соединения мобильного устройства на момент запланированного возврата информации.

Мобильные устройства, как правило, имеют общие функции с фиксированными устройствами использования. Например, сети доступа в Интернет, электронная почта и обработки файлов. Управление информационной безопасности для мобильных устройств в основном состоит из тех, которые приняты в основных устройств с фиксированным

использованием и тех, которые устраняют угрозы, связанные с их использованием вне территории организации.

6.2.2 Телеобработка

Системы управления

Политика и поддерживающие меры безопасности должны быть реализованы для защиты информации, которая доступна, обработана или хранится в местах телеобработки.

Рекомендации по реализации

Организации, позволяющие телеобработку, должна разработать политику, которая определяет условия и ограничения на использование телеобработки. Если телеобработка допускается к применению и разрешена законом, то следующие вопросы должны быть рассмотрены:

a) физическая безопасность места телеобработки, принимая во внимание физическую безопасность здания и местную окружающую среду;

b) предложенная физическая среда телеобработки;

c) требования безопасности коммуникаций, принимая во внимание необходимость удаленного доступа к внутренним системам организации, восприятия информации, которая получит доступ и пройдет по линиям связи и чувствительности внутренней системы;

d) предоставление доступа к виртуальному рабочему столу, что предотвращает обработку и хранение информации на частном оборудовании;

e) угроза несанкционированными лицами несанкционированного доступа к информации или ресурсам с использованием устройств. Например, члены семьи и друзья;

f) использование домашних сетей и требований или ограничений на конфигурацию беспроводных сетевых услуг;

g) политика и процедуры для предотвращения споров, связанных с правами на интеллектуальную собственность, разработанной на частном оборудования;

h) доступ к частному оборудованию (для проверки безопасности устройства или во время расследования), которые могут быть предотвращены с помощью законодательства;

i) лицензированные соглашения о программном обеспечении из-за которых организации могут нести ответственность за лицензирование программного обеспечения клиента на рабочих станциях, принадлежащих частным сотрудникам или внешним пользователям;

j) защита от вредоносных программ и брандмауэров.

Руководящие принципы и механизмы должны содержать следующее:

a) предоставление соответствующего оборудования и мебели для хранения для устройств телеобработки, где не допускается использование частного оборудования вне контроля организации;

b) определение допустимой работы, часов работы, классификации информации, которая может быть проведена, и внутренние системы и услуги, к которым удаленный работник имеет право доступа;

c) предоставление соответствующего оборудования связи, в том числе методов обеспечения удаленного доступа;

d) физическая безопасность;

e) правила и рекомендации по вопросам доступа членов семьи и гостевого доступа к оборудованию и информации;

f) предоставление аппаратного и программного обеспечения и технического обслуживания;

g) предоставление страхования;

h) процедуры для резервного копирования и обеспечения непрерывности бизнеса;

i) аудит и мониторинг для обеспечения безопасности;

j) лишение власти и права доступа и возврат оборудования, когда прекращается работа по телеобработке.

Другая информация

Телеобработка относится ко всем формам работы за пределами офиса, в том числе нетрадиционные условия работы. Такую работу называют «дистанционной», работа «гибкого рабочего места», «удаленной работой» и «виртуальной работой».

7 Безопасность рабочего персонала

7.1 Перед трудоустройством

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осознают свои обязанности и способны выполнять предусмотренные для них роли, и снизить риск хищения, мошенничества или нецелевого использования средств обработки информации.

Меры управления

Тщательная проверка всех кандидатов на постоянную работу, подрядчиков и представителей третьей стороны должна проводиться согласно соответствующим законам, инструкциям и правилам этики, пропорционально требованиям бизнеса, классификации информации, к которой будет осуществляться доступ, и предполагаемым рискам.

Рекомендации по реализации

При проверке следует учитывать конфиденциальность, защиту персональных данных и (или) трудовое законодательство. Такая проверка должна включать следующие элементы:

a) наличие положительных рекомендаций, в частности, в отношении деловых и личных качеств претендента;

b) проверку (на предмет полноты и точности) биографии претендента;

c) подтверждение заявленного образования и профессиональной квалификации;

d) независимую проверку подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа);

e) более детальную проверку, например кредитоспособности или на наличие судимости.

Когда сотрудник принимается на работу в качестве особого специалиста по информационной безопасности, то организация должна быть уверена, что кандидат:

a) обладать соответствующей компетенцией для настоящей работы;
b) можно доверить настоящую должность, если роль особенно важна для организации.

В случаях, когда новому сотруднику непосредственно после приема на работу или в дальнейшем предоставляется доступ к средствам обработки информации, в частности, обрабатывающим чувствительную информацию, например финансовую или секретную информацию, организации следует проводить дополнительную, более детальную проверку.

Процедуры должны определять критерии и ограничения процесса проверки, например, кто имеет право проводить проверку сотрудников, каким образом, когда и с какой целью проводится эта проверка.

Предварительную проверку также следует проводить для подрядчиков и представителей третьей стороны. В тех случаях, когда подрядчики предоставляются через кадровое агентство, контракт с агентством должен четко определять обязанности агентства по предварительной проверке претендентов и процедурам уведомления, которым оно должно следовать, если предварительная проверка не была закончена, или если ее результаты дают основания для сомнения.

Информацию обо всех рассматриваемых кандидатах, претендующих на занятие должностей в организации, следует собирать и обрабатывать согласно законодательству, действующему в соответствующей юрисдикции. В зависимости от действующего законодательства, данные кандидаты должны быть предварительно проинформированы о деятельности, связанной с предварительной проверкой.

7.1.2 Условия занятости

Меры управления

В соглашения о заключении контракта между кандидатом на работу и организацией должны быть четко обозначена ответственность за информационную безопасность.

Руководство по реализации

Условия занятости должны отражать политику безопасности организации и кроме того разъяснять и констатировать:

a) что все сотрудники, подрядчики и представители третьей стороны, имеющие доступ к чувствительной информации, должны подписывать соглашение о конфиденциальности или неразглашении прежде, чем им будет предоставлен доступ к средствам обработки информации (см. 13.2.4);

b) правовую ответственность и права сотрудников, подрядчиков и любых других клиентов, например в части законов об авторском праве или законодательства о защите персональных данных (см. 18.1.2 и 18.1.4);

c) обязанности в отношении классификации информации и менеджмента активов организации, связанных с информационными системами и услугами, выполняются сотрудником, подрядчиком или представителем третьей стороны (см. Раздел 8);

d) ответственность сотрудника, подрядчика или представителя третьей стороны за обработку информации, получаемой от других фирм и сторонних организаций;

e) ответственность организации за обработку персональной информации, включая персональную информацию, полученную в результате или в процессе работы в организации (см. 7.2.3);

Организация должна обеспечивать уверенность в том, что сотрудники, подрядчики и представители третьей стороны согласны с условиями, касающимися информационной безопасности и соответствующими типу и объему доступа, который они будут иметь к активам организации, связанным с информационными системами и услугами.

При необходимости ответственность, возлагаемая на сотрудника по условиям занятости, должна сохраняться сотрудником в течение определенного периода времени и после окончания работы в организации (см. 7.3).

Дополнительная информация

Может быть использован кодекс поведения для распространения информации, касающейся обязанностей сотрудников, подрядчиков или представителей третьей стороны в отношении конфиденциальности, защиты информации, правил этики, соответствующего использования оборудования и средств организации, а также порядка деятельности. Подрядчик или представители третьей стороны могут быть связаны со сторонней организацией, с которой, в свою очередь, может потребоваться заключить договорные соглашения от имени лица, подписавшего договор.

7.2 Во время трудоустройства

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осведомлены об угрозах и проблемах, связанных с информационной безопасностью, о мере их ответственности и обязательствах, а также оснащены всем необходимым для поддержки политики безопасности организации, что снижает риск человеческого фактора.

7.2.1 Обязанности руководства

Меры управления

Руководство организации должно требовать, чтобы сотрудники, подрядчики и представители третьей стороны обеспечивали безопасность в соответствии с установленными политиками и процедурами организации.

Руководство по реализации

Руководство обязано обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны:

a) были проинформированы о своих ролях и обязанностях в области информационной безопасности прежде, чем им был предоставлен доступ к чувствительной информации или информационным системам;

b) обеспечены рекомендациями по формулированию их предполагаемых ролей в отношении безопасности в рамках организации;

c) заинтересованы следовать политикам безопасности организации;

d) достигают уровня осведомленности в отношении безопасности, соответствующего их ролям и обязанностям в организации (см. 7.2.2);

e) следуют условиям занятости, которые включают политику информационной безопасности организации и соответствующие методы работы;

f) продолжают поддерживать соответствующие навыки и квалификацию.

g) снабжены анонимной службой, которая принимает сообщения о нарушениях политики или процедур информационной безопасности («осведомление»).

Руководство должно демонстрировать поддержку политике информационной безопасности, ее процедурам и мерам управления.

Дополнительная информация

Если сотрудники, подрядчики и представители третьей стороны не были осведомлены о своих обязанностях в отношении безопасности, они могут причинить значительный ущерб организации. Заинтересованный персонал, вероятно, будет более надежным и вызовет меньше инцидентов информационной безопасности.

Неэффективный менеджмент может являться причиной того, что персонал будет чувствовать себя недооцененным, что в дальнейшем может иметь негативные последствия для организации. Например, неэффективный менеджмент может привести к игнорированию безопасности или возможному нецелевому использованию активов организации.

7.2.2 Осведомленность, обучение и тренинг в области информационной безопасности

Мера и средство контроля и управления

Все сотрудники организации и, где необходимо, подрядчики и представители третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в организации и необходимых для выполнения их рабочих функций.

Рекомендация по реализации

Обучение, обеспечивающее осведомленность, следует начинать с формального вводного процесса, предназначенного для ознакомления с политиками и ожиданиями организации в области безопасности прежде, чем будет предоставлен доступ к информации или услугам.

Программа информационной безопасности должна быть установлена в соответствии с политикой информационной безопасности организации и соответствующих процедур, принимая во внимание информацию организации, которая должна быть защищенной, и управления, которые были реализованы для защиты информации. Информационная программа должна включать в себя ряд информационно-просветительских мероприятий,

таких как кампании (например, «день информационной безопасности») и выпуск буклетов или рассылок новостей.

Информационная программа должна планироваться с учетом роли сотрудников в организации, и с учетом, какую осведомленность подрядчиков ожидает организация. Деятельность в рамках программы повышения осведомленности должна быть запланирована по истечению определенного времени. Таким образом, деятельность повторяется и позволяя принимать на работу новых сотрудников и подрядчиков. Программа информирования также должна регулярно обновляться, оставаясь в соответствии с организационной политикой и процедурами. Она должна быть построена на уроках, извлеченных из инцидентов информационной безопасности.

Обучение по осведомленности, должно быть выполнено в соответствии с требованиями программы информированности безопасности организации. Обучение по осведомленности может использовать различные средства обучения, в том числе обучение на классной основе, дистанционного обучения, веб-интерфейсом, самостоятельного и других видов обучения.

Образование по информационной безопасности и обучение должно также охватывать общие аспекты, такие как:

a) установление обязанностей организации перед информационной безопасностью;

b) необходимо ознакомиться и соблюдать правила безопасности, которые применяются с правилами информационной безопасности и обязательствами, как это определено в политике, стандартах, законах, правилах, контрактах и соглашениях;

c) личная ответственность за свои действия и бездействие, и общие обязанности по отношению к обеспечению защиты информации, принадлежащей организации и третьим сторонам;

d) основные процедуры информационной безопасности (например, сообщения об инцидентах информационной безопасности) и базовых элементах управления (например, пароля безопасности, вредоносных элементов управления и чистых рабочих столов);

e) контактные пункты и ресурсы для получения дополнительной информации и консультаций по вопросам информационной безопасности, в том числе дополнительного образования информационной безопасности и учебных материалов.

Образование по информационной безопасности и обучение должны периодически проводиться. Первоначальное образование и обучение относится к тем, кто переходит на новые позиции или роли с различными требованиями обеспечения информационной безопасности, а не только к новым сотрудникам. Обучение должно проводиться до начала трудовой занятости.

Организация должна разработать образовательные и обучающие программы для того, чтобы эффективно провести обучение и подготовку. Программа должна быть в соответствии с политикой информационной безопасности организации и соответствующими процедурами, принимая во внимание информацию организации, которая должна быть защищенной, и управление, необходимое для защиты информации. Программа должна рассматривать различные формы образования и профессиональной подготовки. Например, лекции или самостоятельные исследования.

Дополнительная информация

При разработке программы информирования, важно не только сосредоточиться на «что» и «как», но и «почему». Важно, чтобы сотрудники понимали цели информационной безопасности и потенциального воздействия, положительного и отрицательного, по организации собственного поведения.

Осведомленность, образование и обучение может быть частью, или проводится совместно, других учебных мероприятий. Например, общее обучение IT или обучение по общей безопасности. Осведомленность, образование и подготовка кадров должны быть пригодны и актуальны для должностей, обязанностей и навыков.

Оценка понимания работников может быть проведена в конце обучения и подготовки, чтобы проверить знаний.

7.2.3 Дисциплинарный процесс

Мера и средство контроля и управления

Должен существовать формальный дисциплинарный процесс, применяемый в отношении сотрудников, совершивших нарушение безопасности.

Рекомендация по реализации

Не следует начинать дисциплинарный процесс, не получив предварительного подтверждения того, что нарушение безопасности произошло (см. 16.1.7).

Формальный дисциплинарный процесс призван обеспечить уверенность в корректном и справедливом рассмотрении дел сотрудников, подозреваемых в совершении нарушений безопасности. Формальный дисциплинарный процесс следует обеспечивать для дифференцированного реагирования, учитывающего такие факторы, как тип и тяжесть нарушения и его негативное влияние на бизнес, совершено ли нарушение впервые или повторно, получил ли нарушитель должную подготовку, соответствующее законодательство, договоры в сфере бизнеса и другие факторы, если в этом есть необходимость.

Дисциплинарный процесс должен использоваться в качестве сдерживающего средства, чтобы препятствовать сотрудникам нарушать политику и процедуры организации, или наносить вред информационной безопасности. Намеренное нарушение может потребовать за собой немедленных действий.

Дополнительная информация

Дисциплинарный процесс следует также использовать как сдерживающее средство для предотвращения совершения сотрудниками, подрядчиками и представителями третьей стороны нарушений политик и процедур безопасности, принятых в организации, и каких-либо других нарушений безопасности.

7.3 Прекращение или смена занятости

Цель: Защита интересов организации, как часть процесса по изменению условий трудоустройства или по его прекращению.

7.3.1 Прекращение обязанностей

Мера и средство контроля и управления

Обязанности в отношении прекращения занятости или смены занятости должны быть четко определены и установлены.

Рекомендация по реализации

Информирование о прекращении обязанностей должно включать в себя актуальные требования безопасности и правовую ответственность, и, при необходимости, обязанности, содержащиеся в соглашении о конфиденциальности (см. 13.2.4), а также условия занятости (см. 7.1.2), продолжающие действовать в течение определенного периода времени после прекращения занятости сотрудников, подрядчиков или представителей третьей стороны.

Ответственность и служебные обязанности, продолжающие оставаться действительными после прекращения занятости, должны содержаться в договорах с сотрудниками, подрядчиками или представителями третьей стороны (см. 7.1.2).

Изменения обязанности и занятости должны управляться так же, как и прекращение соответствующей обязанности или занятости и началом новых обязанностей или занятости.

Дополнительная информация

Отдел кадров, как правило, отвечает за общий процесс прекращения занятости и действует совместно с руководителем увольняемого лица, чтобы обеспечить управление аспектами безопасности значимых процедур. В отношении подрядчика данный процесс

может быть осуществлен агентством, несущим ответственность за подрядчика, а в отношении представителя третьей стороны - его организацией.

Сотрудников, клиентов, подрядчиков или представителей третьей стороны необходимо информировать об изменениях кадрового состава и действующих договоренностей.

8 Управление активами

8.1 Ответственность за активы

Цель: Определение активов организации и соответствующих обязанностей по защите.

8.1.1 Учет активов

Меры управления

Активы, связанные с информацией и средствами, обрабатывающими информацию, должны быть определены. Перечень этих активов должен быть составлен и поддерживаться в порядке.

Рекомендации по реализации

Организация должна определять активы на соответствующих этапах циклах информации и документировать их значение. Жизненный цикл информации должен включать создание, обработку, хранение, передачу, удаление и разрушение. Документация должна поддерживаться в специальных или существующих документах учета.

Учет активов должна быть точной, актуальной и в соответствии с другими учета. Для каждого из выявленных активов, должно быть назначено право собственности на активы (см. 8.1.2) и определена классификация (см. 8.2).

Дополнительная информация

Учет активов поможет гарантировать, что осуществляется эффективная защита. Или учет активов может потребоваться для других целей, таких как здравоохранение и безопасность, страхование или финансовые (управление активами) причинам.

В [11] приводятся примеры активов, которые, возможно, необходимо рассмотреть организации при выявлении активов. Процесс составления перечня активов является важной предпосылкой управления рисками (см. также ISO/IEC 27000 и [11]).

8.1.2 Право собственности активов

Меры управления

Активы, хранящиеся в учете, должны иметь обладателя.

Рекомендации по реализации

Частные лица, а также другие лица, несущие ответственность за управление жизненным циклом активов должны быть назначены в качестве владельцев активов.

Как правило, реализуется процесс обеспечения своевременного назначения владения активами. Собственность должна быть назначена, когда активы создаются или когда активы переводятся в организации. Владелец активов должен быть ответственным за надлежащее управление активами на протяжении всего жизненного цикла активов.

Владелец активов должен:

a) обеспечить учет активов;

b) обеспечить, чтобы активы были надлежащим образом классифицированы и защищены;

c) определить и периодически пересматривать ограничения доступа и классификаций важных активов, учитывая политики ограничения доступа;

d) обеспечения надлежащего обращения, когда актив будет удален или уничтожен.

Дополнительная информация

Определенный владелец может быть либо физическим или юридическим лицом, который утверждает ответственность за управление активами в течение всего жизненного цикла. Определенный владелец не обязательно обладает правами собственности на актив.

Обычные задачи могут быть переданы, например, хранителю, который сохраняет активы на ежедневной основе, но ответственность возлагается на владельца.

В сложных информационных системах может быть полезным обозначение групп активов, которые действуют вместе, чтобы обеспечить определенную услугу. В этом случае владелец этого сервиса несет ответственность за предоставление услуги, в том числе за работу своих активов.

8.1.3 Допустимое использование активов

Меры управления

Должны быть определены, документированы и реализованы правила допустимого использования информации и активов, связанных с информацией и средствами обработки информации.

Рекомендации по реализации

Сотрудники и внешние пользователи, использующие или имеющие доступ к активам организации, должны быть осведомлены о требованиях информационной безопасности активов организации, связанных с информацией и средствами обработки информации и ресурсов. Они должны нести ответственность за их использование любых ресурсов обработки информации и любое такое использование осуществляется под их ответственность.

8.1.4 Возврат активов

Мера и средство контроля и управления

Все сотрудники, подрядчики и представители третьей стороны обязаны вернуть организации все активы, находящиеся в их пользовании, при прекращении их занятости, договора или соглашения.

Рекомендация по реализации

Процесс прекращения занятости должен быть формализован таким образом, чтобы включать в себя возврат всего ранее выданного программного обеспечения, корпоративных документов и оборудования.

В тех случаях, когда сотрудник, подрядчик или представитель третьей стороны покупает оборудование организации или использует свое собственное оборудование, необходимо следовать процедурам, обеспечивающим уверенность в том, что вся значимая информация была передана организации и удалена из оборудования безопасным образом (см. 11.2.7).

В случаях, когда сотрудник, подрядчик или представитель третьей стороны располагает знаниями, важными для продолжающихся работ, такую информацию следует оформлять документально и передавать организации.

Во время периода расторжения организация должна контролировать несанкционированное копирование актуальной информации (например, интеллектуальной собственности) уволенными сотрудниками и подрядчиками.

8.2 Классификация информации

Цель: обеспечить, что информация получает соответствующий уровень защиты в соответствии с важностью для организации.

8.2.1 Классификация информации

Меры управления

Информация должна быть классифицирована с правовой точки зрения, с точки зрения ценности, критичности и чувствительности к несанкционированному раскрытию или модификации такой информации.

Рекомендации по реализации

Классификация и связанные с ними защитные элементы управления для информации, должны учитывать потребности бизнеса для совместного использования или ограничения доступа к информации, а также юридически требования. Помимо информации, активы также могут быть классифицированы в соответствии с классификацией информации, которая подлежит хранению, обработке или защите активом.

Владельцы информационных активов должны быть подотчетны для их классификации.

Схема классификации должна включать соглашения для классификации и критерии для рассмотрения классификации с течением времени. Уровень защиты в схеме должны быть оценены с помощью анализа конфиденциальности, целостности и доступности. Схема должна быть согласована с политикой управления доступом (см. 9.1.1).

Каждый уровень получить название, что имеет смысл в контексте применения классификации схемы.

Схема должна соответствовать всей организации, так что каждый будет классифицировать информацию и связанные с ними активы в том же пути, обладать общим пониманием требований защиты и применять соответствующую защиту.

Классификация должна быть включена в процессах организации, и быть последовательна и согласованна в рамках всей организации. Результаты классификации должны указывать стоимость активов в зависимости от их чувствительности и критичности для организации. Например, с точки зрения конфиденциальности, целостности и доступности. Результаты классификации должны быть обновлены в соответствии с изменениями их стоимости, чувствительности и критичности их жизненного цикла.

Дополнительная информация

Классификация дает людям, которые занимаются информацией с кратким указанием, как обращаться и защищать ее. Создание группы информации с аналогичными потребностями защиты и определение процедур информационной безопасности, которые применяются ко всей информации в каждой группе, способствует этому. Этот подход снижает необходимость случая к случаю оценки рисков и индивидуальный дизайн элементов управления.

Информация может перестать быть чувствительной или критической по истечению определенного периода времени, например, когда информация была обнародована. Эти аспекты должны быть приняты во внимание, так как пере-классификация может привести к реализации ненужных мер управления, становясь причиной дополнительных расходов. Или наоборот, недостаточная классификация может препятствовать достижению деловых целей.

Пример схемы классификации информации о конфиденциальности может быть основан на четырех уровнях следующим образом:

a) раскрытие не вызывает никакого вреда;

b) раскрытие вызывает незначительные затруднения или незначительную оперативную неудобства;

c) раскрытие имеет значительный краткосрочное влияние на деятельность или тактические задачи;

d) раскрытие имеет серьезное влияние на долгосрочные стратегические цели или подвергает сохранение организации риску.

8.2.2 Прикрепление ярлыков к информации

Меры управления

Соответствующий набор процедур информационной маркировки должен быть развит и осуществлен в соответствии с информационной системой классификации, принятой организацией.

Руководство по реализации

Процедуры информационной маркировки должны касаться информации и связанных активов в физических и электронных форматах. Маркировка должна отразить систему классификации, установленную в 8.2.1. Ярлыки должны быть легко распознаваемыми. Процедуры должны дать указания на то, где и как ярлыки приложены, как к информации получают доступ или как активы обработаны. Процедуры могут определить случаи, где ярлык отсутствует. Например, маркировка не конфиденциальной информации, устанавливающий снижение рабочей нагрузки. Сотрудники и подрядчики должны быть осведомлены о маркировке процедур.

Продукция отличная от систем, содержащих информацию, которая классифицирована как чувствительная или важная, должна нести соответствующую маркировку классификации.

Другая информация

Маркировка секретных данных - ключевое требование для мер совместного пользования информацией. Физические этикетки и метаданные - стандартная форма маркировки.

Маркировка информации и ее связанных активов может иногда иметь отрицательные эффекты. Классифицированные активы легче определить и соответственно украсть лицами к ним доступ или внешним хакерам.

8.2.3 Обработка активов

Меры управления

Способы обработки активов должны быть разработаны и осуществлены в соответствии с информационной системой классификации, принятой организацией.

Руководство по реализации

Процедуры должны быть составлены для обработки, хранения и сообщения информации, совместимой с ее классификацией (см. 8.2.1).

Следующие пункты следует рассмотреть:

a) ограничения доступа, поддерживающие требования защиты для каждого уровня классификации;

b) обслуживание формального отчета уполномоченных получателей активов;

c) защита временных или постоянных копий информации к уровню, совместимому с защитой оригинальной информации;

d) хранение активов IT в соответствии с техническими требованиями изготовителей;

e) четкая маркировка всех копий данных к сведению уполномоченного получателя.

Система классификации, используемая в организации, может не быть эквивалентна схемам, используемым другими организациями, даже если названия уровней одинаковы; кроме того, информация, передаваемая между организациями, может измениться по классификации в зависимости от ее контекста в каждой организации, даже если их системы классификации идентичны.

Соглашения с другими организациями, которые включают совместное пользование информацией, должны включать процедуры, чтобы определить классификацию той информации и интерпретировать этикетки классификации от других организаций.

8.3 Обработка данных

Цель: предотвратить несанкционированное раскрытие, модификацию, удаление или разрушение информации, хранившей на СМИ.

8.3.1 Управление съемными носителями данных

Меры управления

Процедуры должны быть осуществлены для управления съемными носителями в соответствии с системой классификации, принятой организацией.

Руководство по реализации

Следующие рекомендации для управления съемными носителями нужно рассмотреть:

a) содержание любых повторно используемых данных, которые должны быть удалены из организации, должно быть сделано невосстанавливаемым, если больше не требуется;

b) если необходимо, разрешение должно требоваться для данных, удаленных из организации, и отчет таких удалений должен поддерживаться в порядке для ведения контрольного журнала;

c) все данные должны быть сохранены в среде, в соответствии с техническими требованиями изготовителей;

d) если конфиденциальность данных или целостность важны, то должны использоваться шифровальные методы, чтобы защитить данные на съемных носителях;

e) для снижения риска порчи данных, в то время как сохраненные данные все еще необходимы, данные должны быть перенесены на новый носитель данных прежде, чем они станут нечитаемыми;

f) многократные копии ценных данных должны быть сохранены на отдельных носителях, чтобы далее снизить риск совпадающего повреждения данных или потери;

g) регистрация съемных носителей, ограничивает возможность потери данных;

h) съемные носители должны быть позволены, если для этого есть причина;

i) при необходимости использования съемных носителей процесс переноса или передачи информации должна контролироваться.

Процедуры и уровни разрешения должны быть зарегистрированы.

8.3.2 Расположение данных

Меры управления

Данные следует надежно располагать, используя формальные процедуры.

Руководство по реализации

Формальные порядки безопасного размещения данных должны быть установлены, чтобы минимизировать риск утечки конфиденциальной информации посторонним людям. Процедуры безопасного размещения данных, содержащих конфиденциальную информацию, должны быть пропорциональны чувствительности той информации.

Следующие пункты нужно рассмотреть:

a) данные, содержащие конфиденциальную информацию, должны храниться и надежно размещаться. Например, уничтожение данных для использования проводится устройством в организации;

b) процедуры должны существовать, чтобы определить пункты, которые могли бы потребовать безопасного распоряжения;

c) может быть легче принять меры, чтобы все пункты данных были собраны и надежно размещены, вместо того, чтобы выделить важные пункты;

d) множество организаций предлагают сбор и размещение данных; следует внимательно выбирать подходящую третью сторону с надлежащим контролем и опытом;

e) размещение важных пунктов должно быть зарегистрировано для ведения контрольного журнала.

Накапливая данные для размещения, внимание должно быть уделено эффекту накопления, который может заставить большое количество конфиденциальной информации становиться важной.

Другая информация

Поврежденные устройства, содержащие уязвимые данные, могут потребовать, чтобы оценка степени риска определила, нужно ли пункты физически уничтожить, а не послать ремонт или отказаться (см. 11.2.7).

8.3.3 Физическая передача данных

Меры управления

Данные, содержащие информацию, должны быть защищены от несанкционированного доступа, неправильного употребления или коррупции во время транспортировки.

Руководство по реализации

Следующие рекомендации, помогут защищать данные, содержащие передаваемую информацию:

a) должны использоваться надежный транспорт или курьеры;

b) список уполномоченных курьеров должен быть согласован с управлением;

c) должны быть разработаны способы, для проверки идентификации курьеров;

d) упаковка должна быть достаточной, чтобы защитить содержание от любого физического повреждения во время транзита и должна соответствовать техническим требованиям любых изготовителей. Например, защита от любых факторов окружающей среды, которые могут уменьшить эффективность восстановления данных, таких как воздействие высокой температуры, влажности или электромагнитных полей;

e) регистрация должны быть сохранена, определив содержание данных, должна быть применена защита, а также запись времен передачи хранителям транзита и получения в месте назначения.

Другая информация

Информация может быть уязвима для несанкционированного доступа, неправильного употребления или может быть испорчена во время физической транспортировки. Например, посылка через почтовую службу или через курьера. В данном случае данные включают в себя печатные документы.

Когда конфиденциальная информация о данных не зашифрована, нужно рассмотреть дополнительную физическую защиту данных.

9 Управлений доступом

9.1 Деловые требования к управлению доступом

Цель: ограничить доступ к средствам для обработки информации и информации.

9.1.1 Политика управления доступом

Меры управления

Политика управления доступом должна быть установлена, зарегистрирована и рассмотрена, основываясь на работе и требованиях информационных безопасности.

Руководство по реализации

Владельцы активов должны определить соответствующие правила управления доступом, права доступа и ограничения для определенных пользовательских ролей к их активам, с количеством деталей и строгостью средств управления, отражающих связанные информационные угрозы безопасности.

Средства управления доступом (логичные и физические) (см. Раздел 11) должны быть рассмотрены вместе.

Пользователям и поставщикам услуг нужно дать четкое заявление деловых требований, которые будут соответствовать средствами управления доступом.

Политика должна принять во внимание следующее:

a) требования безопасности бизнес-приложений;

b) политика для распространения информации. Например, принцип «положено знать» и информационные уровни безопасности и классификация информации (см. 8.2);

c) последовательность между правами доступа и информационной политикой классификации систем и сетей;

d) соответствующее законодательство и любые договорные обязательства относительно ограничения доступа к данным или услугам (см. 18.1);

e) управление правами доступа в распределенной и сетевой окружающей среде, которая признает все типы доступных связей;

f) сегрегация ролей управления доступом. Например, запрос доступа, разрешение доступа, администрация доступа;

g) требования для формального разрешения запросов доступа (см. 9.2.1 и 9.2.2);

h) требования для периодического обзора прав доступа (см. 9.2.5);

i) удаление прав доступа (см. 9.2.6);

j) архивирование отчетов всех значительных событий относительно использования и управления пользовательскими личностями и секретной информацией об идентификации;

k) роли с привилегированным доступом (см. 9.2.3).

Другая информация

Необходимо соблюдать осторожность, определяя правила управления доступом для рассмотрения:

a) установление правила, основанного на предпосылке «Все запрещается, если не имеется четкого разрешения», а не на «Все разрешено, если не имеется четкого запрета»;

b) изменения в информационной маркировке (см. 8.2.2), которые начаты автоматически средствами для обработки информации, а также изменения, начатые на усмотрение пользователя;

c) изменения в пользовательских разрешениях, которые начаты автоматически информационной системой, а также изменения, начатые на усмотрение администратора;

d) правила, которые требуют определенного одобрения перед постановлением и правила, которые этого не требуют.

Правила управления доступом должны быть поддержаны формальными процедурами (см. 9.2, 9.3, 9.4), и определенными обязанности (см. 6.1.1, 9.3).

Роль, основанная на управлении доступом, является подходом, который успешно используется многими организациями, чтобы связать права доступа с деловыми ролями.

Двумя наиболее часто используемыми принципами, направляющими политику управления доступом являются:

a) Принцип «необходимость доступа к специальной информации» предоставляет доступ к информации только вам для выполнения своих задачи (различные задачи/роли означают различную необходимость и следовательно различный профиль доступа);

b) Принцип «необходимость к использованию»: только вам предоставляется доступ к средствам для обработки информации (оборудование IT, заявления, процедуры, комнаты

9.1.2 Доступ к сетям и сетевым службам

Меры управления

Пользователям нужно только предоставить доступ к сети и сетевым службам, которые предназначены для использования.

Руководство по реализации

Политика должна быть сформулирована относительно использования сетей и сетевых служб. Эта политика должна включать в себя:

a) сети и сетевые службы, которым разрешается доступ;

b) процедуры авторизации для определения, кому разрешают получить доступ к сетям и сетевым услугам;

c) административное управление и процедуры, для защиты доступа к сетевым связям и сетевым службам;

d) средства, привязанные к сетям доступа и сетевым службам (например, использование VPN или беспроводной сети);

e) пользовательские требования идентификации для доступа к различным сетевым службам;

f) контроль использования сетевых служб.

Политика в отношении использования сетевых служб должна быть совместима с политикой управления доступом организации (см. 9.1.1).

Другая информация

Несанкционированные и опасные связи с сетевыми службами, могут оказывать негативное влияние на целую организацию. Настоящая мера управления особенно важна для сетевых связей с чувствительными или критическими бизнес-приложениями или пользователями в рискованных местоположениях. Например, общественных или областях, которые находятся вне информационного управления безопасностью и контроль организации.

9.2 Пользовательское управление доступом

Цель: гарантировать доступ зарегистрированного пользователя и предотвратить несанкционированный доступ к системам и услугам.

9.2.1 Пользовательская регистрация и удаление организации

Меры управления

Формальная пользовательская регистрация и процесс удаления регистрации должны быть осуществлены, чтобы позволить установить права доступа.

Руководство по реализации

Процесс управления идентификаторами пользователей должен включать в себя:

a) использование уникальных идентификаторов пользователей, чтобы определить связь пользователей с действия и ответственностью за них; использование общих идентификаторов пользователя должно быть разрешено, только если они необходимы для бизнеса или ввиду рабочих моментов. Настоящее использование должно быть одобрено и зарегистрировано;

b) немедленное отключение или удаление идентификаторов пользователей, которые покинули организацию (см. 9.2.6);

c) периодическое определение и удаление или отключение резервных идентификаторов пользователей;

d) гарантия, что резервные идентификаторы пользователей не привязаны к другим пользователям.

Другая информация

Обеспечение или отмена доступа к информации или средствам для обработки информации обычно осуществляется в виде двухступенчатой процедуры:

a) назначение и предоставление возможности, или отмены идентификатора пользователя;

b) обеспечение или отмена прав доступа к такому идентификатору пользователя (см. 9.2.2).

9.2.2 Пользовательский обеспечивающий доступ

Меры управления

Формальный пользовательский процесс, обеспечивающий доступ, должен быть осуществлен, чтобы назначить или отменить права доступа для всех пользовательских типов ко всем системам и услугам.

Руководство по реализации

Обеспечивающий процесс для назначения или отмены прав доступа, предоставленных идентификаторам пользователей, должен включать:

a) получение разрешения от владельца информационной системы или услуги для использования информационной системы или услуги (см. мера управления 8.1.2); может потребоваться отдельное одобрение для прав доступа от управления;

b) подтверждение, что уровень предоставленного доступа соответствует политике доступа (см. 9.1) и совместим с другими требованиями, такими как разделение обязанностей (см. 6.1.2);

c) обеспечение, что права доступа не активированы (например, поставщиками услуг) перед завершением процедуры доступа;

d) поддержание централизованного отчета по правам доступа, предоставленного идентификатору пользователя для получения доступа к информационным системам и услугам;

e) согласование прав доступа пользователей, которые изменили свои роли или рабочие места, и немедленное удаление или блокирование прав доступа пользователей, которые покинули организацию;

f) периодическая проверка прав доступа с владельцами информационных систем или услуг (см. 9.2.5).

Другая информация

Внимание должно быть уделено установлению пользовательских ролей доступа, основанных на деловых требованиях, которые содержат в себе множество прав доступа в типичные пользовательские профили доступа. Запросы доступа и проверка (см. 9.2.4) легче осуществляется на подобном уровне ролей, чем на уровне особых прав.

Внимание должно быть уделено включению пунктов в контрактах сотрудников и контрактах на предоставление услуг, которые определяют штрафные санкции, если предпринимается несанкционированный доступ персоналом или подрядчиками (см. 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 Управление привилегированными правами доступа

Меры управления

Распределение и использование привилегированных прав доступа должно быть ограничено и управляемо.

Руководство по реализации

Распределение привилегированных прав доступа должно быть управляемо посредством формального процесса разрешения доступа в соответствии с соответствующей политикой управления доступом (см. контроль 9.1.1). Следует рассмотреть следующие шаги:

a) привилегированные права доступа, связанные с каждой системой или процессом, например, операционной системой, базой данных, системой управления, а также каждое применение и пользователи, которым они необходимы для распространения, должны быть определены;

b) привилегированные права доступа должны быть предназначены пользователям на основе потребности к использованию и на основе действие-за-действием в соответствии с политикой управления доступом (см. 9.1.1), т.е. основанный на минимальном требовании к их функциональным ролям;

c) должен вестись отчет о процессах разрешения и записи всех предназначенных привилегий. Привилегированные права доступа нельзя предоставить, пока процесс разрешения доступа не выполнен;

d) должны быть определены требования для истечения привилегированных прав доступа;

e) привилегированные права доступа должны быть назначены идентификатору пользователя, отличающегося от привилегий для постоянной деловой деятельности. Регулярная деловая деятельность не должна выполняться при входе с ID;

f) знания пользователей вместе с привилегированными правами доступа должны регулярно проверяться, чтобы проверить, соответствуют ли они своим обязанностям;

g) должны устанавливаться и сохраняться конкретные порядки, чтобы избежать несанкционированного использования универсальных идентификаторов администратора, согласно возможностям конфигурации систем;

h) для универсальных идентификаторов администратора конфиденциальность секретной информации об идентификации должна сохраняться при ее распространении (например, изменение паролей чаще и как можно быстрее, когда привилегированный пользователь оставляет или сменяет работу, сообщая пароли привилегированным пользователей с соответствующими механизмами).

Другая информация

Несоответствующее использование привилегий системного администрирования (любая особенность или средство информационной системы, которое позволяет пользователю игнорировать систему или средства управления) является главным фактором, который способствует неудачам или нарушениям системы.

9.2.4 Управление секретной информацией об идентификации пользователей

Меры управления

Распределением секретной информации об идентификации нужно управлять посредством формального управленческого процесса.

Руководство по реализации

Процесс должен включать следующие требования:

a) пользователи должны быть обязаны подписывать заявление, чтобы сохранить личную секретную информацию и сохранять группу (т.е. разделенный) секретной информацией об идентификации исключительно в пределах членов группы; это подписанное заявление может быть включено в положения и условия трудовой занятости (см. 7.1.2);

b) когда пользователи обязаны поддерживать свою собственную секретную информацию об идентификации, они должны быть обеспечены безопасной временной секретной информацией об идентификации', которая они должны изменить после первого использования;

c) порядки должны быть установлены, чтобы проверить личность пользователя до обеспечения новой, сменной или временной секретной информации об идентификации;

d) временная секретная информация об идентификации должна быть выдана пользователям безопасным способом; следует избегать использования услуг третьих сторон или незащищенного (открытый текст) сообщения по электронной почте;

e) временная секретная информация об идентификации должна быть уникальной для человека и должна быть надежной;

f) пользователи должны подтвердить получение секретной информации об идентификации;

g) информация об идентификации продавца по умолчанию должна быть изменена после установки систем или программного обеспечения.

Другая информация

Пароль является традиционным используемым типом секретной информации об идентификации и является общим средством подтверждения личности пользователя. Другие типы секретной информации об идентификации – криптографические ключи и другие данные, хранящиеся на носителях (например, микропроцессорная карточка), которые производят коды идентификации.

9.2.5 Обзор пользовательских прав доступа

Меры управления

Владельцы активов должны рассмотреть права доступа пользователей равномерно.

Руководство по реализации

Проверка прав доступа должна учитывать следующее:

a) права доступа пользователей должны быть рассмотрены равномерно и после любых изменений, таких как продвижение, понижение в должности или завершение занятости (см. Раздел 7);

b) пользовательские права доступа должны быть рассмотрены и перераспределены, переходя от одной роли к другой в той же самой организации;

c) разрешения для привилегированных прав доступа должны быть рассмотрены в более частых интервалах;

d) распределение привилегий должно быть проверено, чтобы гарантировать, что несанкционированные привилегии не были получены;

e) изменения привилегированных счетов должны быть зарегистрированы для периодической проверки.

Другая информация

Настоящая мера управления компенсирует возможные слабые места при реализации мер управления 9.2.1, 9.2.2 и 9.2.6.

9.2.6 Удаление или регулирование прав доступа

Меры управления

Права доступа всех сотрудников и пользователей третьей стороны к информации и средствам для обработки информации должны быть удалены по истечению их трудового договора, контракта или соглашения, либо изменены соответствующим образом.

Руководство по реализации

По истечению прав доступа к информации и активам, связанным со средствами по обработке информации и услугами обработки информации, настоящие права доступа должны быть удалены или приостановлены. Это покажет, необходимо ли удалить права доступа. Изменения трудового договора должны быть отражены при удалении всех прав доступа, которые не были одобрены для нового трудового договора. Права доступа, которые должны быть удалены или изменены, включают в себя физический и логический доступ. Удаление или изменение прав доступа может быть осуществлено удалением, аннулированием или заменой криптографических ключей, удостоверений личности, средств для обработки информации или подписок на права доступа. Любая документация, которая определяет права доступа сотрудников и подрядчиков, должна отразить удаление или изменение прав доступа. Если сотрудник, отбывающий в командировку или уходящий с должности, знает активный пароль-пользователя, то пароль должен быть изменен после завершения или смены трудовой занятости, контракта или соглашения.

Права доступа для получения информации и активов, связанных со средствами для обработки информации, должны быть уменьшены или удалены, прежде чем изменится или истечет трудовой договор в зависимости от оценки факторов риска, таких как:

a) начато ли завершение или изменение трудового договора сотрудником, пользователем третьей стороны или управлением, и причины расторжения трудового договора;

b) текущие обязанности сотрудника, пользователя третьей стороны или любого другого пользователя;

c) ценность в настоящее время доступных активов.

Другая информация

При определенных обстоятельствах права доступа могут быть распределены на основе того, что доступность необходимо большему количеству людей, чем увольняющийся сотрудник или пользователь третьей стороны. При таких обстоятельствах, увольняющиеся

сотрудники должны быть удалены из любых списков групп доступа. Следует сделать приготовлены для совета всем другим сотрудникам и пользователям третьей стороны, чтобы больше не делиться этой информацией с увольняющимся сотрудником.

В случаях расторжения трудового договора по инициативе руководства рассерженные сотрудники или пользователи третьей стороны могут сознательно испортить информацию или нанести вред средствам обработки информации. В случаях отставки или увольнения, таковые сотрудники могут собрать информацию для будущего использования.

9.3 Обязанности по пользователю

Цель: возложить ответственность пользователям за защиту их информации об идентификации.

9.3.1 Использование секретной информации об идентификации

Меры управления

Пользователи должны быть обязаны следовать методам организации в использовании секретной информации об идентификации.

Руководство по реализации

Всем пользователям нужно советовать:

a) сохранение секретной информации об идентификации, гарантируя, что она не обнародована никаким другим сторонам, включая власти;

b) избежание ведения учета (например, в бумажной варианте, файле программного обеспечения или переносном устройстве) секретной информации об идентификации, если это не может быть сохранено надежно, а метод хранения был одобрен (например, хранилище пароля);

c) изменение секретной информации об идентификации каждый раз, когда есть любой признак ее возможного взлома;

d) когда пароли используются в качестве секретной информации об идентификации, выберите качественные пароли с достаточно минимальной длиной, которые:

1) легко запомнить;

2) не основаны на чем-либо о чем можно легко догадаться или получить, используя соответствующую информацию о человеке. Например, имена, номера телефонов, даты рождения и т.д.;

3) не уязвимый для словарной атаки (т.е. не состоят из слов, включенных в словари);

4) свободный от последовательных идентичных, все-числовых или все-буквенных символов;

5) если временный, но измененный при первом входе в систему пароль;

e) не распространение секретной информации об идентификации отдельного пользователя;

f) обеспечение надлежащей защиты паролей, когда пароли будут использоваться в качестве секретной информации об идентификации в автоматизированных процедурах входа в систему и будут сохранены;

g) не использование той же самой секретной информации об идентификации для бизнеса и неделовых целей.

Другая информация

Предоставление Single Sign On (SSO – единая регистрация в сети) или других секретных инструментов управления информацией об идентификации снижает объем секретной информации об идентификации, которую пользователи обязаны защищать, таким образом повышая эффективность настоящей меры управления. Однако настоящие

инструменты могут также повысить влияние разглашения секретной информации об идентификации.

9.4 Система и прикладное управление доступом

Цель: предотвратить несанкционированный доступ к системам и заявлениям.

9.4.1 Информационное ограничение доступа

Меры управления

Доступ к функциям информационной и прикладной системы должен быть ограничен в соответствии с политикой управления доступом.

Руководство по реализации

Ограничения на доступ должны быть основаны на отдельных требованиях бизнес-приложения и в соответствии с определенной политикой управления доступом.

Следующее нужно рассмотреть, чтобы поддержать требования ограничения доступа:

a) предоставление меню, чтобы управлять доступом к функциям прикладной системы;

b) управление, к каким данным может получить доступ особый пользователь;

c) управление правами доступа пользователей, например, прочитать, написать, удалить и выполнить;

d) управление правами доступа других приложений;

e) ограничение информации содержится в продукции;

f) обеспечивая физические или логические средства управления доступом для изоляции чувствительных заявлений, данных приложения или систем.

9.4.2 Безопасные процедуры входа в систему

Меры управления

При необходимости политикой управления доступом, доступом к системам и заявлениям должна управлять безопасная процедура входа в систему.

Руководство по реализации

Должен быть выбран подходящий метод идентификации, чтобы подтвердить требуемую личность пользователя.

Где требуется строгая проверка идентификации и идентичности, альтернатива методов идентификации паролям, таким как шифровальные средства, смарт-карты, символы или биометрические средства, должны использоваться.

Должна быть разработана процедура регистрации в систему или применения, чтобы минимизироваться возможность для несанкционированного доступа. Процедура входа в систему должна раскрывать минимум информации о системе или применении, чтобы избежать предоставления неавторизованному пользователю любой ненужной помощи. Хорошая процедура входа в систему должна:

a) не показывать систему или прикладные идентификаторы, пока процесс входа в систему не был успешно закончен;

b) показать общее уведомление, предупреждающее, что к компьютеру должны только получить доступ зарегистрированные пользователи;

c) не предоставлять сообщения помощи во время процедуры входа в систему, которая помогла бы неавторизованному пользователю;

d) подтверждать информацию о входе в систему только по завершению всех входных данных. Если состояние ошибки возникает, система не должна указывать, какая часть данных правильная или неправильная;

e) защищать от попыток входа в систему грубой силы;

f) зарегистрировать неудачные и успешные попытки;

g) начинать процесс защиты, если потенциальное нарушение средств управления входом в систему обнаружено;

h) покажите следующую информацию о завершении успешного входа в систему:

1) дата и время предыдущего успешного входа в систему;

2) детали любых неудачных попыток входа в систему начиная с последнего успешного входа в систему;

i) не показывает введенный пароль;

j) не передают пароли в открытом тексте по сети;

k) закончите неработающие сессии после определенного периода бездеятельности, особенно в местоположениях высокого риска, таких как общественные зоны вне управления безопасностью организации или на мобильных устройствах;

l) ограничьте время подключения, чтобы обеспечить дополнительную безопасность для рискованных приложений и снизить вероятность несанкционированного доступа.

Другая информация

Пароли являются распространенным способом, который обеспечит идентификацию и идентификацию, основанную на тайне, которую только знает пользователь. То же самое может также быть достигнуто с шифровальными средствами и протоколами аутентификации. Сила пользовательской идентификации должна подходить для классификации информации, к которой получают доступ.

Если пароли переданы в открытом тексте во время сессии входа в систему по сети, то они могут быть захвачены сетевой программой.

9.4.3 Система управления паролем

Меры управления

Системы управления паролем должны быть интерактивными и должны гарантировать качественные пароли.

Руководство по реализации

Система управления паролем должна:

a) проводить в жизнь использование отдельных идентификаторов пользователей и паролей, чтобы поддержать отчетности;

b) позволять пользователям выбирать и изменять свои собственные пароли и включать процедуру подтверждения, чтобы допускать входные ошибки;

c) проводить в жизнь выбор качественных паролей;

d) вынуждать пользователей изменить свои пароли при первом входе в систему;

e) реализовывать регулярные изменения пароля, а также по мере необходимости;

f) ведение отчета ранее используемых паролей и предотвращения повторного использования;

g) не отображение паролей на экране, будучи введенным;

h) хранение файлов с паролями отдельно от данных о прикладной системе;

i) сохранение и передача паролей в защищенной форме.

Другая информация

Некоторые заявления требуют, чтобы пользовательские пароли были назначены независимой стороной; в таких случаях не применяются пункты b), d) и e) вышеупомянутого руководства. В большинстве случаев пароли отбираются и сохраняются пользователями.

9.4.4 Использование привилегированных утилит

Меры управления

Использование программ-утилит, которые могли бы быть способны обходить системы и управление приложений, должно быть ограничено или строго контролируемо:

Руководство по реализации

Следующие рекомендации для использования утилит, которые могли бы быть способны обходить систему и средства управления приложений, нужно рассмотреть:

a) использование идентификации, аутентификации и процедур разрешения утилит;

b) отделение утилит из прикладного программного обеспечения;

c) ограничение использования утилит к минимальному практическому числу доверяемых, разрешенных пользователи (см. 9.2.3);

d) разрешение для специального использования утилит;

e) ограничение доступности утилит, например, на время санкционированного изменения;

f) регистрация всех видов использования программ-утилит;

g) определение и документирование уровней разрешения для утилит;

h) удаление или выведение из строя всех ненужных утилит;

i) не предоставление доступа к утилитам, для пользователей, у которых есть доступ к приложениям в системах, где требуется разделение обязанностей.

Другая информация

У большинства компьютерных установок есть одна или более утилит, которые могли бы быть обойти систему или управление приложениями.

9.4.5 Управление доступом для программирования исходного кода

Меры управления

Доступ к исходному коду программы должен быть ограничен.

Руководство по реализации

Доступом к исходному коду программы и связанным пунктам (таким как проекты, технические требования, планы проверки и планы проверки) нужно строго управлять, чтобы предотвратить введение несанкционированной функциональности и избежать неумышленных изменений, а также поддержать конфиденциальность ценной интеллектуальной собственности. Для исходного кода программы это может быть достигнуто управляемым центральным хранением, предпочтительно в исходных библиотеках программы. Следующие рекомендации, как должны тогда полагать, управляют доступом к таким исходным библиотекам программ, чтобы снизить нанесения вреда компьютерным программ:

a) если это возможно, исходные библиотеки программ не должны быть проведены в эксплуатационных системах;

b) исходным кодом программы и исходными библиотеками программ= нужно управлять согласно установленным порядкам;

c) у вспомогательного персонала не должно быть неограниченного доступа для программирования исходных библиотек;

d) обновление исходных библиотек программ и соответствующих пунктов и создание исходных программ программистам должно только быть выполнено после получения соответствующего разрешения;

e) списки программ должны быть проведены в безопасной окружающей среде;

f) контрольный журнал должен сохранять все посещения к исходным библиотекам программ;

g) обслуживание и копирование исходных библиотек программ должны подвергнуться строгим процедурам контроля изменения (см. 14.2.2).

Если исходный код программы предназначен для публикации, то следует рассмотреть дополнительные средства управления для обеспечения целостности (например, электронная подпись).

10 Криптография

10.1 Шифровальные средства управления

Цель: гарантировать надлежащее и эффективное использование криптографии для защиты конфиденциальность, подлинность и/или целостность информации.

10.1.1 Политика в отношении использования шифровальных средств управления

Меры управления

Должна развиваться и внедряться политика в отношении использования шифровальных средств управления для защиты информации.

Руководство по реализации

Развивая шифровальную политику следующее нужно рассмотреть:

a) управленческий подход к использованию шифровальных средств управления по всей организации, включая общие принципы, под которыми должна быть защищена бизнес-информация;

b) основанный на оценке степени риска, необходимый уровень защиты должен быть определен, приняв во внимание тип, силу и качество требуемого алгоритма шифрования;

c) использование шифрования для защиты информации, транспортируемой устройствами мобильных или съемных носителей или через коммуникационные линии;

d) подход к ключевому менеджменту, включая методы, которые имеют дело с защитой ключей к шифру и восстановлением зашифрованной информации в случае потери, подверженности опасности или поврежденности ключей;

e) роли и обязанности, например, кто ответственен за:

1) внедрение политики;

2) ключевой менеджмент, включая ключевое поколение (см. 10.1.2);

f) стандарты, которые будут приняты для эффективного осуществления по всей организации (какое решение используется для бизнес-процесса);

g) воздействие от использования зашифрованной информации о средствах управления, которые полагаются на контроль содержания (например, вредоносное обнаружение).

Проводя шифровальную политику организации, внимание должно быть уделено инструкциям и национальным ограничениям, которые могли бы относиться к использованию шифровальных методов в различных частях мира и к проблемам потока трансбордера зашифрованной информации (см. 18.1.5).

Шифровальные средства управления могут использоваться для достижения различных информационных целей безопасности, например:

a) конфиденциальности: использование шифрования информации, чтобы защитить чувствительную или важной информации, или сохраненной или переданной;

b) целостность/подлинность: использование цифровых подписей или кодов аутентификации сообщения, чтобы проверить подлинность или целостность сохраненной или переданной чувствительной или важной информации;

c) не отказ от обязательств: использование шифровальных методов, чтобы представить свидетельства возникновения или не возникновения события или действия;

d) идентификация: использование шифровальных методов, чтобы подтвердить подлинность пользователей и других системных предприятий, запрашивающих доступ к системным пользователям, предприятиям и ресурсам или ведущих дела с указанными лицами и организациями.

Другая информация

Принятие решения относительно того, подходит ли шифровальное решение, должно выглядеть как часть более широкого процесса оценки степени риска и выбора средств управления. Настоящая оценка может тогда использоваться для определения, подходит ли шифровальное средство управления, какой контроль должен быть применен и для каких целей и деловых процессов.

Политика в отношении использования шифровальных средств управления необходима, чтобы максимизировать преимущества и минимизировать риски использования шифровальных методов и избежать несоответствующего или неправильного использования.

За советом специалиста нужно обратиться к соответствующим шифровальным средствам управления для достижения информационных целей политики безопасности.

10.1.2 Ключевой менеджмент

Меры управления

Политика в отношении использования криптографических ключей должна развиваться и внедряться в течение всего периода эксплуатации.

Руководство по реализации

Политика должна включать требования для управления ключами к шифру, хотя период их эксплуатации включает создание, хранение, архивирование, восстановление, распределение, удаление и разрушение ключей.

Шифровальные алгоритмы, длина ключа и методы использования должны быть отобраны согласно наиболее успешной практике. Соответствующее управление ключами требует безопасных процессов для создания, хранения, архивирования, восстановления, распределения, удаления и разрушения ключей к шифру.

Все ключи к шифру должны быть защищены от модификации и потери. Кроме того, секретные и частные ключи нуждаются в защите от несанкционированного использования, а также раскрытия. Оборудование, используемое для производства, сохранения и архивирования ключей, должно быть физически защищено.

Система управления ключами должна быть основана на согласованном наборе стандартов, процедур и безопасных методов для:

a) создания ключей для различных шифровальных систем и различных приложений;

b) издания и получения сертификатов открытого ключа;

c) распределение ключей предназначенным для этого предприятиям, включая то, как ключи должны быть активированы после их получения;

d) хранение ключей, включая то, как зарегистрированные пользователи получают доступ к ключам;

e) изменение или обновление ключей, включая правила, когда ключи должны будут быть изменены и как это будет сделано;

f) работа с ключами, которые находятся под угрозой;

g) отмена ключей, включая то, как ключи должны быть отозваны или дезактивированы, например, когда ключи находились под угрозой или когда пользователь покидает организацию (когда ключи должны быть заархивированы);

h) восстановление ключей, которые потеряны или испорчены;

i) поддержка или архивирование ключей;

j) разрушение ключей;

k) регистрация и ревизия действий, связанных с управлением ключами.

Для снижения вероятности неправильного использования, даты активации и даты дезактивации ключей должны быть определены так, чтобы ключи могли только использоваться в течение промежутка времени, определенного в соответствующей политике по управлению ключами.

В дополнение к надежно руководящим секретным и частным ключам нужно также рассмотреть подлинность открытых ключей. Настоящий процесс идентификации может быть произведен, используя свидетельства открытого ключа, которые обычно выпускаются органом сертификации, который должен быть признанной организацией с подходящими средствами управления и процедурами для обеспечения необходимого уровня доверия.

Содержание соглашений о сервисном обслуживании или контрактов с внешними поставщиками шифровальных услуг, например, с органом сертификации должны охватывать проблемы ответственности, надежности услуг и времени, затраченного для предоставления услуг (см. 15.2).

Другая информация

Управление ключами к шифру важно для эффективного использования шифровальных методов.

[2][3][4] предоставля.т дополнительную информацию об управлении ключами.

Шифровальные методы могут также использоваться для защиты ключей к шифру. Процедуры, возможно, должны быть рассмотрены для того, чтобы обработать юридических запросов для доступа к ключам к шифру, например, зашифрованная информация может потребоваться в качестве доказательства в судебном процессе.

11 Физическая и экологическая безопасности

11.1 Безопасная зона

Цель: предотвратить несанкционированный физический доступ, повреждение и вмешательство к информации организации и средствам для обработки информации.

11.1.1 Периметр физической защиты

Меры управления

Периметры безопасности должны определяться и использоваться для защиты области, которые содержат или чувствительную или критическую информацию и средства для обработки информации.

Руководство по реализации

Следующие рекомендации нужно рассмотреть и осуществить в соответствующих случаях для периметров физической защиты:

a) периметры безопасности должны быть определены, и расположение и сила каждого из периметров должны зависеть от требований безопасности активов в пределах периметра и результатов оценки степени риска;

b) периметры здания или места, содержащего средства по обработке информации, должны быть физически адекватными (т.е. отсутствие промежутков в периметре или областях, где легко может произойти взлом); внешняя крыша, стены и пол места должны быть надежно сконструированы, а все внешние двери должны быть соответственно защищены от несанкционированного доступа (например, средства препятствий, тревоги, замки); двери и окна должны быть заперты, когда внешнюю защиту следует рассмотреть для окон, особенно на уровне земли;

c) должна существовать соответствующая приемная или другие средства для управления физическим доступом на сайт или зданием; доступ к местам и зданиям должен быть ограничен уполномоченным персоналом;

d) физические препятствия должны быть построены, чтобы предотвратить несанкционированный физический доступ и экологическое загрязнение;

e) все пожарные двери на периметре безопасности, должны быть в режиме безопасности, проверены и проверены вместе со стенами для установления необходимого уровня сопротивления в соответствии с подходящими региональными, национальными и международными стандартами; они должны работать в соответствии с местными нормами пожарной безопасности;

f) подходящие системы обнаружения злоумышленника должны быть установлены на национальных, региональных или международных стандартах и регулярно проверяться для защиты всех внешних дверей и доступных окон; пустые зоны должны находиться в режиме безопасности; защита должна быть обеспечена для других зон, например, компьютеров, комнат или комнат для различных обсуждений;

g) средства для обработки информации, которыми управляет организация, должны быть физически отделены от тех, которыми управляют третьи стороны.

Другая информация

Физическая защита может быть достигнута, создав один или несколько физических барьеров вокруг помещения организации и средств обработки информации. Использование многократных барьеров дает дополнительную защиту, где неудача единственного барьера не означает, что безопасность немедленно ставится под угрозу.

Безопасная зона может быть блокируемым офисом или несколькими комнатами, окруженными непрерывным внутренним барьером физической защиты. Дополнительные барьеры и периметры, необходимые для управления физическим доступом, могут быть необходимы между областями с различными требованиями безопасности в периметре безопасности. Особое внимание к физической безопасности доступа должно быть уделено в случае зданий, держащих активы для большого количества организаций.

Применение физических средств управления, особенно для безопасных зон, должно быть адаптировано к технической и экономической ситуации организации, как указано в оценке степени риска.

11.1.2 Физические средства управления входом

Меры управления

Безопасные зоны должны быть защищены соответствующими средствами управления входом, чтобы гарантировать, что только уполномоченному персоналу разрешается доступ.

Руководство по реализации

Следующие рекомендации нужно рассмотреть:

a) дата и время входа и отъезда посетителей должна быть зарегистрирована, и все посетители должны контролироваться, если их доступ не был ранее одобрен; им нужно только предоставить доступ в определенных, санкционированных целях и нужно выпустить с инструкциями относительно требований безопасности области и чрезвычайных мер. Личность посетителей должна быть заверена соответствующим средством;

b) доступ к областям, где конфиденциальная информация обрабатывается или хранится, должен быть ограничен уполномоченными людьми только после внедрения соответствующих средств управления доступом, например, внедрение механизма двухфакторной аутентификации, такие как карта доступа и секретный PIN;

c) физический журнал учета или электронный контрольный журнал всего доступа должен надежно охраняться и проверяться;

d) все сотрудники, подрядчики и третьи стороны должны быть обязаны носить некоторую форму видимой идентификации и должны немедленно уведомить персонал службы безопасности, если они сталкиваются с несопровождаемыми посетителями и людьми без видимой идентификации;

e) персоналу службы поддержки третьей стороны нужно предоставить ограниченный доступ, чтобы охранять территории или средства по обработке конфиденциальной информации только при необходимости; этот доступ должен быть разрешен и проверен;

f) права доступа для безопасной зоны должны регулярно рассматриваться и обновляться и отменяться (см. 9.2.5 и 9.2.6).

11.1.3 Защита офисов, комнат и средств

Меры управления

Физическая защита для офисов, комнат и средств должна быть разработана и применена.

Руководство по реализации

Следующие рекомендации, как должны полагать, обеспечивают офисы, комнаты и средства:

a) средства по работе с ключами должны быть размещены во избежание общественного доступа;

b) здания должны быть незаметными и минимально указывать на цель своего строения, без очевидных знаков внутри или снаружи здания, которые отображают действия по обработке информации;

c) средства должны формироваться таким образом, чтобы препятствовать тому, чтобы конфиденциальная информация или действия были видимыми и слышимыми с внешней стороны. Электромагнитное ограждение нужно также рассмотреть;

d) справочники и внутренние телефонные книги, определяющие местоположения средств по обработке конфиденциальной информации, не должны быть доступны для неавторизованных лиц.

11.1.4 Защита от внешних и экологических угроз

Меры управления

Физическая защита от стихийных бедствий, вредоносная атака или несчастные случаи должны быть разработаны и применены.

Руководство по реализации

Совет специалиста должен быть получен относительно, как избежать повреждения от огня, наводнения, землетрясения, взрыва, общественных беспорядков и других форм стихийного бедствия или техногенной катастрофы.

11.1.5 Работа в безопасной зоне

Меры управления

Процедуры для работ в безопасной зоне должен быть разработаны и применены.

Руководство по реализации

Следующие рекомендации следует рассмотреть:

a) персонал должен знать о существовании, или деятельности в пределах безопасной зоны на основе необходимых данных;

b) следует избегать безнадзорной работы в безопасной зоне из соображений безопасности и предотвратить возможности злонамеренных действий;

c) свободные зоны безопасности должен быть физически закрыты и периодически проверяться;

d) фотографическое, видео, аудио или другое записывающее оборудование, такие как камеры в мобильных устройствах, не разрешается проносить на территорию безопасной зоны, если не получено разрешение.

Меры для работы в безопасной зоне включают в себя средства управления для сотрудников и пользователей третьей стороны, работающих в безопасной зоне, и они учитывают все действия, которые осуществляются в безопасной зоне.

11.1.6 Место поставки и погрузки

Меры управления

Точками доступа, такими как зоны поставки и погрузки, где посторонние люди могли войти в помещение, нужно управлять и изолировать от средств обработки информации, чтобы избежать несанкционированного доступа.

Руководство по реализации

Следующие рекомендации следует рассмотреть:

a) доступ к зоне поставки и погрузки, находящейся за пределами здания, должен быть ограничен определенным и уполномоченным персоналом;

b) область доставки и погрузки должна быть разработана так, чтобы поставки могли быть загружены и разгружены без персонала доставки, получающего доступ к другим частям здания;

c) внешние двери зоны поставки и погрузки должны быть закрыты, когда внутренние двери открыты;

d) поступающий материал должен быть осмотрен и исследован на взрывчатые вещества, химикаты или другие опасные материалы, прежде чем он будет перемещен из зоны поставки и погрузки;

e) поступающий материал должен быть зарегистрирован в соответствии с процедурами управления активами (см. пункт 8) или при входе на территорию;

f) поступающие и коммуникабельные поставки должны быть физически отделены;

g) поступающий материал должен быть осмотрен для доказательств вмешательства в пути. Если такое вмешательство обнаружено, оно должно быть немедленно сообщено персоналу службы безопасности.

11.2 Оборудование

Цель: предотвратить потерю, повреждение, воровство или компромисс активов и прерывания к действиям организации.

11.2.1 Расположение оборудования и защита

Меры управления

Оборудование должно быть расположено и защищено для снижения риска от экологических угроз и опасностей и возможностей для несанкционированного доступа.

Руководство по реализации

Следующие рекомендации помогут защищать оборудование:

a) оборудование должно быть расположено для минимизирования ненужного доступа в рабочие области;

b) средства обработки информации, обрабатывающие уязвимые данные, должны быть тщательно расположить для снижения риск раскрытия информации несанкционированным персоналом;

c) должны быть склады во избежание несанкционированного доступа;

d) оборудование, требующее специальной защиты, должно быть предоставлено для снижения общего уровня требуемой защиты;

e) средства управления должны быть приняты для минимизирования риска потенциальных физических и экологических угроз, например, воровство, огонь, взрывчатые вещества, дым, вода (или проблемы с водоснабжением), пыль, вибрация, химические эффекты, вмешательство электропитания, коммуникационное вмешательство, электромагнитная радиация и вандализм;

f) рекомендации для еды, питья и курения в близости к средствам обработки информации должны быть установлены;

g) условия окружающей среды, такие как температура и влажность, должны быть проверены для условий, которые могли оказать негативное влияние на обработку средств обработки информации;

h) защита от молний должна быть применена ко всем зданиям и фильтры защиты молнии должны быть приспособлены к любой поступающей мощности и коммуникационным линиям;

i) использование методов специальной защиты, таких как клавишные мембраны, нужно рассмотреть для оборудования в промышленных средах;

j) оборудование, обрабатывающее конфиденциальную информацию, должно быть защищено для минимизирования риска утечки информации из-за электромагнитного испускания.

11.2.2 Поддержка коммунальных услуг

Меры управления

Оборудование должно быть защищено от перебоев в питании и других нарушениях, вызванных трудностями в поддержке коммунальных услуг.

Руководство по реализации

Поддержка коммунальных услуг (например, электричество, телекоммуникации, водоснабжение, газ, сточные воды, вентиляция и кондиционирование воздуха) должна:

a) соответствовать техническим требованиям производителя оборудования и местным законным требованиям;

b) регулярно оценивать их возможности соответствия деловому росту и взаимодействию с другими коммунальными услугами;

c) регулярно проверяться и проходить испытания, чтобы гарантировать надлежащее функционирование;

d) быть в режиме охраны для обнаружения сбоев;

e) при необходимости, обладать большим количеством линий передач с различными физическими доступами.

Должны быть обеспечены аварийное освещение и коммуникации. Аварийные выключатели и переключатели для отключения электричества, воды, газа или других коммунальных услуг должны быть расположены около комнат оборудования или запасных выходов.

Другая информация

Дополнительная избыточность для сетевого соединения может быть получена посредством многократных маршрутов больше чем от одного сервисного поставщика.

11.2.3 Безопасность кабелей

Меры управления

Телекоммуникационные кабели и кабели питания, которые несут в себе данные или услуги дополнительной информации, должны быть защищены от перехвата, вмешательства или повреждения.

Руководство по реализации

Нужно рассмотреть следующие рекомендации для защиты кабелей:

a) кабели питания и телекоммуникационные кабели в средствах обработки информации должны находиться под покрытием, либо рассмотреть альтернативную защиту;

b) силовые кабели должны быть отдельными от коммуникационных кабелей для предотвращения помех;

c) для чувствительных или критических систем дальнейшие средства управления для рассмотрения включают в себя:

1) установка бронированного трубопровода и запертых комнат или коробок при контроле и пунктах завершения;

2) использование электромагнитного ограждения для защиты кабелей;

3) инициирование технических зачисток и физических проверок для несанкционированных устройств, бывших присоединенных к кабелям;

4) контролируемый доступ чтобы для защиты панелей и кабельных комнат

11.2.4 Обслуживание оборудования

Меры управления

Оборудование должно правильно сохраняться, чтобы гарантировать его длительную доступность и целостность.

Руководство внедрения

Следующие рекомендации для обслуживания оборудования нужно рассмотреть:

a) оборудование должно сохраняться в соответствии с рекомендуемыми сервисными интервалами и техническими требованиями поставщика;

b) только уполномоченный персонал обслуживания должен выполнить сервисное оборудование и ремонт;

c) учет нужно вести всех подозреваемых или фактических ошибок, и всего профилактического и корректирующего обслуживания;

d) соответствующие средства управления должны быть осуществлены, когда оборудование намечено для обслуживания, приняв во внимание, выполнено ли это обслуживание персоналом на территории или внешнее к организации; в случае необходимости, конфиденциальная информация должна быть очищена от оборудования, или персонал обслуживания должен быть достаточно очищен;

e) должны быть выполнены все требования к обслуживанию, наложенные страховыми полисами;

f) прежде, чем ввести оборудование в эксплуатацию назад после его обслуживания, это должно быть осмотрено, чтобы гарантировать, что в оборудование не вмешались и не работает со сбоями.

11.2.5 Удаление активов

Меры управления

Оборудование, информация или программное обеспечение не должны быть взяты вне рабочего без предшествующего разрешения.

Руководство по реализации

Следующие рекомендации нужно рассмотреть:

a) должны быть опознаны сотрудники и пользователи третьей стороны, у которых есть полномочия разрешить удаление активов удаленным способом;

b) сроки для удаления актива должны быть установлены, а их восстановление должно быть проверено на соответствие;

c) в случае необходимости, активы должны быть зарегистрированы как удаленные с удаленного доступа и зарегистрированы, когда они восстановлены;

d) идентичность, роль и подключение к делу любого, кто обращается или использует активы, должны быть зарегистрированы, и настоящая документация возвращается вместе с оборудованием, информацией или программным обеспечением.

Другая информация

Выборочные проверки, предпринятые для обнаружения несанкционированного удаления активов, могут также быть выполнены, для обнаружения несанкционированных устройств записи, оружия, и т.д., и предотвращения их входов. Такие выборочные проверки должны быть выполнены в соответствии с соответствующим законодательством и инструкциями. Люди должны быть проинформированы, что выборочные проверки уже выполнены. Проверки должны быть выполнены с разрешением, подходящим для законных и нормативных требований.

11.2.6 Безопасность оборудования и активов вне помещения

Меры управления

Безопасность должна быть применена к удаленным активам, принимающим во внимание различные риски работы близ помещения организации.

Руководство по реализации

Использование любого информационного хранения и технологического оборудования возле помещения организации должно быть разрешено управлением. Это относится к оборудованию, принадлежавшему организации и частному оборудованию, которое используется от имени организации.

Следующие рекомендации нужно рассмотреть для защиты удаленного оборудования:

a) оборудование и данные, которые получены вне территории организации, не должны быть оставлены без присмотра в общественных местах;

b) инструкции изготовителей для защиты оборудования должны проверяться в любом случае, например, защита от воздействия сильных электромагнитных полей;

c) средства управления для рабочих мест вне организации, таких как надомная работа, удаленные и временные места должны быть определены оценкой степени риска и подходящими средствами управления. Например, запирающиеся шкафы для хранения

документов, ясная политика стола, средства управления доступом для компьютеров и безопасная связь с офисом (см. также [15][16][17][18][19]);

d) когда оборудование вне помещения распространено среди различных людей или третьих сторон, регистрация должна сохраняться, которая позволит определить имена и организации тех, кто ответственен за оборудование.

Риски, например, повреждения, воровство или подслушивания, могут измениться значительно между местоположениями и должны быть приняты во внимание в определении самых соответствующих средств управления.

Другая информация

Информационное хранение и технологическое оборудование включают все формы персональных компьютеров, организаторов, мобильных телефонов, смарт-карт, бумаги или другой формы, которая необходима для домашней работы или для транспортировки с обычного местоположения работы.

Больше информации о других аспектах защиты мобильного оборудования можно найти в 6.2.

Уместным может быть избежание риска, поясняя сотрудникам риски удаленной работы или ограничивая их использование портативного оборудования IT;

11.2.7 Безопасное распоряжение или повторное использование оборудования

Меры управления

Все оборудование, содержащее носители данных, должно быть проверено, чтобы гарантировать, что любые уязвимые данные и лицензированное программное обеспечение было удалены или надежно переписано до распоряжения или повторного использования.

Руководство по реализации

Оборудование должно быть проверено, чтобы гарантировать, содержатся ли носители данных до распоряжения или повторного использования.

Носители данных, содержащие конфиденциальную или защищенную авторским правом информацию, должны быть физически разрушены, или информация должна быть разрушена, удалена, или переписана с помощью техник, которые делают оригинальную информацию невосстановимой вместо того, чтобы использовать удаленный стандарт.

Другая информация

Поврежденное оборудование, содержащее носители данных, может потребовать, чтобы оценка степени риска определила, нужно ли пункты физически уничтожить, а не послать ремонт или отказаться. Информация может быть распространена из-за небрежного распоряжения или повторного использования оборудования.

Кроме того, чтобы обеспечить дисковое стирание, шифрование целого диска снижает риск раскрытия конфиденциальной информации, когда от оборудования избавляются или повторно развертывают, при условии, что:

a) процесс шифрования достаточно силен и покрывает весь диск (включая слабое пространство, файлы обмена, и т.д.);

b) ключи шифрования достаточно длинны, чтобы сопротивляться атаке грубой силы;

c) ключи шифрования самостоятельно сохраняют конфиденциальным образом (например, никогда не хранятся на том же самом диске).

Для дальнейшей информации относительно шифрования см. Раздел 10.

Методы для надежной переписи носителей данных отличаются согласно технологии носителей данных.

Переписывание инструментов должно быть рассмотрено, чтобы удостовериться, что они применимо к технологиям носителей данных.

11.2.8 Оставленное без присмотра пользовательское оборудование

Меры управления

Пользователи должны гарантировать, что у оставленного без присмотра оборудования есть соответствующая защита.

Руководство по реализации

Все пользователи должны знать о требованиях безопасности и процедурах защиты оставленного без присмотра оборудования, а также их обязанностей по осуществлению такой защиты. Пользователям нужно советовать:

a) завершить активные сессии по завершению работы, если они не могут быть обеспечены соответствующим механизмом блока, например, защищенным паролем скринсейвером;

b) выход из приложений или сетевых служб по истечению надобности;

c) защитить компьютеры или мобильные устройства от несанкционированного использования с помощью блокировки клавиш или эквивалентным контролем, например, доступом пароля, если не используется.

11.2.9 Политика чистого стола и чистого экрана

Меры управления

Должны быть принята политика чистого стола для бумаг и сменных носителей данных и политика чистого экрана для средств обработки информации.

Руководство по реализации

Политика чистого стола и чистого экрана должны принять во внимание информационные классификации (см. 8.2), юридические и договорные требования (см. 18.1), и соответствующие риски и культурные аспекты организации. Следующие рекомендации нужно рассмотреть:

a) чувствительная или критическая бизнес-информация, например, на бумаге или на электронных носителях данных, должна быть заперта (идеально в сейфе или в кабинете или других формах мебели безопасности) особенно когда офис освобожден.

b) следует выполнить выход из компьютера или терминалов или защитить экраном и клавишным механизмом захвата, которым управляет пароль, знаком или аналогичным пользовательским механизмом идентификации, когда не проводится работа и должен быть защищен замками, паролями или другими средствами управления если не используется;

c) несанкционированное использование фотокопировальных устройств и другой технологий воспроизводства (например, сканеры, цифровые фотоаппараты) должно быть предотвращено;

d) информация, содержащая чувствительные или секретные данные, должна быть немедленно удалены из принтеров.

Другая информация

Политика чистого стола и чистого экрана снижает риск несанкционированного доступа, потерю и повреждение информации в течение рабочего времени и по его истечению. Сейфы или другие формы безопасных складов могли бы также защитить информацию, хранившую там против бедствий, таких как огонь, землетрясение, наводнение или взрыв.

Рассмотрите использование принтеров с функцией PIN-кода, таким образом, организаторы являются единственными, которые могли получить их распечатки, стоя рядом с принтером.

12 Операционная безопасность

12.1 Эксплуатационные процедуры и обязанности

Цель: гарантировать правильные и безопасные операции средств для обработки информации.

12.1.1 Зарегистрированные рабочие процессы

Меры управления

Рабочие процессы должны быть зарегистрированы и стать доступными для всех пользователей, которым они нужны.

Руководство по реализации

Зарегистрированные процедуры должны быть подготовлены к эксплуатационным действиям, связанным со средствами обработки информации и коммуникациями, такими как компьютерный запуск и процедуры завершения работы, резервная копия, обслуживание оборудования, обработка информации, компьютерная комната и обработка корресподенции и безопасность.

Рабочие процессы должны определить эксплуатационные инструкции, включая:

a) установка и конфигурация систем;

b) обработка и автоматизированная и ручная обработка информации;

c) резервная копия (см. 12.3);

d) планирование требований, включая взаимозависимости с другими системами, самым ранним началом работы и последним часом завершения работы;

e) инструкции для ошибок из-за неправильного обращения или других исключительных условий, которые могли бы возникнуть во время выполнения работы, включая ограничения на использование системных утилит (см. 9.4.4);

f) контакты поддержки и подъема включая внешнюю поддержку связываются в случае неожиданных эксплуатационных или технических трудностей;

g) инструкции к особому производству и обработке данных, таких как использование специальной канцелярской бумаги или управление конфиденциальной продукцией включая, процедуры безопасного избавления от продукции с неудавшихся рабочих мест (см. 8.3 и 11.2.7);

h) системный перезапуск и процедуры восстановления использования в случае системного отказа;

i) управление контрольным журналом и системной информацией о регистрации (см. 12.4);

j) процедуры контроля.

Рабочие процессы и зарегистрированные процедуры системных действий нужно рассматривать как формальные документы и изменения, разрешенные управлением. Где технически выполнимо, информационными системами нужно последовательно управлять, используя те же самые процедуры, инструменты и утилиты.

12.1.2 Управление изменениями

Меры управления

Нужно управлять изменениями организации, бизнес-процессов, средств для обработки информации и систем, которые затрагивают информационную безопасность.

Руководство внедрения

В частности следующие пункты нужно рассмотреть:

a) идентификация и запись существенных изменений;

b) планирование и тестирование изменений;

c) оценка потенциальных воздействий, включая информационные воздействия безопасности, таких изменений;

d) формальная процедура одобрения предложенных изменений;

e) проверка, что информационные требования безопасности соответствуют;

f) сообщение об изменениях передаются всем соответствующим людям;

g) процедуры отступления, включая процедуры и обязанности по прерыванию и восстановлению от неудачных изменений и непредвиденных событий;

h) предоставление процесса чрезвычайного изменения, чтобы позволить быстрое и контролируемое внедрение изменений, необходимое для решения всех инцидентов (см. 16.1).

Формальные управленческие функции и процедуры должны существовать, чтобы гарантировать удовлетворительный контроль всех изменений. Когда изменения внесены, контрольный журнал, содержащий всю актуальную информацию, должен быть сохранен.

Другая информация

Несоответствующий контроль изменений средств обработки информации и систем - частая причина неудач безопасности или системы. Изменения рабочей среды, особенно от стадии передачи к стадии работы, могут повлиять на надежность заявлений (см. 14.2.2).

12.1.3 Полное управление

Меры управления

Использование ресурсов должно быть проверено и настроено. Должен быть разработан план будущего полного управления, чтобы гарантировать необходимую системную работу.

Руководство по реализации

Требования управления должны быть определены, приняв во внимание деловую критичность заинтересованной системы. Системная настройка и контроль должны быть применены для гарантии улучшения доступности и эффективности систем. Детективные средства управления должны находиться на положенном месте, чтобы указать на проблемы в срок. Планы будущих требований управления должны принять во внимание новые деловые и системные требования и текущие и спроектированные тенденции в возможностях обработки информации организации.

Особое внимание должно быть обращено на любые ресурсы с долгим временем выполнения заказа приобретения или высокой стоимостью; поэтому менеджеры должны контролировать использование ключевых системных ресурсов. Они должны определить тенденции в использовании, особенно относительно инструментов управления информационных систем или бизнес-приложений.

Менеджеры должны использовать эту информацию, чтобы определить и избежать потенциальных препятствий и зависимости от ведущих специалистов, которые могли бы представить угрозу безопасности системы или услугам, и запланировать соответствующие меры.

Обеспечение достаточной способности может быть достигнуто, увеличив способность или уменьшив требование. Примеры руководящего полного требования включают:

a) удаление устаревших данных (дисковое пространство);

b) списывание заявлений, систем, баз данных или окружающей среды;

c) оптимизация серийных производств и графиков;

d) оптимизация прикладной логики или вопросов базы данных;

e) отрицание или ограничение полосы пропускания для голодных ресурса услуг, если это не важный бизнес (например, вытекание видео).

Зарегистрированный полный план управления нужно рассматривать для систем с непрерывным доступом к данным.

Другая информация

Этот контроль также обращается к способности человеческих ресурсов, а также офисам и средствам.

12.1.4 Разделение развития, тестирования и рабочих сред

Меры управления

Развитие, тестирование и рабочие среды должны быть отделены, чтобы снизить риск несанкционированного доступа или изменений рабочей среды.

Руководство по реализации

Уровень разделения между рабочими, испытательными и средами развития, необходимыми для предотвращения эксплуатационных проблем, должен быть определены и внедрен.

Следующие пункты нужно рассмотреть:

a) правила для передачи программного обеспечения от разработки до эксплуатации должны быть определены и зарегистрированы;

b) развитие и эксплуатационное программное обеспечение должны управляться на различных системах или компьютерных процессорах и в различных областях или справочниках;

c) изменения эксплуатационных систем и заявлений должны быть проверены в тестировании или организации окружающей среды до того, чтобы быть примененным к эксплуатационным системам;

d) кроме как при исключительных обстоятельствах, тестирование не должно быть проведено на эксплуатационных системах;

e) компиляторы, редакторы и другие средства разработки или системные программы не должны быть доступны для эксплуатационных систем;

f) пользователи должны использовать различные профили пользователя для эксплуатационных и проверяющих систем, и меню должны показать соответствующие идентификационные сообщения, чтобы снизить риск ошибки;

g) уязвимые данные не должны быть скопированы в системную окружающую среду тестирования, если эквивалентные средства управления не обеспечены для системы тестирования (см. 14.3).

Другая информация

Развитие и действия тестирования могут вызвать серьезные проблемы, например, нежелательную модификацию файлов или системной окружающей среды или системного отказа. Есть потребность поддержать известную и стабильную окружающую среду, в которой можно выполнить значащее тестирование и предотвратить несоответствующий доступ разработчика к рабочей среде.

Если сотрудники по развитию и проведению испытаний обладают доступом к эксплуатационной системе и ее информации, то они могут быть в состоянии ввести несанкционированный и непроверенный кодекс или изменить рабочие данные. На некоторых системах эта способность могла неправильно использоваться, чтобы совершить мошенничество или ввести непроверенный или вредоносный код, который может вызвать серьезные эксплуатационные проблемы.

Персонал по развитию и проведению испытаний также ставит под угрозу конфиденциальность эксплуатационной информации.

Развитие и действия тестирования могут вызвать непреднамеренные изменения программного обеспечения или информации, если они разделяют ту же самую вычислительную окружающую среду. Отделение развития, тестирование и рабочих сред поэтому желательны, чтобы снизить риск случайного изменения или несанкционированного доступа к эксплуатационному программному обеспечению и коммерческой информации (см. 14.3 для защиты данных испытаний).

12.2 Защита от вредоносного программного обеспечения

Цель: гарантировать, что информация и средства для обработки информации защищены от вредоносного программного обеспечения.

12.2.1 Средства управления против вредоносного программного обеспечения

Меры управления

Обнаружение, предотвращение и средства управления восстановлением, чтобы защитить от вредоносного программного обеспечения, должны быть осуществлены вместе с соответствующей пользовательской осведомленностью.

Руководство по реализации

Защита от вредоносного программного обеспечения должна быть основана на вредоносном программном обеспечении обнаружения и восстановительном программном обеспечении, информационной осведомленности безопасности и соответствующем системном доступе и средствами управления изменениями. Следующее руководство нужно рассмотреть:

a) установление формальной политики, запрещающей использование несанкционированного программного обеспечения (см. 12.6.2 и 14.2.);

b) внедрение управления, которое предотвращает или обнаруживает использование несанкционированного программного обеспечения (например, приложение по списку лиц, прошедших проверку безопасности);

c) осуществление средств управления, которое предотвращает или обнаруживает использование известных или подозрительных вредоносных веб-сайтов (например, помещение в черный список);

d) установление формальной политики для защиты от рисков, связанных с получением файлов и программного обеспечения, либо из внешних сетей, либо через внешние сети или на любом другом средстве, указывая на то, какие защитные меры должны быть приняты;

e) сокращение слабых мест, которые могли эксплуатироваться вредоносным программным обеспечением, например, через техническое управление уязвимостью (см. 12.6);

f) проведение регулярных обзоров программного обеспечения и содержания данных систем, поддерживающих важные деловые процессы; присутствие любых неутвержденных файлов или несанкционированных поправок должно быть формально исследовано;

g) установка и регулярное обновление вредоносного программного обеспечения обнаружения и восстановления, чтобы просмотреть компьютеры и данные в качестве предупредительного контроля, или на обычной основе; сканирование должно включать:

1) просмотрите любые файлы, полученные по сетям или через любую форму носителя данных для вредоносного программного обеспечения перед использованием;

2) просмотрите приложения электронной почты и загрузки для вредоносного программного обеспечения перед использованием; этот просмотр должен быть выполнен в различных местах, например, в серверах электронной почты, настольных компьютерах и при входе в сеть организации;

3) веб-страницы просмотра для вредоносного программного обеспечения;

h) определение процедур и обязанностей для работы с вредоносной защитой на системах, обучением в их использовании, сообщая и восстанавливая после вредоносных нападений;

i) подготовка соответствующих планов обеспечения непрерывности бизнеса для восстановления от вредоносных нападений, включая все необходимые данные и резервную копию программного обеспечения и меры восстановления (см. 12.3);

j) использование процедур, чтобы регулярно собирать информацию, такую как подписка на списки рассылки или подтверждение веб-сайтов, дающих информацию о новом вредоносном программном обеспечении;

k) осуществление процедур, чтобы проверить информацию, касающуюся вредоносного программного обеспечения и гарантировать, что бюллетени предупреждения точны и информативны; менеджеры должны гарантировать, что квалифицированные источники, например, известные журналы, надежная защита программного обеспечения производства сайтов или поставщиков от вредоносного программного обеспечения, используются, чтобы

различать между обманами и реальным вредоносным программным обеспечением; все пользователи должны знать о проблеме обманов и что сделать по их получению;

l) изоляция окружающей среды, где катастрофические воздействия могут закончиться.

Другая информация

Использование двух или более защитного программного обеспечения против вредоносного программного обеспечения через информационную среду от различных продавцов и технологии может улучшить эффективность вредоносной защиты.

Необходимо соблюдать осторожность, чтобы защитить от введения вредоносного программного обеспечения во время обслуживания и чрезвычайных процедур, которые могут обойти нормальные вредоносные средства управления защитой.

При определенных условиях вредоносная защита могла бы вызвать волнение в рамках операций.

Использование одного только вредоносного программного обеспечения обнаружения и ремонта как вредоносный контроль обычно не соответствует и обычно должно сопровождаться рабочими процессами, которые предотвращают введение вредоносного программного обеспечения.

12.3 Резервная копия

Цель: защищать от потери данных.

12.3.1 Информационная резервная копия

Меры управления

Резервные копии информации, программного обеспечения и системных изображений должны быть сделаны и регулярно проверяться в соответствии с согласованной резервной политикой.

Руководство по реализации

Резервная политика должна быть установлена, чтобы определить требования организации для резервной копии информации, программного обеспечения и систем.

Политика резервной копии должна определить требования защиты и сохранение.

Соответствующие резервные услуги должны быть предоставлены, чтобы гарантировать, что вся существенная информация и программное обеспечение могут быть восстановлены после отказа системы хранения данных или бедствия.

Проектируя резервный план, следующие пункты должны быть учтены:

a) должны быть составлены точные и полные отчеты резервных копий и зарегистрированные процедуры восстановления;

b) степень (например, полная или отличительная резервная копия) и частота резервных копий должна отразить деловые требования организации, требования безопасности включенной информации и критичность информации к длительной деятельности организации;

c) резервные копии должны быть сохранены в отдаленном местоположении на достаточном расстоянии, чтобы избежать любого повреждения от нарушений на главном месте;

d) резервной информации нужно дать соответствующий уровень физической защиты и охраны окружающей среды (см. пункт 11), совместимый со стандартами, примененными на главном месте;

e) резервные данные должны регулярно проверяться, чтобы гарантировать, что на них можно положиться для использования в крайнем случае; это должно быть объединено с тестом процедур восстановления и проверено против требуемого времени восстановления. Тестирование способности восстанавливать поддержанные данные должно быть выполнено на специальных испытательных данных, не переписывая оригинальные данные в случае,

если процесс резервной копии или восстановления подводит и наносит непоправимый ущерб данным или их потерю;

f) в ситуациях, где конфиденциальность имеет значение, резервные копии должны быть защищены посредством шифрования.

Эксплуатационные процедуры должны контролировать выполнение резервных копий и направлять ошибки запланированных резервных копий, чтобы гарантировать полноту резервных копий согласно политике резервных копий.

Резервные меры для отдельных систем и услуг должны регулярно проверяться, чтобы гарантировать, чтобы они отвечали требованиям планов обеспечения непрерывности бизнеса. В случае критических систем и услуг, резервные меры должны включать всю информацию о системах, заявления и данные, необходимые, чтобы возвратить полную систему в случае бедствия.

Период сохранения для существенной деловой информации должен быть определен, приняв во внимание любое требование для копий архива, которые будут постоянно сохранены.

12.4 Регистрация и контроль

Цель: сделать запись событий и произвести доказательства.

12.4.1 Регистрация событий

Меры управления

Журналы событий, делающие запись пользовательских действий, исключений, ошибок и информационных событий безопасности, должны быть произведены, сохранены и регулярно рассматриваться.

Руководство по реализации

Журналы событий должны включать актуальные:

a) идентификаторы пользователей;

b) системные действия;

c) даты, времена и детали ключевых событий, например, вход в систему и выход;

d) идентичность устройства или местоположение, если возможно, и системный идентификатор;

e) отчеты успешных и отклоненных системных попыток доступа;

f) отчеты успешных и отклоненных данных и других попыток доступа ресурса;

g) изменения системной конфигурации;

h) использование привилегий;

i) использование системных программ и заявлений;

j) файлы получения доступа и вид доступа;

k) сетевые адреса и протоколы;

l) тревоги, поднятой системой управления доступом;

m) активация и дезактивация систем защиты, таких как антивирусные системы и системы обнаружения вторжения;

n) отчеты сделок выполнены пользователями в заявлениях.

Регистрация событий закладывает основу автоматизированных систем мониторинга, которые способны к созданию сводных отчетов и тревог системы безопасности.

Другая информация

Журналы событий могут содержать уязвимые данные и личные данные. Соответствующие меры по обеспечению секретности должны быть приняты (см. 18.1.4).

Если возможно, то у системных администраторов не должно быть разрешения стереть или дезактивировать журналы их собственных действий (см. 12.4.3).

12.4.2 Защита информации о регистрации

Меры управления

Регистрация средств и информации о регистрации должна быть защищена от вмешательства и несанкционированного доступа.

Руководство по реализации

Средства управления должны стремиться защищать от несанкционированных изменений, чтобы зарегистрировать информацию и эксплуатационные проблемы с регистрирующимся средством, включая:

a) изменения к типам сообщения, которые зарегистрированы;

b) файлы системного журнала, отредактированные или удаленные;

c) вместимость превышаемых данных файла системного журнала, приводя или к отказу сделать запись событий или к переписыванию прошлых зарегистрированных событий.

Некоторые контрольные журналы могут потребоваться, чтобы быть заархивированными как часть рекордной политики задержания или из-за требований, чтобы собрать и сохранить доказательства (см. 16.1.7).

Другая информация

Системные регистрации часто содержат большой объем информации, большая часть которой посторонняя для информационного контроля состояния безопасности. Чтобы помочь определить значительные события в информационных целях контроля состояния безопасности, копирование соответствующего сообщения печатается автоматически во второй регистрации, или использование подходящих программ систем или контрольных инструментов, чтобы выполнить запрос файла и рационализацию следует рассмотреть.

Системные регистрации должны быть защищены, потому что, если данные могут быть изменены или данные в них удалены, то их существование может создать ложное ощущение безопасности. Копирование в реальном времени регистраций к системе вне контроля системного администратора или оператора может использоваться, чтобы охранять регистрации.

12.4.3 Администратор и регистрации оператора

Меры управления

Системный администратор и системные действия оператора должны быть зарегистрированы, а регистрации защищены и регулярно проверяемы.

Руководство по реализации

Привилегированные держатели учетной записи пользователя могут быть в состоянии управлять входом в систему средств для обработки информации под их прямым управлением, поэтому необходимо защитить и рассмотреть регистрации, чтобы поддержать ответственность для привилегированных пользователей.

Другая информация

Система обнаружения вторжения, которая управляется за пределами контроля системы и сетевых администраторов, может использоваться, чтобы контролировать системное администрирование и действия администрирования сети для соответствия.

12.4.4 Синхронизация часов

Меры управления

Часы всех обрабатывающих актуальную информацию систем в организации или домене безопасности должны быть синхронизированы единственному справочному источнику времени.

Руководство по реализации

Должны быть зарегистрированы внешние и внутренние требования для представления времени, синхронизации и точности. Такие требования могут быть юридическими, регулирующими, договорными требованиями, соблюдением стандартов или требованиями для внутреннего контроля. Должно быть определено стандартное справочное время для использования в организации.

Подход организации к получению справочного времени из внешнего источника (ов) и как синхронизировать внутренние часы достоверно должен быть зарегистрирован и осуществлен.

Другая информация

Правильная настройка компьютерных часов важна, чтобы гарантировать точность контрольных журналов, которые могут требоваться для расследований или как доказательства в юридических или дисциплинарных случаях. Неточные контрольные журналы могут препятствовать таким расследованиям и повредить доверию таким доказательствам. Часы, связанные с радио-передачей времени от национальных атомных часов, могут использоваться в качестве основных часов для регистрации систем. Сетевой протокол времени может использоваться, чтобы держать все серверы в синхронизации с основными часами.

12.5 Контроль эксплуатационного программного обеспечения

Цель: гарантировать целостность эксплуатационных систем.

12.5.1 Установка программного обеспечения на эксплуатационных системах

Меры управления

Процедуры должны быть осуществлены, чтобы управлять установкой программного обеспечения на эксплуатационных системах.

Руководство по реализации

Следующие рекомендации, как должны полагать, управляют изменениями программного обеспечения на эксплуатационных системах:

a) обновление эксплуатационного программного обеспечения, приложений и библиотек программы должно быть выполнено только обученными администраторами на соответствующее управленческое разрешение (см. 9.4.5);

b) эксплуатационные системы должны содержать одобренный выполняемую программу, а не код развития или компиляторы;

c) приложения и программное обеспечение операционной системы должны только быть осуществлены после обширного и успешного тестирования; тесты должны включать удобство использования, безопасность, эффекты на другие системы и легкость в использовании и должны быть выполнены на отдельных системах (см. 12.1.4); следует знать, что все соответствующие библиотеки источников программ были обновлены;

d) система управления конфигурации должна использоваться, чтобы удержать контроль над всем осуществленным программным обеспечением, а также системной документацией;

e) стратегия обратной перемотки должна существовать, прежде чем изменения осуществлены;

f) контрольный журнал должен состоять из всех обновлений эксплуатационных библиотек программы;

g) предыдущие версии прикладного программного обеспечения должны быть сохранены как мера по непредвиденному обстоятельству;

h) старые версии программного обеспечения должны быть заархивированы, вместе со всей запрошенной информацией и параметрами, процедурами, деталями конфигурации и программным обеспечением поддержки столько, сколько данные сохранены в архиве.

Поставляемое программное обеспечение продавца, используемое в эксплуатационных системах, должно сохраняться на уровне, поддержанном поставщиком. В течение долгого времени продавцы программного обеспечения прекратят поддерживать более старые версии программного обеспечения. Организация должна рассмотреть риски доверия неподдержанному программному обеспечению.

Любое решение по обновлению до нового выпуска должно принять во внимание деловые требования для изменений и безопасности выпуска, например, введения новой информационной функциональности безопасности или числа и серьезности информационных проблем безопасности, затрагивающих эту версию. Участки программного обеспечения должны быть применены, когда они могут помочь удалить или уменьшить информационные слабые места безопасности (см. 12.6).

Физическому или логическому доступу нужно предоставлять поставщикам только в целях поддержки, когда необходимо и с управленческим одобрением. Действия поставщика должны быть проверены (см. 15.2.1).

Программное обеспечение может полагаться на внешнее поставляемое программное обеспечение и модули, которые нужно проверить и управлять ими, чтобы избежать несанкционированных изменений, которые могли стать причиной слабых мест безопасности.

12.6 Техническое управление уязвимостью

Цель: предотвратить эксплуатацию технических слабых мест.

12.6.1 Управление техническими слабыми местами

Меры управления

Информация о технических слабых местах, используемых информационными системами, должна быть получена своевременно, воздействие организации таких слабых мест должна быть оценена и соответствующие меры должны быть приняты, чтобы работать со связанным риском.

Руководство по реализации

Текущий и полный перечень активов (см. Раздел 8) является предпосылкой для эффективного технического управления уязвимостью. Определенная информация должна была поддержать техническое управление уязвимостью, включая программное обеспечение продавца, номера версий, текущее состояние развертывания (например, какое программное обеспечение установлено на какой системы), и человека (людей) в организации, ответственной за программное обеспечение.

Соответствующие и своевременные меры должны быть приняты в ответ на идентификацию потенциальных технических слабых мест. Следующее руководство должно сопровождаться, чтобы установить эффективный управленческий процесс для технических слабых мест:

a) организация должна определить и установить роли и обязанности, связанные с техническим управлением уязвимостью, включая контроль уязвимости, оценку степени риска уязвимости, внесение исправлений, прослеживание актива и любые требуемые обязанности по координации;

b) информационные ресурсы, которые будут использоваться, чтобы определить соответствующие технические слабые места и поддержать осведомленность о них, должны быть определены для программного обеспечения и других технологий (основанные на списке активов, см. 8.1.1); эти информационные ресурсы должны быть обновлены, основанные на изменениях в списке или когда найдены другие новые или полезные ресурсы;

c) график времени должен быть определен, чтобы реагировать на уведомления о потенциально соответствующих технических слабых местах;

d) как только потенциальная техническая уязвимость была определена, организация должна определить связанные риски и действия, которые будут предприняты; такое действие могло включить внесение исправлений уязвимых систем или применение других средств управления;

e) в зависимости от того, как срочно должна быть обращена техническая уязвимость, принятые меры должны быть выполнены согласно средствам управления, связанным с

управлением изменениями (см. 12.1.2), или выполняя информационные процедуры реагирования на инциденты безопасности (см. 16.1.5);

f) если участок доступен из законного источника, риски, связанные с установкой участка, должны быть оценены (угрозы, представляемые уязвимостью, должны быть сравнены с риском установки участка);

g) участки должны быть проверены и оценены, прежде чем они будут установлены, чтобы гарантировать, что они эффективны и не приводят к побочным эффектам, которые не могут быть допущены; если никакой участок не доступен, нужно рассмотреть другие средства управления, такие как:

1) выключение услуг или возможностей, имеющих отношение к уязвимости;

2) адаптация или добавление средств управления доступом, например, брандмауэров на сетевых границах (см. 13.1);

3) увеличенный контроль, чтобы обнаружить фактические атаки;

4) повышение осознания уязвимости;

h) контрольный журнал должен быть сохранен для всех предпринятых процедур;

i) технический процесс управления уязвимостью должен регулярно проверяться и оцениваться, чтобы гарантировать его эффективность и эффективность;

j) системы с высоким риском должны быть обработаны в первую очередь;

k) эффективный технический управленческий процесс уязвимости должен быть выровнен с управленческими действиями инцидента, чтобы сообщить данные по уязвимости для функции реагирования на инциденты и обеспечивают, а технические процедуры, которые будут выполнены;

l) определите процедуру для работы с ситуацией, где уязвимость была определена, но нет никакой подходящей контрмеры. В этой ситуации организация должна оценить риски, касающиеся известной уязвимости, и определить соответствующие детективные и корректирующие действия.

Другая информация

Техническое управление уязвимостью может быть рассмотрено как подфункция управления изменениями, и как таковой может использовать в своих интересах процессы управления изменениями и процедуры (см. 12.1.2 и 14.2.2).

Продавцы часто являются объектом значительного давления, чтобы выпустить патчи (обновления) как можно скорее. Поэтому, есть возможность, что участок не решает проблему, соответственно и имеет отрицательные побочные эффекты. Кроме того, в некоторых случаях удаление патча не может быть легко достигнуто, как только патч был применен.

Если соответствующее тестирование участков невозможно, например, из-за затрат или отсутствия ресурсов, задержка внесения исправлений, как могут полагать, оценивает связанные риски, основанные на опыте, о котором сообщают другие пользователи. Использование [14] может быть выгодным.

12.6.2 Ограничения на установку программного обеспечения

Меры управления

Правила, управляющие установкой программного обеспечения пользователями, должны быть установлены и внедрены.

Руководство по реализации

Организация должна определить и реализовать строгую политику, на которую могут быть установлены типы программного обеспечения.

Принцип наименьшего количества привилегий должен быть применен. Если предоставлены определенные привилегии, у пользователей может быть способность установить программное обеспечение. Организация должна определить то, какие типы установок программного обеспечения разрешены (например, обновления и участки

безопасности к существующему программному обеспечению) и каковы типы установок запрещены (например, программное обеспечение, которое является только для личного использования и программного обеспечения, происхождение которого относительно того, чтобы быть потенциально злонамеренным неизвестна или подозрительна). Эти привилегии нужно предоставить, учтя роли заинтересованных пользователей.

Другая информация

Регулярная установка программного обеспечения на вычислительных устройствах может привести к представлению слабых мест и затем к утечке информации, потере целостности или других информационных инцидентов безопасности, или к нарушению прав на интеллектуальную собственность.

12.7 Соображения аудита информационных систем

Цель: минимизировать воздействие контрольных действий по эксплуатационным системам.

12.7.1 Средства управления аудитом информационных систем

Меры управления

Контрольные требования и действия, включающие проверку эксплуатационных систем, должны быть тщательно запланированы и согласованы, чтобы минимизировать разрушения к бизнес-процессам.

Руководство по реализации

Следующие рекомендации должны наблюдаться:

a) контрольные требования для доступа к системам и данным должны быть согласованы с соответствующим управлением;

b) объем технических аудиторских тестов нужно согласовать и управлять;

c) аудиторские тесты должны быть ограничены доступом только для чтения к программному обеспечению и данным;

d) доступ кроме только для чтения должен быть позволен только для изолированных копий системных файлов, которые должны быть стерты, когда аудит закончен или придать соответствующую защиту, если есть обязательство держать такие файлы под контрольными требованиями документации;

e) требования для специальной или дополнительной обработки должны быть определены и согласованы;

f) аудиторскими тестами, которые могли затронуть системную доступность, нужно управлять вне рабочего времени;

g) весь доступ должен быть проверен и зарегистрирован, чтобы произвести справочный след.

13 Безопасность коммуникаций

13.1 Управление сетевой безопасностью

Цель: обеспечивать защиту информации в сетях и ее средствах для обработки информации поддержки.

13.1.1 Сетевые средства управления

Контроль

Сетями нужно управлять, чтобы защитить информацию в системах и заявлениях.

Руководство по реализации

Средства управления должны быть осуществлены, чтобы гарантировать безопасность информации в сетях и защите связанных услуг от несанкционированного доступа. В частности следующие пункты нужно рассмотреть:

a) обязанности и процедуры для управления сетевым оборудованием должны быть установлены;

b) эксплуатационная ответственность за сети должна быть отделена от компьютерных операций (см. 6.1.2);

c) специальные средства управления должны быть установлены, чтобы охранять конфиденциальность и целостность данных, передающих по общедоступным сетям или по беспроводным сетям и защитить связанные системы и заявления (см. пункт 10 и 13.2); специальные средства управления могут также потребоваться, чтобы поддерживать доступность сетевых служб и связанных компьютеров;

d) соответствующая регистрация и контроль должны быть применены, чтобы позволить делать запись и обнаружение действий, которые могут затронуть или относятся к информационной безопасности;

e) управленческие действия должны быть хорошо скоординированы, чтобы оптимизировать обслуживание организации и гарантировать, что средства управления последовательно применяются через инфраструктуру обработки информации;

f) системы в сети должны быть заверены;

g) связь систем с сетью должна быть ограничена.

Другая информация

Дополнительная информация о сетевой безопасности может быть найдена в [15][16][17][18][19]

13.1.2 Безопасность сетевых служб

Меры управления

Механизмы безопасности, сервисное обслуживание и управленческие требования всех сетевых служб должны быть определены и включены в соглашения сетевых служб, предоставлены ли эти услуги в помещении или вне его.

Руководство по реализации

Способность поставщика сетевой службы управлять согласованными услугами безопасным способом должна быть определена и регулярно проверяться, а право проверки должно быть согласовано.

Меры безопасности, необходимые для особых услуг, таких как механизмы безопасности, сервисное обслуживание и управленческие требования, должны быть определены. Организация должна гарантировать, чтобы поставщики сетевой службы осуществили эти меры.

Другая информация

Сетевые службы включают предоставление связей, услуг частной сети и оценивают добавленные сети и решения для сетевой безопасности, которыми управляют, такие как брандмауэры и системы обнаружения вторжения. Эти услуги могут колебаться от простой неуправляемой полосы пропускания до сложных предложений с добавленной стоимостью.

Механизмы безопасности сетевых служб могли быть:

a) технологии, применяемые для безопасности сетевых служб, таких как идентификация, шифрование и сетевые средства управления связью;

b) технические параметры, требуемые для обеспеченной связи с сетевыми службами в соответствии с безопасностью и сетевыми правилами связи;

c) процедуры использования сетевой службы, чтобы ограничить доступ к сетевым службам или заявлениям, в случае необходимости.

13.1.3 Разделение в сетях

Меры управления

Группы информационных услуг, пользователей и информационных систем должны быть отдельными в сетях.

Руководство по реализации

Один метод управления безопасностью больших сетей должен разделить их на отдельные сетевые области. Могут быть выбраны области, основанные на уровнях доверия (например, область открытого доступа, настольная область, область сервера), вдоль организационных единиц (например, человеческие ресурсы, финансы, маркетинг) или некоторая комбинация (например, область сервера, соединяющаяся с многократными организационными единицами). Разделение может быть осуществлено, используя также физически различные сети или при помощи различных логических сетей (например, частная виртуальная сеть).

Периметр каждой области должен быть хорошо определен. Доступ между сетевыми областями разрешен, но нужно управлять в периметре, используя межсетевой интерфейс (например, брандмауэр, фильтруя маршрутизатор). Критерии разделение сетей на домены должны быть основаны на оценке требований безопасности каждой области. Оценка должна быть в соответствии с политикой управления доступом (см. 9.1.1), требованиями доступа, стоимостью и классификацией обработанной информации и также принимая во внимание относительную стоимость и исполнительное воздействие слияния подходящего межсетевого перехода.

Беспроводные сети требуют специального режима из-за плохо определенного сетевого периметра. Для чувствительной окружающей среды соображение должно быть сделано о рассмотрении всего беспроводного доступа, как внешние связи, и выделять этот доступ от внутренних сетей, пока доступ не прошел через межсетевой интерфейс в соответствии с сетевой политикой средств управления (см. 13.1.1) прежде, чем предоставить доступ к внутренним системам.

Идентификация, шифрование и пользовательские технологии управления доступом сети уровня современных, основанных на стандартах беспроводных сетях могут быть достаточными для прямой связи с внутренней сетью организации, когда должным образом осуществлено.

Другая информация

Сети часто простираются вне организационных границ, поскольку деловые партнерства сформированы, которые требуют соединения или обмена информацией обрабатывающих и сетевые средств. Такие расширения могут увеличить риск несанкционированного доступа к информационным системам организации, которые используют сеть, некоторые из которых требуют защиты от других сетевых пользователей из-за их чувствительности или критичности.

13.2 Информационная передача

Цель: поддержать безопасность информации, которая передается внутри организации и любому внешнему предприятию.

13.2.1 Информационная политика передачи и процедуры

Меры управления

Формальная политика передачи, процедуры и средства управления должны существовать, чтобы защитить передачу информации с помощью всех типов средств коммуникации.

Руководство по реализации

Процедуры и средства управления, которые будут сопровождаться, используя средства для коммуникации для информационной передачи, должны рассмотреть следующие пункты:

a) процедуры, разработанные, чтобы защитить переданную информацию от перехвата, копирования, модификации, неправильного направления и разрушения;

b) процедуры обнаружения и защиты от вредоносного программного обеспечения, которое может быть передано с помощью электронных средств связи (см. 12.2.1);

c) процедуры защиты сообщенной чувствительной электронной информации, которая находится в форме приложения;

d) политика или рекомендации, обрисовывающие в общих чертах приемлемое использование средств для коммуникации (см. 8.1.3);

e) персонал, третья сторона и обязанности любого другого пользователя не поставить под угрозу организацию, например, через клевету, преследование, олицетворение, отправление писем счастья, несанкционированную покупку, и т.д.;

f) использование шифровальных методов, например, защищать конфиденциальность, целостность и подлинность информации (см. Раздел 10);

g) задержание и рекомендации по распоряжению для всей деловой переписки, включая сообщения, в соответствии с соответствующим национальным и местным законодательством и инструкциями;

h) средства управления и ограничения, связанные с использованием средств для коммуникации, например, автоматическим отправлением электронной почты к внешним почтовым адресам;

i) уведомление персоналу принять соответствующие меры предосторожности, чтобы не показать конфиденциальную информацию;

j) не отправляющиеся сообщения, содержащие конфиденциальную информацию об автоответчиках, т.к. они могут быть повторены посторонними людьми, хранящиеся на коммунальных системах или хранящиеся неправильно в результате неправильного набора адреса;

k) уведомление персоналу о проблемах использования фототелеграфных аппаратов или услуг, а именно:

1) несанкционированный доступ к встроенным архивам сообщений, чтобы восстановить сообщения;

2) умышленное или случайное программирование машин, чтобы послать сообщения в определенные числа;

3) отправка документов и сообщений к неправильному числу или неправильному набору или использованием неправильного сохраненного числа.

Кроме того, персоналу нужно напомнить, что у них не должно быть конфиденциальных разговоров в общественных местах или по опасным каналам связи, открытым офисам и местам для собраний.

Информационные услуги по передаче должны выполнить любые соответствующие законные требования (см. 18.1).

Другая информация

Информационная передача может произойти с помощью многих различных типов средств коммуникации, включая электронную почту, голосовое сообщение, факсимиле и видео сообщение.

Передача программного обеспечения может произойти через многие различные среды, включая загрузку с Интернета и приобретение от продавцов, продающих стандартные продукты.

Деловые, законные и защитные значения, связанные с электронным обменом данными, электронной торговлей и электронными средствами связи и требованиями для средств управления, нужно рассмотреть.

13.2.2 Соглашения по информационной передаче

Меры управления

Соглашения должны обратиться к безопасной передаче бизнес-информации между организацией и третьими сторонами.

Руководство по реализации

Информационные соглашения о передаче должны включить следующее:

a) управленческие функции по управлению и уведомлению передачи, отправки и получения;

b) процедуры, чтобы гарантировать отслеживаемость и не отказ от обязательств;

c) минимальные технические стандарты для упаковки и передачи;

d) соглашения об условном депонировании;

e) идентификационные стандарты курьера;

f) обязанности и обязательства в случае информационных инцидентов безопасности, таких как потеря данных;

g) использование согласованной системы маркировки для чувствительной или критической информации, гарантируя, что значение ярлыков немедленно понято и что информация соответственно защищена (см. 8.2);

h) технические стандарты для записи и чтения информации и программного обеспечения;

i) любые специальные средства управления, которые требуются, чтобы защищать чувствительные пункты, такие как криптография (см. Раздел 10);

j) поддержание цепи заключения для получения информации, которая находится в пути;

k) допустимые уровни управления доступом.

Политика, процедуры и стандарты должны устанавливаться и сохраняться, чтобы защитить информацию и физическую среду в пути (см. 8.3.3), и должен быть сослан в таких соглашениях о передаче.

Информационное содержание безопасности любого соглашения должно отразить чувствительность включенной бизнес-информации.

Другая информация

Соглашения могут быть электронными или ручными, и могут принять форму формальных контрактов. Для конфиденциальной информации определенные механизмы, используемые для передачи такой информации, должны быть последовательными для всех организаций и типов соглашений.

13.2.3 Электронная передача сообщений

Меры управления

Информация, вовлеченная в электронную передачу сообщений, должна быть соответственно защищена.

Руководство по реализации

Информационные соображения безопасности для электронной передачи сообщений должны включать следующее:

a) защиту сообщений от несанкционированного доступа, модификации или отказа в обслуживании, соразмерного с системой классификации, принятой организацией;

b) обеспечение правильного обращения и транспортировки сообщения;

c) надежность и доступность обслуживания;

d) юридические соображения, например требования для электронных подписей;

e) получение одобрения до использования внешних социальных услуг, таких как мгновенный обмен сообщениями, социальная сеть или совместное использование файлов;

f) более сильные уровни доступа управления идентификации от публично доступных сетей.

Другая информация

Есть много типов электронной передачи сообщений, таких как электронная почта, электронный обмен данными и социальная сеть, которые играют роль в деловом общении.

13.2.4 Конфиденциальность или соглашения о неразглашении

Меры управления

Требования для конфиденциальности или соглашений о неразглашении, отражающих потребности организации в защите информации, должны быть определены, регулярно рассматриваться и документироваться.

Руководство по реализации

Конфиденциальность или соглашения о неразглашении должны удовлетворить требование, чтобы защитить конфиденциальную информацию, использующую юридически осуществимые термины. Конфиденциальность или соглашения о неразглашении применимы к третьим сторонам или сотрудникам организации. Элементы должны быть отобраны или добавлены с учетом типа другой стороны и ее допустимого доступа или обработки конфиденциальной информации. Чтобы определить требования для конфиденциальности или соглашений о неразглашении, следующие элементы нужно рассмотреть:

a) определение информации, которая будет защищена (например, конфиденциальная информация);

b) ожидаемый срок действия соглашения, включая случаи, где конфиденциальность, возможно, должна была бы сохраняться конфиденциальной;

c) необходимые действия, когда соглашение расторгнуто;

d) обязанности и действия подписавшихся, чтобы избежать несанкционированного информационного раскрытия;

e) собственность информации, коммерческих тайн и интеллектуальной собственности, и каким образом это относится к защите конфиденциальной информации;

f) разрешенное использование конфиденциальной информации и права подписавшегося использовать информацию;

g) право проверять и контролировать действия, которые включают конфиденциальную информацию;

h) процесс для уведомления и сообщения о несанкционированном раскрытии или утечки конфиденциальной информации;

i) условия для получения информации, которая будет возвращена или разрушена по истечению срока соглашения;

j) ожидаемые действия, которые будут взяты в случае нарушения соглашения.

Основанные на информационных требованиях безопасности организации, другие элементы могут быть необходимы для конфиденциальности или соглашения о неразглашении.

Конфиденциальность и соглашения о неразглашении должны соответствовать всем действующим законам и инструкциям для юрисдикции, к которой они применяются (см. 18.1).

Требования для конфиденциальности и соглашений о неразглашении должны рассматриваться периодически и когда изменения происходят, которые влияют на эти требования.

Другая информация

Конфиденциальность и соглашения о неразглашении защищают организационную информацию и сообщают подписавшимся об их обязанности защитить, использовать и раскрыть информацию ответственным и санкционированным способом.

Может быть потребность в организации, чтобы использовать различные формы конфиденциальности или соглашений о неразглашении при различных обстоятельствах.

14 Системных приобретений, развитие и обслуживание

14.1 Требования безопасности информационных систем

Цель: гарантировать, что информационная безопасность - неотъемлемая часть информационных систем в течение всего периода эксплуатации. Это также включает требования для информационных систем, которые предоставляют услуги по общедоступным сетям.

14.1.1 Информационный анализ требований безопасности и спецификация

Меры управления

Требования, имеющие отношение к информационной безопасности, должны быть включены в требования для новых информационных систем или улучшений к существующим информационным системам.

Руководство по реализации

Информационные требования безопасности должны быть определены, используя различные методы, такие как происходящие требования соблюдения от политики и инструкций, моделирования угрозы, обзоров инцидентов или использования порогов уязвимости. Результаты идентификации должны быть зарегистрированы и рассмотрены всеми заинтересованными сторонами.

Информационные требования безопасности и средства управления должны отразить деловую ценность включенной информации (см. 8.2) и потенциальное отрицательное деловое воздействие, которое могло бы следовать из отсутствия соответствующей безопасности.

Идентификация и управление информационными требованиями безопасности и связанными процессами должны быть объединены на ранних стадиях проектов информационных систем. Раннее рассмотрение информационных требований безопасности, например, в стадии проектирования может привести к более эффективным и прибыльным решениям.

Информационные требования безопасности должны также рассмотреть:

a) уровень уверенности, требуемой к требуемой личности пользователей, чтобы получить пользовательские требования идентификации;

b) обеспечивающий доступ и процессы разрешения, для деловых пользователей, а также для привилегированных или технических пользователей;

c) информирование пользователей и операторов об их обязанностях и ответственности;

d) необходимые потребности защиты включенных активов, в особенности относительно доступности, конфиденциальности, целостности;

e) требования, которые появились из бизнес-процессов, таких как операционная регистрация и контроль, требования не отказа от обязательств;

f) требования, переданные под мандат другими мерами обеспечения безопасности, например, интерфейсами к регистрации и контролю или системам обнаружения утечки данных.

Для заявлений, которые предоставляют услуги по общедоступным сетям или которые осуществляют сделки, нужно рассмотреть специальные средства управления 14.1.2 и 14.1.3.

Если продукты приобретены, формальный процесс тестирования и приобретения должен сопровождаться. Контракты с поставщиком должны обратиться к определенным требованиям безопасности. Где функциональность безопасности в предложенном продукте не удовлетворяет указанное требование, риск введенный и связанный со средствами управления, должен быть пересмотрен до покупки продукта.

Доступное руководство для конфигурации безопасности продукта, соответствующего заключительному программному обеспечению/набору услуг системы, должно быть оценено и осуществлено.

Критерии принятия продуктов должны быть определены, например, с точки зрения их функциональности, которая даст гарантию, что определенные требования безопасности находятся в соответствии. Продукты должны быть оценены против этих критериев перед приобретением. Дополнительная функциональность должна быть рассмотрена, чтобы гарантировать, что она не вводит недопустимые дополнительные риски.

Другая информация

[11] и [27] дают представление об использовании процессов управления рисками, чтобы определить средства управления для соответствия информационным требованиям безопасности.

14.1.2 Обеспечение сервисов приложений на общедоступных сетях

Меры управления

Информация, вовлеченная в сервисы приложений, передающие по общедоступным сетям, должна быть защищена от мошеннической деятельности, спорам по контракту и несанкционированному раскрытию и модификации.

Руководство по реализации

Информационные соображения безопасности для сервисов приложений, передающих по общедоступным сетям, должны включать следующее:

a) уровень уверенности, который требует каждая сторона в идентичности друг друга, например, посредством идентификации;

b) процессы разрешения, связанные с тем, кто может одобрить содержание, выпустить или подписать ключевые транзакционные документы;

c) обеспечение, что общающиеся партнеры хорошо проинформированы об их разрешениях по предоставлению или использованию обслуживания;

d) определения и требования соответствия для конфиденциальности, целостности, доказательства отправки и получения ключевых документов и не отказа от контрактов, например, связанный с предложением и процессами контракт;

e) уровень доверия требуется в целостности ключевых документов;

f) требования защиты любой конфиденциальной информации;

g) конфиденциальность и целостность любых сделок заказа, информации об оплате, деталей адреса доставки и подтверждения квитанций;

h) степень проверки, соответствующей, чтобы проверить информацию оплаты, предоставленную клиентом;

i) выбор самой соответствующей формы оплаты урегулирования, чтобы принять меры против мошенничества;

j) уровень защиты, требуемый поддержать конфиденциальность и целостность информации для заказа;

k) предотвращение потери или дублирование информации о сделке;

l) ответственность, связанная с любыми мошенническими сделками;

m) страховые требования.

Многие вышеупомянутые соображения могут быть решены применением шифровальных средств управления (см. Раздел 10), принимая во внимание соответствие законным требованиям (см. Раздел 18, особенно см. 18.1.5 для законодательства криптографии).

Меры сервиса приложений между партнерами должны быть поддержаны зарегистрированным соглашением, которое передает обе стороны согласованным условиям услуг, включая детали разрешения (см. b) выше).

Требования упругости против нападений нужно рассмотреть, которые могут включать требования для защиты включенных серверов приложений или обеспечения наличия сетевых соединений, требуемых предоставить услугу.

Другая информация

Заявления, доступные через общедоступные сети, подвергаются диапазону связанных угроз сети, таких как мошеннические действия, споры контракта или разглашение информации общественности. Поэтому, подробные оценки степени риска и надлежащий выбор средств управления обязательны. Средства управления включают шифровальные методы для передачи данных идентификации и обеспечения.

Сервисы приложений могут использовать безопасные методы идентификации, например, использующий криптографию открытого ключа и цифровые подписи (см. Раздел 10) снижать риск. Кроме того, могут использоваться доверенные третьи стороны, где такие услуги необходимы.

14.1.3 Защита сделок сервисов приложений

Меры управления

Информация, вовлеченная в сделки сервиса приложений, должна быть защищена, чтобы предотвратить неполную передачу, неправильное направление, несанкционированное изменение сообщения, несанкционированное раскрытие, несанкционированное дублирование сообщения или переигровку.

Руководство по реализации

Информационные соображения безопасности для сделок сервиса приложений должны включать следующее:

a) использование электронных подписей каждой из участвующих в сделке сторон;

b) все аспекты сделки, т.е. обеспечение, что:

1) секретная информация об идентификации пользователя всех сторон действительна и проверена;

2) сделка остается конфиденциальной;

3) частная жизнь, связанная со всеми участвующими сторонами, сохранена;

c) коммуникационный путь между всеми участвующими сторонами зашифрован;

d) протоколы, используемые для общения между всеми участвующими сторонами, обеспечены;

e) обеспечение, что хранение деталей транзакции расположено за пределами любой публично доступной среды, например, на платформе хранения, существующей на организационном интранете, и не сохранено и выставлено на носителе данных, непосредственно доступном из интернета;

f) где власть, которой доверяют, используется (например, в целях выйти и поддержать цифровые подписи или цифровые свидетельства), безопасность объединена и включена в течение всего непрерывного процесса управления свидетельствами/подписями.

Другая информация

Степень средств управления приняла потребности быть соразмерной с уровнем риска, связанного с каждой сервисной сделкой бланка заявки на участие.

Сделки, возможно, должны выполнить законные и нормативные требования в юрисдикции, от которой сделка произведена, обработана, закончена или сохранена.

14.2 Безопасность в развитии и процессах поддержки

Цель: гарантировать, что информационная безопасность разработана и осуществлена в пределах жизненного цикла развития информационных систем.

14.2.1 Безопасная стратегия развития

Меры управления

Правила для развития программного обеспечения и систем должны устанавливаться и относиться к событиям в организации.

Руководство по реализации

Безопасное развитие является требованием, чтобы создать безопасное обслуживание, архитектуру, программное обеспечение и систему.

В пределах безопасной стратегии развития следующие аспекты должны быть помещены на рассмотрении:

a) безопасность среды проектирования;

b) руководство по безопасности в жизненном цикле разработки программного обеспечения:

1) безопасность в методологии разработки программного обеспечения;

2) использование безопасных кодирующих рекомендаций для каждого языка программирования;

c) требования безопасности в стадии проектирования;

d) контрольно-пропускные пункты безопасности в течение этапов проекта;

e) безопасные хранилища;

f) безопасность в контроле вариантов;

g) необходимое прикладное знание безопасности;

h) способность разработчиков предотвращения, нахождения и фиксации слабых мест.

Безопасные программные методы должны использоваться и для новых разработок и в кодовых сценариях повторного использования, где стандарты относились к развитию, могут быть неизвестны или не совместимы с текущими методами наиболее успешной практики. Безопасные кодирующие стандарты нужно рассмотреть, а также рассмотреть, если они актуальны для использования.

Разработчики должны быть обучены в их использовании и тестировании, и кодовый обзор должен проверить их использование.

Если развитие произведено на стороне, организация должна получить гарантию, что третья сторона выполняет эти правила для безопасного развития (см. 14.2.7).

Другая информация

Развитие может также иметь место в приложениях, таких как офисные приложения, написание кодов, браузеры и базы данных.

14.2.2 Системные процедуры контроля изменения

Меры управления

Изменениями систем в пределах жизненного цикла развития нужно управлять при помощи формальных процедур контроля изменения.

Руководство по реализации

Формальные процедуры контроля изменения должны быть зарегистрированы и осуществлены, чтобы гарантировать целостность системы, приложений и продуктов, от ранних стадий проектирования до всех последующих усилий по обслуживанию.

Введение новых систем и существенных изменений к существующим системам должно следовать за формальным процессом документации, спецификации, тестирования, контроля качества и управляемого внедрения.

Этот процесс должен включать оценку степени риска, анализ воздействий изменений и спецификации необходимых мер обеспечения безопасности. Этот процесс должен также гарантировать, что существующая безопасность и процедуры контроля не поставлены под угрозу, что программистам поддержки предоставляют доступ только к тем частям системы, необходимой для их работы и что формальное соглашение и одобрение для любого изменения получено.

Везде, где реально, применение и эксплуатационные процедуры контроля изменения должны быть объединены (см. 12.1.2). Процедуры контроля изменения должны включать, но не быть ограничены:

a) поддержание отчета согласованных уровней разрешения;

b) гарантирующие изменения представлены зарегистрированными пользователями;

c) рассмотрение управления и процедуры целостности, чтобы гарантировать, что они не будут скомпрометированы изменениями;

d) определение всего программного обеспечения, информации, предприятия базы данных и аппаратных средств, которые требуют поправки;

e) идентификация и проверка безопасности критического кодекса, чтобы минимизировать вероятность известных слабых мест безопасности;

f) получение формального одобрения для детальных предложений перед работой;

g) гарантирующие зарегистрированные пользователи принимают изменения до внедрения;

h) обеспечение, что системный набор документации обновлен на завершении каждого изменения и что старую документацию архивируют или избавляются;

i) обеспечение контроля вариантов для всех обновлений программного обеспечения;

j) поддержание контрольного журнала всех запросов на изменение;

k) обеспечение, что операционная документация (см. 12.1.1) и пользовательские процедуры изменены по мере необходимости, чтобы остаться соответствующими;

l) обеспечение, что внедрение изменений имеет место в нужное время и не нарушает включенные бизнес-процессы.

Другая информация

Изменяемое программное обеспечение может повлиять на рабочую среду и наоборот.

Хорошая практика включает тестирование нового программного обеспечения в окружающей среде, отдельной и от производства и от сред проектирования (см. 12.1.4). Это обеспечивает средство управления новым программным обеспечением и разрешение дополнительной защиты эксплуатационной информации, которая используется для тестирования цели. Это должно включать участки, пакеты обновления и другие обновления.

Где рассматриваются автоматические обновления, риск для целостности и доступности системы должен быть взвешен против выгоды быстрого развертывания обновлений. Автоматизированные обновления не должны использоваться на критических системах, поскольку некоторые обновления могут заставить важные приложения терпеть неудачу.

14.2.3 Технический обзор заявлений после операционной платформы изменяется

Меры управления

Когда операционные платформы изменены, важные деловые заявления должны быть рассмотрены и проверены, чтобы гарантировать, что нет никакого неблагоприятного воздействия на организационные операции или безопасность.

Руководство по реализации

Этот процесс должен покрыть:

a) обзор прикладных процедур контроля и целостности, чтобы гарантировать, что они не были скомпрометированы операционными изменениями платформы;

b) обеспечение, что уведомление об операционных изменениях платформы предоставлено вовремя, чтобы позволить соответствующим тестам и обзорам иметь место перед внедрением;

c) обеспечение, что соответствующие изменения внесены в планы обеспечения непрерывности бизнеса (см. Раздел 17).

Другая информация

Операционные платформы включают операционные системы, базы данных и платформы промежуточного программного обеспечения. Контроль должен также быть применен для изменений заявлений.

14.2.4 Ограничения на изменения пакетов программ

Меры управления

Модификациям к пакетам программ нужно препятствовать, ограничить необходимыми изменениями и всеми изменениями нужно строго управлять.

Руководство по реализации

Как можно возможнее снабженные продавцами пакеты программ должны использоваться без модификации. Где пакет программ должен быть изменен, следующие моменты нужно рассмотреть:

a) риск встроенных средств управления и поставивших под угрозу процессов целостности;

b) должно ли согласие продавца быть получено;

c) возможность получения необходимых изменений от продавца в качестве стандартного обновления программы;

d) воздействие, если организация становится ответственной за будущее обслуживание программного обеспечения в результате изменений;

e) совместимость с другим программным обеспечением в использовании.

Если изменения необходимы, то оригинальное программное обеспечение должно быть сохранено, а изменения относились бы к определяемой копии. Управленческий процесс обновления программного обеспечения должен быть осуществлен, чтобы гарантировать самые актуальные одобренные участки, а прикладные обновления установлены для всего санкционированного программного обеспечения (см. 12.6.1). Все изменения должны быть полностью проверены и зарегистрированы, чтобы они могли быть повторно использованы, при необходимости, к будущим модернизациям программного обеспечения. При необходимости модификации должны быть проверены и утверждены независимым телом оценки.

14.2.5 Безопасные системные принципы разработки

Меры управления

Принципы для технических безопасных систем должны устанавливаться, документироваться, сохраняться и относиться к внедрению информационной системы.

Руководство по реализации

Безопасные порядки разработки информационной системы, основанные на принципах разработки безопасности, должны устанавливаться, документироваться и относиться к внутренним действиям разработки информационной системы. Безопасность должна быть разработана во все слои архитектуры (бизнес, данные, приложения и технология), соразмеряя потребности в информационной безопасности с потребностью в доступности. Новая технология должна быть проанализирована для угроз безопасности, а дизайн должен быть рассмотрен против известных образцов нападения.

Эти принципы и установленные технические порядки должны регулярно рассматриваться, чтобы гарантировать, что они эффективно способствуют расширенным стандартам безопасности в рамках процесса разработки. Они должны также регулярно рассматриваться, чтобы гарантировать, чтобы они остались актуальными с точки зрения борьбы с любым новыми потенциальными угрозами и с точки зрения оставаться применимыми к достижениям в технологиях и применяемых решениях.

Установленные принципы разработки безопасности должны быть применены, когда это применимо, к произведенным на стороне информационным системам через контракты и другие обязывающие соглашения между организацией и поставщиком, которому

организация производит на стороне. Организация должна подтвердить, что строгость принципов инженерной безопасности поставщиков сопоставимо с принципами организации.

Другая информация

Процедуры разработки приложений должны применить безопасную технику в развитии приложений, у которых есть интерфейсы входа и выхода. Безопасная техника дает представление о пользовательских методах идентификации, обеспечивает контроль за сессией и подтверждение правильности данных, обработкой и устранение отладки кодексов.

14.2.6 Безопасная среда проектирования

Меры управления

Организации должны установить и соответственно защитить безопасные среды проектирования для системного развития и усилий по интеграции в течение всего периода эксплуатации.

Руководство по реализации

Безопасная среда проектирования включает людей, процессы и технологию, связанную с системным развитием и интеграцией.

Организация должны оценить риски, связанные с отдельными системными усилиями по развитию, и установить безопасные среды проектирования для определенных системных усилий по развитию, рассмотрев:

a) чувствительность данных, которые будут обработаны, сохранены и переданы системой;

b) применимые внешние и внутренние требования, например, из инструкций или политики;

c) меры обеспечения безопасности, уже осуществленные организацией для развития системы поддержки;

d) кредитоспособность персонала, работающего в окружающей среде (см. 7.1.1);

e) степень аутсорсинга, связанного с системным развитием;

f) потребность в разделении между различными средами проектирования;

g) контроль доступа к среде проектирования;

h) контроль изменения окружающей среды и сохраненного кодекса;

i) резервные копии сохранены в безопасных удаленных местоположениях;

j) контроль над движением данных от и до окружающей среды.

Как только уровень защиты определен для определенной среды проектирования, организации должны зарегистрировать соответствующие процессы в безопасных процедурах развития и предоставить их всем людям, которым нужны они.

14.2.7 Произведенное на стороне развитие

Меры управления

Организация должна контролировать и контролировать деятельность произведенного на стороне системного развития.

Руководство по реализации

Где системное развитие произведено на стороне, следующие моменты нужно рассмотреть через всю внешнюю систему поставок организации:

a) лицензирование мер, кодовой собственности и прав на интеллектуальную собственность, связанных с произведенным на стороне содержанием (см. 18.1.2);

b) договорные требования для безопасного дизайна, кодирования и проверки методов (см. 14.2.1);

c) предоставление одобренной модели угрозы внешнему разработчику;

d) приемное тестирование на качество и точность конечного результата;

e) предоставление доказательств, что пороги безопасности использовались, чтобы установить минимальные допустимые уровни качества безопасности и частной жизни;

f) предоставление доказательств, что достаточное тестирование было применено, чтобы принять меры против отсутствия и намеренного и неумышленного злонамеренного содержания по доставке;

g) предоставление доказательств, что достаточное тестирование было применено, чтобы принять меры против присутствия известных слабых мест;

h) меры условного депонирования, например, если исходный код больше не доступен;

i) договорное право ревизовать процессы развития и средства управления;

j) эффективная документация построения окружающей среды раньше создавала конечный результат;

k) организация остается ответственной за соответствие действующим законам и проверке эффективности контроля.

Другая информация

Дополнительная информация об отношениях поставщика может быть найдена в [21][22][23]

14.2.8 Тестирование безопасности системы

Меры управления

Тестирование функциональности безопасности должно быть выполнено во время развития.

Руководство по реализации

Новые и обновленные системы требуют полного тестирования и проверки во время процессов развития, включая подготовку подробного графика действий и проверяют входы и ожидаемую продукцию под рядом условий. Для внутренних событий такие тесты должны первоначально быть выполнены группой разработчиков. Независимое приемное тестирование должно тогда быть предпринято (и для внутреннего и для произведенных на стороне событий), чтобы гарантировать, что система работает как ожидалось (см. 14.1.1 и 14.1.9). Степень тестирования должна быть в пропорции к важности и природе системы.

14.2.9 Системное приемное тестирование

Меры управления

Приемные программы тестирования и связанные критерии должны быть установлены для новых информационных систем, модернизаций и новых версий.

Руководство по реализации

Системное приемное тестирование должно включать тестирование информационных требований безопасности (см. 14.1.1 и 14.1.2) и приверженность, чтобы обеспечить системные методы развития (см. 14.2.1). Тестирование должно также быть проведено на полученных компонентах и интегрированных системах. Организации могут усилить автоматизированные инструменты, такие как кодовые аналитические инструменты или сканеры уязвимости, и должны проверить, что исправление безопасности связало дефекты.

Тестирование должно быть выполнено в реалистических условиях испытаний, чтобы гарантировать, что система не введет уязвимость для среды организации и что тесты надежны.

14.3 Данные испытаний

Цель: обеспечивать защиту данных, используемых для тестирования.

14.3.1 Защита данных испытаний

Меры управления

Данные испытаний нужно отобрать тщательно, защитить и управлять.

Руководство по реализации

Использования рабочих данных, содержащих личные данные или любую другую конфиденциальную информацию для тестирования целей, нужно избежать. Если личные

данные или иначе конфиденциальная информация используется для тестирования целей, все чувствительные детали и содержание должны быть защищены удалением или модификацией (см. [26]).

Следующие рекомендации должны быть применены, чтобы защитить рабочие данные, когда используются для тестирования целей:

a) процедуры управления доступом, которые относятся к эксплуатационным прикладным системам, должны также примениться к испытательным прикладным системам;

b) должно быть отдельное разрешение каждый раз, когда эксплуатационная информация скопирована к условиям испытаний;

c) эксплуатационная информация должна быть немедленно удалена из условий испытаний после того, как тестирование будет завершено;

d) копирование и использование эксплуатационной информации должны быть зарегистрированы, чтобы обеспечить контрольный журнал.

Другая информация

Система и приемо-сдаточные испытания требуют существенных объемов данных испытаний, которые максимально близки к рабочим данным.

15 Отношения с поставщиками

15.1 Информационная безопасность в отношениях с поставщиками

Цель: Обеспечить защиту активов организации, доступных поставщикам.

15.1.1 Политика информационной безопасности для отношений с поставщиками

Меры управления

Требования информационной безопасности, предназначенные для того, чтобы снизить риски, связанные с доступом поставщика к активам организации, должны быть согласованы с поставщиком и задокументированы.

Руководство по применению

Организация должна определить и установить в качестве обязательных, информационные меры обеспечения безопасности, чтобы определенным образом работать с доступом поставщика к информации организации. Эти меры обеспечения безопасности должны относиться к процессам и процедурам, которые будет выполнять организация, а также к тем процессам и процедурам, выполнение которых организация должна потребовать у поставщика, включая:

a) определение и документирование типа поставщиков, таких как, услуги ИТ, услуги логистики, финансовые услуги, компоненты инфраструктуры ИТ, которым организация предоставит доступ к своей информации;

b) стандартизированный процесс и период для управления отношениями поставщиками;

c) определение вида информационного доступа, который будет доступен различным типам поставщиков, а также контроль и управление доступом;

d) минимальные требования информационной безопасности к каждому виду информации и к каждому виду доступа, предназначенных служить основанием для индивидуальных соглашений поставщика, которые основаны на деловых потребностях и требованиях организации и ее профиля риска;

e) процессы и процедуры контроля соблюдения установленных требований информационной безопасности для каждого типа поставщика и каждого вида доступа, включая осмотр и проверку продукта третьим лицом;

f) точность меры управления завершенностью для обеспечения целостности информации или обработки информации, которая предоставляется другой стороной;

g) вид обязательств, применяемый к поставщикам для того, чтобы защитить информацию организации;

h) работа с инцидентами и непредвиденными обстоятельствами, связанных с доступом поставщика, включая, обязанности организации, а также поставщика;

i) устойчивость системы и способность восстанавливаться, если необходимо, и контингенция для обеспечения доступности информации или обработки информации каждой стороне;

j) вводный курс для персонала организации, вовлеченного в приобретения относительно применимой политики, процессов и процедур;

k) вводный курс для персонала организации, взаимодействующему с персоналом поставщика относительно соответствующих правил обязательств и режима работы, основанных на типе поставщика и уровне доступа поставщика к системам и информации организации;

l) условия, при которых требования информационной безопасности и меры обеспечения безопасности будут документированы в соглашении, которое подписано обеими сторонами;

m) управление необходимыми переходами информации, средствами для обработки информации и т.д., которые должны быть перемещены, и гарантия того, что информационная безопасность сохраняется в течение переходного периода.

Дополнительная информация

Соглашения могут значительно отличаться для различных организаций и среди различных типов поставщиков. Поэтому, нужно быть осторожным, чтобы охватить все угрозы безопасности используемой информации и требования. Соглашения с поставщиками могут также охватывать другие стороны (например, субпоставщики).

В случае, когда поставщик становится не способным поставлять свои продукты или предоставлять свои услуги, в соглашении должны быть рассмотрены процедуры продолжения процесса, чтобы избежать любой задержки подготовки замещающих продуктов или услуг.

15.1.3 Система поставок информационно-коммуникационных технологий

Меры управления

Соглашения с поставщиками должны включать требования к угрозам информационной безопасности, связанных с услугами информационно-коммуникационных технологий и системой поставок продукта.

Руководство по применению

Следующие темы нужно рассмотреть для включения в соглашения поставщика относительно безопасности системы поставок:

a) определение требований информационной безопасности, чтобы применить к продукту информационно-коммуникационных технологий или сервисному приобретению в дополнение к требованиям безопасности общей информации для отношений поставщика;

b) для информационных и коммуникационных услуг, которые требуют распространения требований безопасности информации по всей цепи поставки, если субконтракт поставщиков предоставлен организации о частях информации и услуг по телекоммуникационным технологиям;

c) для продуктов информационно-коммуникационных технологий, которые требуют, чтобы поставщики распространили соответствующие методы безопасности по всей системе поставок, если эти продукты включают компоненты, купленные от других поставщиков;

d) осуществление процесса контроля и приемлемых методов для утверждения, которое предоставило продукты информационно-коммуникационных технологий и услуги, придерживается установленных требований безопасности;

e) осуществление процесса по идентификации продукта или сервисных компонентов, которые важны для поддержания функциональности и поэтому требуют повышенного внимания и исследования, когда построено за пределами организации, если поставщик высшего ранга производит аспекты на стороне продукта или сервисных компонентов другим поставщикам;

f) получение гарантии, что критические компоненты и их происхождение могут быть прослежены по всей системе поставок;

g) получение гарантии, что поставленные продукты информационно-коммуникационных технологий функционируют, как ожидалось без любых неожиданных или нежелательных особенностей;

h) определение правил для обмена информацией относительно системы поставок и любых потенциальных проблем и компромиссов среди организации и поставщиков;

i) осуществление определенных процессов во периода эксплуатации компонента информационно-коммуникационных технологий и доступности и связанных с ними угроз безопасности. Настоящее включает управление рисками компонентов, больше не являющихся доступным из-за поставщиков, больше не находящихся в бизнесе или поставщиках, которые более не обеспечивают настоящие компоненты из-за технологических продвижений.

Другая информация

Определенные методы управления рисками системы поставок информационно-коммуникационных технологий основано на высших практиках безопасности общей информации, качества, управления проектом и системных методов разработки, но не заменяют их.

Организациям советуют работать с поставщиками, чтобы понять систему поставок информационно-коммуникационных технологий и любые вопросы, которые оказывают важное влияние на продукты и предоставленные услуги. Организации могут влиять на методы безопасности информации о системе поставок информационно-коммуникационных технологий, ясно давая понять в соглашениях с их поставщиками вопросы, которые должны быть обращены другими поставщиками в системе поставок информационно-коммуникационных технологий.

Система поставок информационно-коммуникационных технологий, как показано здесь, включает услуги по облачным вычислениям.

15.2 Управление предоставлением услуг поставщика

Цель: поддержать согласованный уровень информационной безопасности и предоставления услуг в соответствии с соглашениями поставщика.

15.2.1 Контроль и обзор услуг поставщика

Меры управления

Организации должны регулярно контролировать, рассматривать и проверять предоставление услуг поставщика.

Руководство по реализации

Контроль и обзор услуг поставщика должен гарантировать, что к информационным положениям и условиям безопасности соглашений придерживаются и что информационными инцидентами безопасности и проблемами управляют должным образом.

Это должно включить сервисный управленческий процесс отношений между организацией и поставщиком:

a) сервисные уровни выполнения обзора, чтобы проверить приверженность соглашениям;

b) проверка сервисных отчетов, представленных поставщиком и назначение регулярных встречи прогресса в соответствии с соглашениями;

c) проведение аудитов поставщиков, вместе с обзором отчетов независимого аудитора и плановый отчет по определенным вопросам;

d) предоставление информации об информационных инцидентах безопасности и рассмотрение информации в соответствии с соглашениями и любым рекомендациям по поддержке и процедурам;

e) рассмотрение контрольного журнала поставщика и отчеты информационных событий безопасности, эксплуатационных проблем, неудач, отслеживания ошибок и разрушений, связанных с предоставленной услугой;

f) решение и управление любыми определенными проблемами;

g) аспекты безопасности информации об обзоре отношений поставщика с ее собственными поставщиками;

h) гарантирование, что поставщик поддерживает достаточную сервисную способность вместе с осуществимыми планами, разработанными, чтобы гарантировать, что согласованные сервисные уровни непрерывности сохраняются после основных сервисных неудач или бедствий (см. Раздел 17).

Ответственность за руководящие отношения поставщика должна быть возложена на назначенного человека или сервисное руководство. Кроме того, организация должна гарантировать, чтобы поставщики возложили обязанности для рассмотрения соблюдения и предписания требований соглашений. Достаточные технические навыки и ресурсы должны быть сделаны доступными, чтобы контролировать, что требованиям соглашения, в особенности информационным требованиям безопасности, отвечают. Соответствующие меры должны быть приняты, когда наблюдается нехватка в предоставлении услуг.

Организация должна сохранить достаточный полный контроль и видимость во все аспекты безопасности для чувствительной или критической информации, или средства обработки информации получили доступ, обработали или справились поставщиком. Организация должна сохранить видимость в действиях безопасности, в таких как управление изменениями, идентификация слабых мест и информационной отчеты об инцидентах безопасности, а также ответов посредством определенного процесса сообщения.

15.2.2 Управление изменениями услуг поставщика

Меры управления

Изменениями предоставления услуг поставщиками, включая поддержание и улучшение существующей информационной политики безопасности, процедур и средств управления, нужно управлять, принимая во внимание критичность бизнес-информации, систем и включенных процессов и переоценки рисков.

Руководство по реализации

Следующие аспекты должны быть учтены:

a) изменения соглашений поставщика;

b) изменения, внесенные организацией, чтобы осуществить:

1) улучшения к текущим предложенным услугам;

2) развитие любых новых заявлений и систем;

3) модификации или обновления политики и процедур организации;

4) новые или измененные средства управления, чтобы решить информационные инциденты безопасности и улучшить безопасность;

c) изменения в услугах поставщика, чтобы осуществить:

1) изменения и улучшение сетей;

2) использование новых технологий;

3) принятие новых продуктов или более новых версий/выпусков;

4) инструменты новой разработки и окружающей среды;

5) изменения физического местоположения средств обслуживания;
6) изменение поставщиков;
7) заключение субподрядного договора другому поставщику.

16 Информационное управление инцидентом безопасности

16.1 Управление информационными инцидентами безопасности и улучшениями

Цель: гарантировать последовательный и эффективный подход к управлению информационными инцидентами безопасности, включая обсуждение событий безопасности и слабых мест.

16.1.1 Обязанности и процедуры

Меры управления

Управленческие функции и процедуры должны быть установлены, чтобы гарантировать быстрый, эффективный и организованный ответ на информационные инциденты безопасности.

Руководство по реализации

Следующие рекомендации для управленческих функций и процедуры относительно информационного управления инцидентом безопасности нужно рассмотреть:

a) управленческие функции должны быть установлены, чтобы гарантировать, что следующие процедуры развиты и сообщены соответственно в организации:

1) процедуры планирования реагирования на инциденты и подготовки;
2) процедуры контроля, обнаружения, анализа и сообщения информационных событий безопасности и инцидентов;
3) процедуры регистрации управленческих действий инцидента;
4) процедуры обработки данных судебной экспертизы;
5) процедуры оценки и решения об информационных событиях безопасности и оценке информационных слабых мест безопасности;
6) процедуры ответа, включая распространение, управляемое восстановление после инцидента и общение с внутренним и внешним персоналом или организациями;

b) установленные порядки должны гарантировать, что:

1) компетентный персонал работает с проблемами, которые имеют отношение к информационным инцидентам безопасности в организации;
2) установлена точка контакта для обнаружения инцидентов безопасности и сообщений;
3) сохраняются соответствующие контакты с властями, внешними заинтересованными группами или форумами, которые обращаются с проблемами, связанными с информационными инцидентами безопасности;

c) процедуры отчетности должны включать:

1) подготовка информационного сообщения безопасности событий, чтобы поддержать действие сообщения и помочь человеку, который составляет сообщение, помнить все необходимые действия в случае информационного события безопасности;
2) процедура, которая будет предпринята в случае информационного события безопасности, например, замечания всех деталей, таких как тип несоответствия или нарушения, происходящего из-за сбоя, сообщений на экране и немедленное сообщение в пункт контакта и принятие только скоординированный действий;
3) ссылка на установленный формальный дисциплинарный процесс для контакта с сотрудниками, которые передают нарушения правил безопасности;

4) подходящая обратная связь обрабатывает, чтобы гарантировать, что те люди, сообщающие об информационных событиях безопасности, уведомлены относительно результатов после того, как с проблемой имели дело и закрыли.

Цели для информационного управления инцидентом безопасности должны быть согласованы с управлением, и должно быть обеспечено что, ответственные за информационное управление инцидентом безопасности понимают приоритеты организации для обработки информационных инцидентов безопасности.

Руководство по реализации

Информационные инциденты безопасности могли бы превысить организационные и национальные границы. Чтобы ответить на такие инциденты существует увеличивающаяся потребность скоординировать ответ и поделиться информацией об этих инцидентах с внешними организациями.

Подробное руководство на информационном управлении инцидентом безопасности содержится в [20]/

16.1.2 Сообщение об информационных событиях безопасности

Меры управления

Об информационных событиях безопасности нужно сообщать как можно быстрее через соответствующие управленческие каналы.

Руководство по реализации

Все сотрудники и подрядчики должны знать об их обязанности сообщить об информационных событиях безопасности, как можно быстрее. Они должны также знать о процедуре сообщения об информационных событиях безопасности и точке контакта, которой нужно сообщить о событиях.

Ситуации, которые рассмотрят для информационного сообщения безопасности событий, включают:

a) неэффективный контроль за безопасностью;

b) нарушение информационной целостности, конфиденциальности или ожиданий доступности;

c) человеческие ошибки;

d) несоблюдения политики или рекомендаций;

e) нарушения мер физической защиты;

f) безудержные системные изменения;

g) сбои программного обеспечения или аппаратных средств;

h) нарушения доступа.

Другая информация

Сбои или другое аномальное системное поведение могут быть индикатором атаки на безопасность или фактического нарушения правил безопасности и должны поэтому всегда сообщаться как информационное событие безопасности.

16.1.3 Сообщение об информационных слабых местах безопасности

Меры управления

Сотрудники и подрядчики, использующие информационные системы и услуги организации, должны быть обязаны отмечать и сообщать о любых наблюдаемых или подозреваемых информационных слабых местах безопасности в системах или услугах.

Руководство по реализации

Все сотрудники и подрядчики должны сообщить об этих вопросах в пункт контакта как можно быстрее, чтобы предотвратить информационные инциденты безопасности. Механизм сообщения должен быть максимально легким и доступным.

Другая информация

Сотрудникам и подрядчикам нужно советовать не попытаться доказать подозреваемые слабые места безопасности. Тестирование слабых мест могло бы интерпретироваться как

потенциальное неправильное употребление системы и могло также нанести ущерб информационной системе или обслуживанию и привести к юридической ответственности за человека, выполняющего тестирование.

16.1.4 Оценка и решение об информационных событиях безопасности

Меры управления

Информационные события безопасности должны быть оценены и решены, если они должны быть классифицированы как информационные инциденты безопасности.

Руководство по реализации

Точка контакта должна оценить каждое информационное событие безопасности, используя согласованное информационное событие безопасности и шкалу классификации инцидентов, и решают, должно ли событие быть классифицировано как информационный инцидент безопасности. Классификация и установление приоритетов инцидентов могут помочь определить воздействие и степень инцидента.

В случаях, где у организации есть информационная команда реагирования на инциденты безопасности (далее - ISIRT), оценка и решение могут быть отправлены ISIRT для подтверждения или переоценки.

Результаты оценки и решения должны быть зарегистрированы подробно в целях будущей ссылки и проверки.

16.1.5 Ответ на информационные инциденты безопасности

Меры управления

На информационные инциденты безопасности нужно ответить в соответствии с зарегистрированными процедурами.

Руководство по реализации

На информационные инциденты безопасности должна отвечать назначенная точка контакта и другие соответствующие люди организации или третьих сторон (см. 16.1.1).

Ответ должен включать следующее:

a) собирание доказательств как можно скорее;

b) проведение информационного анализа судебной экспертизы безопасности, согласно требованию (см. 16.1.7);

c) подъем (распространение) согласно требованию;

d) обеспечение, что все включенные действия ответа должным образом зарегистрированы для более позднего анализа;

e) сообщение существования информационного инцидента безопасности или любых соответствующих деталей другим внутренним и внешним людям или организациям;

f) контакт с информационной слабостью(-ми) безопасности, которая вызвала или способствовала инциденту;

g) как только был успешно исчерпан, формально закрыть дело и составить отчет.

Анализ постинцидента должен иметь место, по мере необходимости, чтобы определить источник инцидента.

Другая информация

Первая цель реагирования на инциденты состоит в том, чтобы возобновить «нормальный уровень безопасности» и затем начать необходимое восстановление.

16.1.6 Приобретение знаний из информационных инцидентов безопасности

Меры управления

Знание, полученное от анализа и решения информационных инцидентов безопасности, должно использоваться, чтобы уменьшить вероятность или воздействие будущих инцидентов.

Руководство по реализации

Должен существовать механизмы, чтобы позволить типам, объемам и затратам на информационные инциденты безопасности быть определенными количественно и

проверенными. Информация, полученная от оценки информационных инцидентов безопасности, должна использоваться, чтобы определить возвращение или высоко повлиять на инциденты.

Другая информация

Оценка информационных инцидентов безопасности может указать на потребность в расширенных или дополнительных средствах управления, чтобы ограничить частоту, повреждение и затраты на будущие случаи, или быть принятой во внимание в процессе рассмотрения политики безопасности (см. 5.1.2).

С должной заботой об аспектах конфиденциальности анекдоты от фактических информационных инцидентов безопасности могут использоваться в пользовательском обучении осведомленности (см. 7.2.2) как примеры того, что могло произойти, как ответить на такие инциденты и как избежать их в будущем.

16.1.7 Сбор доказательств

Меры управления

Организация должна определить и применить процедуры идентификации, коллекции, приобретения и сохранения информации, которая может служить доказательствами.

Руководство реализации

Внутренние способы должны разрабатываться и сопровождаться, имея дело с доказательствами в целях дисциплинарных мер и судебного иска.

В целом настоящие процедуры доказательств должны обеспечить процессы идентификации, коллекции, приобретения и сохранения доказательств в соответствии с различными типами данных, устройств и статуса устройств, например, приведенный в действие или выключенный. Процедуры должны принять во внимание:

a) цепь заключения;

b) безопасность доказательств;

c) безопасность персонала;

d) роли и обязанности персонала;

e) компетентность персонала;

f) документация;

g) брифинг.

Где доступно, сертификация или другие соответствующие средства квалификации персонала и инструментов должны быть найдены, чтобы усилить ценность сохраненных доказательств.

Данные судебной экспертизы могут превысить организационные или подведомственные границы. В таких случаях это должно быть обеспечено, что организация наделена правом собрать необходимую информацию как данные судебной экспертизы. Требования различной юрисдикции, как должны также полагать, максимизируют возможности допуска через соответствующую юрисдикцию.

Другая информация

Идентификация является процессом, включающим поиск, признание и документацию потенциальных доказательств. Коллекция - процесс сбора физических пунктов, которые могут содержать потенциальные доказательства. Приобретение - процесс создания копии данных в пределах определенного набора. Сохранение - процесс, чтобы поддержать и охранять целостность и оригинальное условие потенциальных доказательств.

Когда информационное событие безопасности обнаружено впервые, может быть неясно, приведет ли событие к судебному иску. Поэтому, существует опасность, что необходимые доказательства разрушены преднамеренно или случайно, прежде чем серьезность инцидента будет понята. Желательно привлечь адвоката или полицию в любом рассмотренном судебном иске и получить совет относительно требуемых доказательств.

[24] предоставляет рекомендации для идентификации, коллекции, приобретения и сохранения цифровых доказательств.

17 Информационные аспекты безопасности управления непрерывностью бизнеса

17.1 Информационная непрерывность безопасности

Цель: информационная непрерывность безопасности должна быть включена в системы управления непрерывностью бизнеса организации.

17.1.1 Планирование информационной непрерывности безопасности

Меры управления

Организация должна определить свои требования для информационной безопасности и непрерывности информационного управления безопасностью в неблагоприятных ситуациях, например, во время кризиса или бедствия.

Руководство по реализации

Организация должна определить, находится ли непрерывность информационной безопасности в рамках управленческого процесса непрерывности бизнеса или в рамках управленческого процесса аварийного восстановления. Информационные требования безопасности должны быть определены, планируя непрерывность бизнеса и аварийное восстановление.

В отсутствие формальной непрерывности бизнеса и планирования аварийного восстановления, информационное управление безопасностью должно предположить, что информационные требования безопасности остаются тем же самым в неблагоприятных ситуациях, по сравнению с нормальными эксплуатационными условиями. Альтернативно, организация могла выполнить деловой анализ воздействия для информационных аспектов безопасности, чтобы определить информационные требования безопасности, применимые к неблагоприятным ситуациям.

Другая информация

Чтобы уменьшить время и усилие по «дополнительному» деловому анализу воздействия для информационной безопасности, рекомендуется получить информационные аспекты безопасности в пределах нормального управления непрерывностью бизнеса, или управлением аварийного восстановления, влияющего на анализ. Настоящее подразумевает, что информационные требования непрерывности безопасности явно сформулированы в управлении непрерывностью бизнеса или управленческих процессах аварийного восстановления.

Информация об управлении непрерывностью бизнеса может быть найдена в [14], [9] и [8].

17.1.2 Осуществление информационной непрерывности безопасности

Меры управления

Организация должна установить, зарегистрировать, осуществить и поддержать процессы, процедуры и средства управления, чтобы гарантировать необходимый уровень непрерывности для информационной безопасности во время неблагоприятной ситуации.

Руководство по реализации

Организация должна гарантировать, что:

a) соответствующая управленческая структура существует, чтобы подготовиться, смягчить и ответить на подрывные действия, используя необходимую власть, опыт и компетентность;

b) назначается персонал реагирования на инциденты с необходимой ответственностью, властью и компетентностью для управления инцидентом и поддержанием информационной безопасности;

c) зарегистрированные планы, ответ и процедуры восстановления развиты и одобрены, детализируя, как организация будет управлять подрывным событием и поддержит его информационную безопасность на предопределенном уровне, основанном на одобренных управлением информационных целях непрерывности безопасности (см. 17.1.1).

Согласно информационным требованиям непрерывности безопасности, организация должна установить, зарегистрировать, осуществить и поддержать:

a) информационные меры обеспечения безопасности в пределах непрерывности бизнеса или процессов аварийного восстановления, процедур и систем поддержки и инструментов;

b) процессы, процедуры и внедрение изменяются, чтобы поддержать существующие средства управления информационной безопасности во время неблагоприятной ситуации;

c) компенсирующие средства управления для средств управления информационной безопасностью, которые не могут сохраняться во время неблагоприятной ситуации.

Другая информация

В пределах контекста непрерывности бизнеса или аварийного восстановления, возможно были определены определенные процессы и процедуры. Информация, которая обработана в рамках этих процессов и процедур или в пределах специальных информационных систем, чтобы поддержать их, должна быть защищена. Поэтому организация должна привлечь информационных специалистов по безопасности, устанавливая, осуществляя и поддерживая непрерывность бизнеса или процессов аварийного восстановления и процедуры.

Информационные меры обеспечения безопасности, которые были осуществлены, должны продолжить работать во время неблагоприятной ситуации. Если меры обеспечения безопасности не в состоянии продолжить обеспечивать информацию, другие средства управления должны устанавливаться, осуществляться и сохраняться, чтобы поддержать допустимый уровень информационной безопасности.

17.1.3 Проверка, рассмотрение и оценка непрерывности информационной безопасности

Меры управления

Организация должна проверить установленные и осуществленные информационные средства управления непрерывностью безопасности равномерно, чтобы гарантировать, что они действительны и эффективны во время неблагоприятных ситуаций.

Руководство по реализации

Организационные, технические, процедурные и процессуальные изменения в эксплуатационном контексте или контексте непрерывности, может привести к изменениям в информационных требованиях непрерывности безопасности. В таких случаях непрерывность процессов, процедур и средств управления для информационной безопасности должна быть рассмотрена против этих измененных требований.

Организации должны проверить свою информационную управленческую непрерывность безопасности:

a) изучение и тестирование функциональности информационных процессов непрерывности безопасности, процедур и средств управления, чтобы гарантировать, что они совместимы с информационными целями непрерывности безопасности;

b) проверка и тестирование знания и установленного порядка, чтобы управлять информационными процессами непрерывности безопасности, процедурами и средствами управления, чтобы гарантировать, что их работа совместима с информационными целями непрерывности безопасности;

c) рассмотрение законности и эффективности информационной непрерывности безопасности имеет размеры, когда информационные системы, информационные процессы

безопасности, процедуры и средства управления или управленческое изменение процессов и решений управления/аварийного восстановления непрерывностью бизнеса.

Другая информация

Проверка информационных средств управления непрерывностью безопасности отличается от тестирования безопасности общей информации и проверки и должна быть выполнена вне тестирования изменений. Если возможно, предпочтительно объединить проверку информационных средств управления непрерывностью безопасности с непрерывностью бизнеса организации или тестами на аварийное восстановление.

17.2 Избыточность

Цель: гарантировать доступность средств для обработки информации.

17.2.1 Доступность средств для обработки информации

Меры управления

Средства для обработки информации должны быть осуществлены с избыточностью, достаточной, чтобы ответить требованиям доступности.

Руководство по реализации

Организации должны определить деловые требования для доступности информационных систем. Где доступность не может быть гарантирована, используя существующую архитектуру систем, избыточные компоненты или архитектуру нужно рассмотреть.

Где применимо, избыточные информационные системы должны быть проверены, чтобы гарантировать отказоустойчивость от одного компонента до другого компонента работы, как предназначено.

Другая информация

Внедрение увольнений может ввести риски для целостности или конфиденциальности информации и информационных систем, которые нужно рассмотреть, проектируя информационные системы.

18 Соответствие

18.1 Соответствие юридическим и договорным требованиям

Цель: избегать нарушений юридических, установленных законом, регулирующих или договорных обязательств, которые имеют отношение к информационной безопасности и любых требований безопасности.

18.1.1 Идентификация применимого законодательства и договорных требований

Меры управления

Все соответствующие законодательные установленные законом, регулирующие, договорные требования и подход организации, чтобы ответить этим требованиям, должны быть определены, зарегистрированы и усовершенствованы для каждой информационной системы и организации.

Руководство по реализации

Определенные средства управления и индивидуальная ответственность, отвечающая этим требованиям, должна также быть определена и зарегистрирована.

Менеджеры должны определить все законодательство, применимое к их организации, чтобы ответить требованиям для их типа бизнеса. Если организация ведет дело в других странах, менеджеры должны рассмотреть соблюдение во всех соответствующих странах.

18.1.2 Права на интеллектуальную собственность

Меры управления

Соответствующие процедуры должны быть осуществлены, чтобы гарантировать соответствие законодательным, регулирующим и договорным требованиям, связанным с правами на интеллектуальную собственность и использованием составляющих собственность программных продуктов.

Руководство по реализации

Следующие рекомендации, как должны полагать, защищают любой материал, который можно считать интеллектуальной собственностью:

a) публикация политики соблюдения прав на интеллектуальную собственность, которая определяет юридическое использование информационных продуктов и программного обеспечения;

b) приобретение программного обеспечения только через известные и уважаемые источники, чтобы гарантировать, что авторское право не нарушено;

c) поддержание осознания политики защитить права на интеллектуальную собственность и предоставление уведомления о намерении принять дисциплинарные меры против персонала, нарушающего их;

d) ведение соответствующих реестров актива и идентификация всех активов с требованиями, чтобы защитить права на интеллектуальную собственность;

e) поддерживающие доказательства и доказательства собственности лицензий, основных дисков, руководств, и т.д.;

f) внедрение мер управления, чтобы гарантировать, что любое максимальное количество пользователей, разрешенных в рамках лицензии, не превышено;

g) выполнение обзоров только по установленному программному обеспечению и лицензированным продуктам;

h) обеспечение политики для поддержания соответствующих условий лицензии;

i) обеспечение политики для избавления или передачи программного обеспечения другим;

j) исполнение положений и условий для программного обеспечения и информации получено из общедоступных сетей;

k) не дублирование, преобразования в другой формат или извлечение из коммерческих записей (фильм, аудио) кроме разрешенного законом об авторском праве;

l) не копирование полностью или частично, книги, статьи, докладов или других документов кроме разрешенного законом об авторском праве.

Другая информация

Права на интеллектуальную собственность включают авторское право программного обеспечения или документа, дизайнерские права, торговые марки, патенты и лицензии исходного кода.

Составляющие собственность программные продукты обычно поставляются в соответствии с лицензионным соглашением, которое определяет сроки действия лицензии и условия, например, ограничение использование продуктов к указанным машинам или ограничение копирования созданием резервных копий. Важность и осознание прав на интеллектуальную собственность должны быть сообщены штату для программного обеспечения, развитого организацией.

Законодательные, регулирующие и договорные требования могут установить ограничения для копирования составляющего собственность материала. В частности они могут потребовать, что только материал, который развит организацией или это лицензируется или обеспечивается разработчиком к организации, может использоваться. Нарушение авторского права может привести к судебному иску, который может включить штрафы и уголовное судопроизводство.

18.1.3 Защита отчетов

Меры управления

Отчеты должны быть защищены от потери, разрушения, фальсификации, несанкционированного доступа и несанкционированного выпуска, в соответствии с законодательными, регулирующими, договорными и деловыми требованиями.

Руководство по реализации

Когда решение защиты определенных организационных отчетов, их соответствующую классификацию, основанную на системе классификации организации, следует рассмотреть. Отчеты должны быть поделены на категории в рекордные типы, например, бухгалтерские отчеты, отчеты базы данных, журналы транзакций, контрольные журналы и эксплуатационные процедуры, каждого с деталями периодов задержания и типом допустимых носителей данных, например, бумагой, микрофишей, магнитной, оптической. Любые связанные ключи к шифру и программы, связанные с зашифрованными архивами или цифровыми подписями (см. пункт 10), должны также быть сохранены, чтобы позволить декодирование отчетов в течение отрезка времени, отчеты сохранены.

Внимание должно быть уделено возможности ухудшения данных, используемых для хранения отчетов. Хранение и процедуры обработки должны быть осуществлены в соответствии с рекомендациями изготовителя.

Где электронные носители данных выбраны, процедуры, чтобы гарантировать, чтобы способность получить доступ к данным (оба СМИ и удобочитаемость формата) в течение периода задержания была установлена, чтобы охранять против потери из-за будущего технологического изменения.

Системы хранения данных должны быть выбраны таким образом, что необходимые данные могут быть восстановлены в приемлемом периоде и формате, в зависимости от требований, которые будут выполнены.

Система хранения и обработки должна гарантировать идентификацию отчетов и их периода задержания, как определено национальным или региональным законодательством или инструкциями, если возможно. Настоящая система должна разрешить соответствующее разрушение отчетов после того периода, если они не необходимы организации.

Чтобы достигнуть этих рекордных целей охраны, следующие шаги должны быть взяты в организации:

a) рекомендации должны быть выпущены на задержании, хранении, обработке и избавлении от отчетов и информации;

b) график задержания должен быть составлен, определив отчеты и промежуток времени, в течение которого они должны быть сохранены;

c) инвентарь источников ключевой информации должен сохраняться.

Другая информация

Некоторые отчеты, возможно, должны быть надежно сохранены, чтобы ответить установленным законом, регулирующим или договорным требованиям, а также поддержать существенную деловую активность. Примеры включают отчеты, которые могут требоваться как доказательства, что организация работает в рамках установленных законом или регулирующих правил, чтобы гарантировать защиту против потенциального гражданского процесса или преступного деяния или подтвердить финансовое положение организации акционерам, третьим сторонам и аудиторам. Государственное право или регулирование могут установить период времени и содержание данных для информационного задержания.

Дополнительная информация об управлении организационными отчетами может быть найдена в [5].

18.1.4 Частная жизнь и защита личных данных

Меры управления

Частная жизнь и защита личных данных должны быть обеспечена, как требуется в соответствующем законодательстве и регулировании, когда это применимо.

Руководство по реализации

Политика данных организации для частной жизни и защиты личных данных должна развиваться и проводиться. Эта политика должна быть сообщена всем заинтересованным лицам в обработке личных данных.

Соответствие этой политике и всему соответствующему законодательству и инструкциям относительно защиты частной жизни людей и защиты личных данных требует соответствующей управленческой структуры и контроля. Часто это лучше всего достигнуто назначением ответственного человека, такого как чиновник частной жизни, который должен дать представление менеджерам, пользователям и поставщикам услуг на их индивидуальной ответственности и конкретных процедурах, которые должны быть выполнены. С ответственностью за обработку личных данных и обеспечение осознания принципов частной жизни нужно иметь дело в соответствии с соответствующим законодательством и инструкциями. Должны быть осуществлены соответствующие технические и организационные меры, чтобы защитить личные данные.

Другая информация

[25] служит основой высокого уровня для защиты личных данных в пределах систем информационно-коммуникационных технологий. Много стран ввели законодательство, осуществляя контроль над сбором, обработкой и передачей личных данных (обычно информация о живущих людях, которые могут быть опознаны от той информации). В зависимости от соответствующего национального законодательства такие средства управления могут наложить обязанности на тех, которые собирают, обрабатывают и распространяют личные данные, и могут также ограничить способность передавать личные данные другим странам.

18.1.5 Регулирование шифровальных средств управления

Меры управления

Шифровальные средства управления должны использоваться в соответствии со всеми соответствующими соглашениями, законодательством и инструкциями.

Руководство по реализации

Следующие пункты нужно рассмотреть для соответствия соответствующим соглашениям, законам и постановлениям:

a) ограничения на импорт или экспорт компьютерной техники и программного обеспечения для выполнения шифровальных функций;

b) ограничения на импорт или экспорт компьютерной техники и программного обеспечения, которое разработано, чтобы добавить шифровальные функции к нему;

c) ограничения на использование шифрования;

d) обязательные или контролируемые методы доступа властями стран к информации, зашифрованной аппаратными средствами или программным обеспечением, чтобы обеспечить конфиденциальность содержания.

За юридическим советом нужно обратиться, чтобы гарантировать соответствие соответствующему законодательству и инструкциям. Прежде чем зашифрованная информация или шифровальные средства управления перемещены через подведомственные границы, юридический совет должен также быть воспринят.

18.2 Информационные обзоры безопасности

Цель: гарантировать, что информационная безопасность осуществляется и управляется в соответствии с организационной политикой и процедурами.

18.2.1 Независимый обзор информационной безопасности

Меры управления

Подход организации к руководящей информационной безопасности и ее внедрение (т.е. цели контроля, средства управления, политика, процессы и процедуры информационной

безопасности) должны быть рассмотрены независимо в запланированных интервалах или когда существенные изменения происходят.

Руководство по реализации

Управление должно начать независимый обзор. Такой независимый обзор необходим, чтобы гарантировать продолжающуюся пригодность, соответствие и эффективность подхода организации к руководящей информационной безопасности. Обзор должен включать возможности оценки для улучшения и потребность в изменениях подхода к безопасности, включая цели контроля и политику.

Такой обзор должен быть выполнен людьми, независимыми от рассматривающейся области, например, функция внутреннего аудита, независимый менеджер или организация третьей стороны, специализирующаяся на таких обзорах. У людей, выполняющих эти обзоры, должны быть соответствующие навыки и опыт.

Результаты независимого обзора нужно зарегистрировать и сообщить управлению, которое начало обзор. Эти отчеты должны сохраняться.

Если независимый обзор определяет, что подход организации и внедрение к руководящей информационной безопасности - несоответствующие, например, зарегистрированные цели, и требованиям не отвечают, или не совместимы с направлением для информационной безопасности, прописанной в информационной политике безопасности (см. 5.1.1), управление должно рассмотреть корректирующие действия.

Другая информация

[12], «Рекомендации для информационной ревизии систем управления безопасностью» и [13], «Рекомендации для аудиторов на информационных мерах обеспечения безопасности» также дают представление для выполнения независимого обзора.

18.2.2 Соответствие политике безопасности и стандартам

Меры управления

Менеджеры должны регулярно рассматривать соблюдение обработки информации и процедур в пределах их сферы ответственности с соответствующей политикой безопасности, стандартами и любыми другими требованиями безопасности.

Руководство по реализации

Менеджеры должны определить, как рассмотреть информацию, что требования информационной безопасности, определенные в политике, стандартах и других применимых инструкциях, находятся в соответствии. Автоматическое измерение и сообщение об инструментах нужно рассмотреть для эффективного регулярного обзора.

Если какое-либо несоблюдение найдено в результате обзора, менеджеры должны:

a) определить причины несоблюдения;

b) оценить потребность в действиях, чтобы достигнуть соблюдения;

c) осуществить соответствующее корректирующее действие;

d) рассмотреть меры по ликвидации последствий, принятые, чтобы проверить его эффективность и определить любые дефициты или слабые места.

Результаты обзоров и корректирующих действий, выполненных менеджерами, должны быть зарегистрированы и настоящие отчеты должны сохраняться. Менеджеры должны сообщить о результатах людям, выполняющим независимые обзоры (см. 18.2.1), когда независимый обзор имеет место в области их ответственности.

Другая информация

Эксплуатационный контроль системного использования покрыт в 12.4.

18.2.3 Технический обзор соблюдения

Меры управления

Информационные системы должны регулярно рассматриваться для соответствия информационной политике безопасности и стандартам организации.

Руководство по реализации

Техническое соблюдение должно быть рассмотрено предпочтительно с помощью автоматизированных инструментов, которые производят технические отчеты для последующей интерпретации техническим специалистом. Альтернативно, ручные обзоры могли бы быть выполнены (поддержанный соответствующими программными средствами, если необходимо) опытным системным инженером.

Если тесты проникновения или оценки уязвимости используются, то предостережение должно быть осуществлено. Действия как таковые могли бы привести к компромиссу безопасности системы. Такие тесты должны быть запланированы, зарегистрированы и повторены.

Любой технический обзор соблюдения должен только быть выполнен компетентными, доверенными лицами или под наблюдением таких людей.

Другая информация

Технические обзоры соблюдения включают экспертизу эксплуатационных систем, чтобы гарантировать, что средства управления аппаратным и программным обеспечением были правильно осуществлены. Этот тип обзора соблюдения требует специалиста с техническими экспертными знаниями.

Обзоры соблюдения также касаются, например, тестирования проникновения и оценок уязвимости, которые могли бы быть выполнены независимыми экспертами, определенно законтрактованными с этой целью. Это может быть полезно в обнаружении слабых мест в системе и для осмотра, насколько эффективны средства управления в предотвращении несанкционированного доступа из-за этих слабых мест.

Тестирование проникновения и оценки уязвимости обеспечивают снимок системы в определенном государстве в определенное время. Снимок ограничен теми частями системы, фактически проверенной во время попытки (ок) проникновения. Тестирование проникновения и оценки уязвимости не замена для оценки степени риска.

[13] обеспечивает определенное руководство относительно технических обзоров соблюдения.

Библиография

[1] ISO/IEC, Directives, Part 2 (Директивы, Часть 2.)

[2] ISO/IEC 11770-1, *Information technology - Security techniques - Key management - Part 1: Framework (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент ключей. Часть 1. Структура)*

[3] ISO/IEC 11770-2, *Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques (Информационная технология. Методы и средства обеспечения безопасности. Управление ключами защиты. Часть 2. Механизмы, использующие симметричные методы)*

[4] ISO/IEC 11770-3, *Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques (Информационная технология. Методы и средства обеспечения безопасности. Управление ключами защиты. Часть 3. Механизмы, использующие ассиметричные методы)*

[5] ISO 15489-1, *Information and documentation - Records management - Part 1. General (Информация и документация. Управление записями. Часть 1. Общие требования)*

[6] ISO/IEC 20000-1, *Information technology - Service management - Part 1: Service management system requirements (Информационная технология. Менеджмент услуг. Часть 1. Требования к системе менеджмента услуг)*

[7] ISO/IEC 20000-2, *Information technology - Service management - Part 2: Guidance on the application of service management systems (Информационная технология. Менеджмент услуг. Часть 2. Руководство по применению систем менеджмента услуг)*

[8] ISO 22301, *Societal security - Business continuity management systems - Requirements (Социальная безопасность. Системы менеджмента непрерывности бизнеса. Требования)*

[9] ISO 22313, *Societal security - Business continuity management systems - Guidance (Социальная безопасность. Системы менеджмента устойчивости бизнеса. Руководство)*

[10] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements (Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования)*

[11] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности)*

[12] ISO/IEC 27007, *Information technology - Security techniques - Guidelines for information security management systems auditing (Информационная технология. Методы и средства обеспечения безопасности. Руководящие указания по аудиту систем менеджмента систем информационной безопасности)*

[13] ISO/IEC TR 27008, *Information technology - Security techniques - Guidelines for auditors on information security controls (Информационные технологии. Методы обеспечения защиты. Руководящие указания для аудиторов по оценке органов управления)*

[14] ISO/IEC 27031, *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity (Информационная технология. Методы и средства обеспечения безопасности. Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса)*

[15] ISO/IEC 27033-1, I*nformation technology - Security techniques - Network security - Part 1: Overview and concepts (Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции)*

[16] ISO/IEC 27033-2, *Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security (Информационная*

технология. Методы и средства обеспечения безопасности. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети)

[17] ISO/IEC 27033-3, *Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues (Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления)*

[18] ISO/IEC 27033-4, *Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways (Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности)*

[19] ISO/IEC 27033-5, *Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs) (Информационная технология. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных систем)*

[20] ISO/IEC 27035, *Information technology - Security techniques - Information security incident management (Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности)*

[21] ISO/IEC 27036-1, *Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts (Информационная технология. Методы и средства обеспечения безопасности. Защита информации для связей с поставщиками. Часть 1. Обзор и концепция)*

[22] ISO/IEC 27036-2, *Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements (Информационная технология. Методы и средства обеспечения безопасности. Защита информации для связей с поставщиками. Часть 2. Требования)*

[23] ISO/IEC 27036-3, *Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security (Информационная технология. Методы и средства обеспечения безопасности. Защита информации для связей с поставщиками. Часть 3. Руководящие указания по защите цепей поставки информационных и коммуникационных технологий)*

[24] ISO/IEC 27037, *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (Информационная технология. Методы и средства обеспечения безопасности. Руководящие указания по идентификации, сбору, приобретению и сохранению цифровых данных)*

[25] ISO/IEC 29100, *Information technology - Security techniques - Privacy framework (Информационная технология. Методы и средства обеспечения безопасности. Схема конфиденциальности)*

[26] ISO/IEC 29101, *Information technology - Security techniques - Privacy architecture framework (Информационные технологии. Технология обеспечения защиты. Архитектура для обеспечения конфиденциальности)*

[27] ISO 31000, *Risk management - Principles and guidelines (Менеджмент рисков. Принципы и руководящие указания)*

Приложение В.А
(информационное)

Таблица В.А.1 – Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств

Обозначение и наименование международного, регионального стандартов, стандарта иностранного государства	Степень соответствия	Обозначение и наименование национального стандарта, межгосударственного стандарта
ISO/IEC 27000:2012 Information technology - Security techniques - Information security management systems - Overview and vocabulary	IDT	СТ РК ISO/IEC 27000-2013 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь
ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements	IDT	СТ РК ISO/IEC 27001-201_* Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования.

_____
* Подлежит публикации.

УДК 534.322.3.08.006.354 **МКС 35.040**

Ключевые слова: информационные технологии, методы защиты информационной безопасности, программное обеспечение, риски, уязвимость, конфиденциальность, ответственность, патч, аутентификация, мобильные устройства, программа, активы, данные, идентификация, права доступа, криптография, шифр, угрозы, резервная копия, тестирование, инцидент, избыточность, шифровальные средства управления

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) 79 33 24