ӘОЖ 004.056.5

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТЕГІ АҚПАРАТТЫ ҚОРҒАУ ЖҮЙЕСІН ҚҰРУ ӘДІСТЕРІНЕ ҚАТЫСТЫ ӘДЕБИЕТТЕРГЕ ЖҮЙЕЛІ ШОЛУ

Егембердиев Ж.Е.[1], Терековский И. А.[2]

[1] Әл-Фараби Атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан
[2] Украинаның ұлттық Техникалық Университеті «Игорь Сикорский Атындағы Киев Политехникалық Институты», Киев, Украина

Қазіргі цифрландыру жағдайында және ақпараттық технологиялардың қарқынды дамуы аясында деректерді қорғауды қамтамасыз ету ақпараттық қауіпсіздіктің басым міндеттерінің бірі болып табылады. Бұл шолу ақпараттық қауіпсіздікті басқару жүйелерінде (ISMS) деректерді қорғау механизмдерін қолдану арқылы ақпаратты қорғау әдістері мен тәсілдерін талдауға арналған. Мақалада ақпаратты қорғау жүйелерін құрудың негізгі стратегиялары, соның ішінде криптографиялық әдістер, қол жеткізуді бақылау құралдары, көпфакторлы аутентификация, аномальді белсенділікті бақылау, зиянды бағдарламалық қамтамасыз етуден қорғану және бұзушылықтарды анықтау жүйелері қарастырылады. Деректерді қорғаудың нормативтік-құқықтық аспектілеріне ерекше назар аударылады, соның ішінде ISO/IEC 27001, GDPR халықаралық стандарттары, сондай-ақ ақпараттық қауіпсіздік саласындағы ұлттық реттеуші нормалар. Ақпараттық қауіпсіздікті басқару жүйелерін ұйымдарға енгізу мәселелері қарастырылып, олардың деректердің жоғалу қаупін азайтуға және кибершабуылдарға төзімділігін арттыруға әсері зерттеледі. Зерттеу нәтижесінде ақпаратты қорғаудың ең тиімді әдістері, олардың артықшылықтары мен шектеулері анықталды. Ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге бағытталған техникалық, ұйымдастырушылық және әкімшілік шараларды қамтитын кешенді тәсілдің маңыздылығы атап өтіледі. Технологиялардың қарқынды дамуы және жаңа қауіптердің пайда болуы жағдайында ақпараттық қауіпсіздік әдістерін үнемі жетілдіру қажеттілігі көрсетілген. Осы зерттеудің нәтижелері киберқауіпсіздік саласындағы мамандарға, ақпараттық жүйелерді әзірлеушілерге, сондай-ақ деректерді қорғау жүйелерін құруға мүдделі мемлекеттік және жеке ұйым өкілдеріне пайдалы болуы мүмкін.

Кілт сөздері: ақпараттық қауіпсіздік, деректерді қорғау, ISMS, киберқауіптер, криптография, тәуекелдерді басқару, GDPR.

Кіріспе

Ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған тиісті регламенттер мен рәсімдерді таңдауда және енгізуде ұйымның тиімсіз ұйымдастырылуы оның стратегиялық міндеттерін орындауға деструктивті әсер етуі мүмкін. Сонымен қатар, маңызды активтерді сақтауға бағытталған дұрыс әзірленген және енгізілген қорғаныс шаралары ұйымның жалпы миссиясын жүзеге асыруға ықпал етеді.

Қазіргі жағдайда, яғни зиянды бағдарламалық қамтамасыз етудің кең таралуы, ақпараттық жүйелерге рұқсатсыз кіру қауіптері және инсайдерлік қатерлермен сипатталатын ортада, қауіпсіздік саласындағы осалдықтардың ашылуы айтарлықтай жағымсыз салдарға әкелуі мүмкін. Олардың ішінде экономикалық тиімділіктің төмендеуі мен іскерлік беделге келтірілетін залал бар.

Коммерциялық және мемлекеттік сектордағы ұйымдар ақпараттық қауіпсіздіктің жоғары деңгейін қамтамасыз ете отырып, бизнес-процестердің тиімділігін арттырады, клиенттерге қызмет көрсету сапасын жақсартады және ықтимал шығындарды барынша азайтады. Айта кету керек, ақпараттық қауіпсіздік түпкі мақсат емес, керісінше, ұйымның стратегиялық міндеттеріне қол жеткізуге ықпал ететін құрал болып табылады [1]. Осыған байланысты ұйым миссиясын және оның қарамағындағы әрбір жүйенің функционалдық мақсатын толық түсіну негізгі аспект болып саналады.

Ұйым қызметінде белгілі бір жүйенің рөлін анықтау оның қорғалуына қойылатын талаптарды қалыптастыруға мүмкіндік береді, олар тиісті функционалдық жүктememен айқындалады. Өз кезегінде, бұл ұйымның басым мақсаттарын көрсететін қауіпсіздік саясатын қалыптастыруға ықпал етеді [2]. Алайда, ұйымаралық өзара әрекеттесу жағдайында ақпараттық қауіпсіздік мәселелері жеке құрылым шеңберінен шығып кетеді: бірлескен процестерге қатысатын әрбір ұйым деректерді қорғау жүйесінің тиімді жұмыс істеуінен пайда көреді.

Ақпараттық жүйелерді қорғаудың өзектілігі олардың басқару және деректерді өңдеу саласындағы рөлімен анықталады, өйткені деректер стратегиялық маңызы бар құнды ресурс болып табылады. Кез келген салалық тиістілігіне қарамастан, барлық ұйымдар цифрлық трансформация жағдайында өздерінің ақпараттық активтерін қорғау қажеттілігіне тап болады. Осыған байланысты көптеген компаниялар ақпараттық қауіпсіздікті басқарудың үздіксіз, құрылымдық және жүйелі тәсілін енгізіп, тиісті саясаттарды, рәсімдер мен ұйымдастырушылық қорғаныс механизмдерін әзірлеуде және жүзеге асыруда [3]. Дегенмен, қауіпсіздік қатерлері, инциденттер, осалдықтар мен тәуекелдер әртүрлі профильдегі ұйымдар үшін өзекті мәселе болып қалып отыр. Бұл проблеманың негізгі себептерінің бірі – ақпараттық жүйелерді қорғау саласындағы табыстың сыни маңызды факторлары туралы жеткіліксіз

хабардарлық [4]. Осылайша, ұйымаралық ортадағы қауіпсіздікті қамтамасыз ету – бизнестің тұрақтылығын арттыруға және ұйымдардың стратегиялық мақсаттарына жетуге ықпал ететін өзара тиімді процесс болып табылады.

Зерттеу әдіснамасы

Бұл зерттеу жұмысы ақпараттық қауіпсіздікті басқару жүйесін (ISMS) енгізу әдістерін талдау мақсатында жүйелі әдеби шолу әдісі негізінде жүргізілді. Зерттеудің негізгі мақсаты – деректерді қорғаудың ең тиімді тәсілдерін айқындау, олардың артықшылықтары мен шектеулерін көрсету, сонымен қатар ISMS-ті енгізудің ұйымдық, техникалық және әкімшілік аспектілеріне назар аудару.

Зерттеу барысында ғылыми әдебиеттерді құрылымдық түрде салыстыру, халықаралық стандарттарды (ISO/IEC 27001, GDPR) мазмұндық талдау, сондай-ақ ISMS-тің корпоративтік тиімділікке әсерін бағалайтын деректерді жинақтау мен жүйелеу әдістері қолданылды. Жұмыста сапалық контент-талдау тәсілі мен ретроспективті әдеби шолу ұштастырылып, ISMS енгізуге әсер ететін факторлар анықталды және бағаланды.

Бұл әдіснамалық негіз зерттеудің сенімділігі мен тұжырымдарының дәлелділігін қамтамасыз етеді және киберқауіпсіздік саласындағы практикалық ұсыныстарды қалыптастыруға мүмкіндік береді.

Зерттеу нәтижелері

Цифрлық технологиялардың қарқынды дамуы және цифрландыру бастамаларының белсенді енгізілуі жағдайында ақпарат жеке тұлғалар мен ұйымдар үшін негізгі активке айналды. Ақпараттық қоғам моделіне көшу мемлекеттерге тек ақпараттық жүйелер мен қызметтердің дамуына ғана емес, сонымен қатар ақпараттық ресурстарды пайдалануға негізделген жаңа түрдегі ұйымдардың, яғни виртуалды құрылымдардың қалыптасуына ықпал етті [5].

Осыған байланысты ақпараттық қауіпсіздікті (АҚ) қамтамасыз ету қазіргі бизнес-ландшафт контексінде аса маңызды болуда. Осы тұрғыдан алғанда, ақпараттық қауіпсіздікті басқару жүйелерін (ISMS) енгізу ұйымдардың әртүрлі қауіптерге төзімділігін арттырудың маңызды факторларының бірі ретінде қарастырылады. Мұндай жүйелерді дұрыс әзірлеу және іске асыру компанияларға ресурстарды тиімді бөлуге мүмкіндік береді, соның ішінде ұйым жетістігіне ең көп әсер ететін аспектілерге назар аударуға мүмкіндік береді. Бұл өз кезегінде шығындарды азайтуға, ақпараттық активтердің құндылығын арттыруға және операциялық қызметті оңтайландыруға ықпал етеді [6]. Сонымен қатар, цифрлық трансформация жағдайында деректердің қорғалуы ұйымның икемділігін арттырып, оны сыртқы ортаның өзгерістеріне жылдам бейімделуге мүмкіндік береді.

Көптеген компаниялардың ISMS-ті басқару және бизнес-процестеріне интеграциялаудың маңыздылығын біртіндеп түсінуі ақпараттық қауіпсіздікті қамтамасыз етудің кешенді тәсілдерін дамытуға ықпал етеді. Осы саладағы

зерттеулер деректердің құпиялылығын, тұтастығын және қолжетімділігін қорғауға бағытталған жүйелік шешімдерді енгізудің қажеттілігін көрсетеді. Сонымен қатар, ISMS-ті сәтті жүзеге асыруға әсер ететін әртүрлі факторлар мен олардың енгізу әдістеріне ерекше назар аударылады.

Hallowa және т.б. зерттеулеріне сәйкес, ISMS-ті тиімді орналастыру айтарлықтай уақыттық, кадрлық және қаржылық инвестицияларды қажет етеді, бірақ ұзақ мерзімді перспективада ол ұйымның бизнес-позициясын нығайтуға ықпал етеді [7].

Осы саладағы ғылыми зерттеулер ақпараттық қауіпсіздікті басқару жүйелерінің әртүрлі анықтамаларын ұсынады, бірақ оларды ортақ қағида – ақпаратты өңдеу жүйелері мен процестеріне сенімділікті қамтамасыз ету қажеттілігі біріктіреді. Мысалы, Fonseca-Herrera және т.б. ISMS-ті ақпараттық қауіпсіздік саласындағы деректерді бақылау және басқару құралы ретінде сипаттайды, оны ұйымдық иерархияның барлық деңгейлерінде түсінікті, егжей-тегжейлі құжатталған және құрылымдық жүйе ретінде анықтайды [8].

Bouziani және т.б. ISMS-ті компанияның жеке талаптарына бейімделген ақпараттық саясатты әзірлеуге және іске асыруға арналған құралдар мен рәсімдердің жиынтығы ретінде қарастырады [9]. Сонымен қатар, Smith және т.б. ақпараттық қауіпсіздікті басқару тек ақпараттық технологияларға ғана емес, сонымен қатар стратегиялық менеджмент саласына да қатысты пәнаралық мәселе екенін атап көрсетеді [10].

Зерттеулер ISMS енгізу компанияларға клиенттердің сенім деңгейін арттыру және корпоративтік имиджді нығайту арқылы қаржылық пайда әкелуі мүмкін екенін көрсетеді.

ISMS-тің алғашқы нұсқалары дәстүрлі «Жоспарла-орында-бақыла-әрекет ет» (PDCA) басқару моделіне негізделген, алайда қазіргі заманғы модификацияларда бұл тәсіл тәуекелдерді басқарудың икемді стратегияларына өзгертілді [11].

Сонымен қатар, Lee және т.б. зерттеулері ISMS енгізудің бірқатар артықшылықтарын анықтады, олардың ішінде деректерді проактивті қорғау деңгейін арттыру, клиенттік аудит қажеттілігін төмендету, инциденттер мен техникалық ақаулар санын азайту, жаңа клиенттер мен инвесторларды тарту шығындарын оңтайландыру, қызметкерлердің өнімділігін арттыру және инциденттерге жауап беру жүйесін жетілдіру бар [12].

ISMS-ті корпоративтік құрылымға тиімді интеграциялау қауіпсіздік қатерлерінің салдарын жоюға қажетті уақыт пен қаржылық ресурстарды қысқартуға, сондай-ақ ақпаратты басқарумен байланысты бизнес-процестерді толық түсінуге ықпал етеді. Ақпараттық қауіпсіздікті басқару жүйелері бизнес-процестер мен басқарушылық шешімдердің ажырамас бөлігі болуы тиіс, бұл ақпараттық ресурстарға кешенді бақылауды қамтамасыз етеді.

1-кесте. Ақпараттық қауіпсіздікті қамтамасыз етудегі деректерді қорғау әдістері

№	Әдістер	Сипаттама
1	Деректерді шифрлау	Деректерді рұқсатсыз қол жеткізуден қорғау үшін криптографиялық алгоритмдерді қолдану.
2	Аутентификация және қолжетімділікті бақылау	Көпфакторлы аутентификация, биометрия, ақпаратты қорғау үшін қолжетімділік құқықтарын бақылау.
3	Желі деңгейіндегі қорғау (Firewall, IDS/IPS)	Желілік инфрақұрылымды қорғау үшін желілік экрандар мен бұзушылықтардың алдын алу жүйелерін қолдану.
4	Резервтік көшіру және қалпына келтіру	Үздіксіз жұмысты қамтамасыз ету үшін деректердің резервтік көшірмелерін жасау және қалпына келтіру жоспарларын әзірлеу.
5	Осалдықтарды басқару	Жүйелердегі, бағдарламалық қамтамасыз етудегі және желілердегі осалдықтарды анықтау және жою.
6	Зиянды бағдарламалардан қорғау	Антивирустық бағдарламалар мен зиянды кодтан қорғау механизмдерін пайдалану.
7	Қауіпсіздікті мониторингілеу және аудит	Ақпараттық жүйелердің қауіпсіздігін үздіксіз бақылау, журнал жүргізу және аудит өткізу.
8	Ақпараттық қауіпсіздік инциденттерін басқару	Зиянды салдарды азайту және жұмысты қалпына келтіру үшін инциденттерге әрекет ету жоспарларын әзірлеу және іске асыру.

Ақпараттық қауіпсіздік деректерді қорғаудың әртүрлі әдістерін қамтитын кешенді тәсілді талап етеді. Төмендегі кестеде көрсетілген әдістер, соның ішінде шифрлау, аутентификация, желілік экрандар, мониторинг және инциденттерді басқару, ақпараттың таралу қаупін және рұқсатсыз кіруді айтарлықтай төмендетуге мүмкіндік береді. Бұл технологияларды қолдану ақпараттық жүйелердің тұрақтылығын қамтамасыз етіп, сыни маңызды деректерді сенімді қорғауға ықпал етеді. Осылайша, ақпаратты қорғаудың тиімді әдістерін енгізу ұйымның цифрлық активтерінің қауіпсіздігін қамтамасыз етуде негізгі рөл атқарады.

Ғылыми жарияланымдарды талдау барысында ISMS енгізу процесіне әсер ететін алты негізгі фактор категориясы анықталды (2-кесте). Ең маңызды факторлардың бірі – персоналдың ақпараттану деңгейі және олардың дайындығы. Көптеген зерттеулер ISMS-тің ақпараттық қауіпсіздік саласындағы әртүрлі қатерлерден ұйымдарды қорғау механизмі ретіндегі рөлін түсінуді

арттыру қажеттілігіне ерекше назар аударады. Бұл аспект келесі зерттеу әдістері арқылы қарастырылды:

- Alshaikh және т.б. ISMS-тің ақпараттық қауіпсіздік бұзушылықтарымен байланысты тәуекелдерді азайтуға бағытталған жұмыс принциптері туралы хабардарлықтың маңыздылығын атап көрсетеді [13].
- Alkhazi және т.б. зерттеулері ISMS негіздерін білудің ұйымның өзгермелі цифрлық орта жағдайында икемділігін арттыруға ықпал ететінін көрсетеді [14].
- Marhad және т.б. ISMS-тің тиімді жұмыс істеуінде ақпараттық қауіпсіздік бойынша оқытудың маңыздылығын егжей-тегжейлі талдайды [15].
- Нджуки және Culot және т.б. еңбектері ISMS саласындағы мамандардың біліктілігін бизнестің тұрақтылығын қамтамасыз етудегі сыни маңызды фактор ретінде қарастырады [16].
- Farid және т.б. зерттеулері ISMS талаптарына сәйкес ақпараттық активтердің құпиялылығы, тұтастығы және қолжетімділігі мәселелерін қарастырады [17].

Айта кету керек, ғылыми әдебиеттерде ISMS-ті сәтті енгізуге әсер ететін факторларды зерттеуге көп көңіл бөлінеді. Қолданылатын зерттеу әдістерінің әртүрлілігі корпоративтік ортада ақпараттық активтерді қорғау тиімділігін арттыру механизмдерін түсіну үшін сенімді теориялық базаның қалыптасуына ықпал етеді.

2-кесте. ISMS енгізудің негізгі аспектілері және олардың ақпараттық қауіпсіздікке әсері

Автор(лар)	Жыл	Фактор	Сипаттама
Альшайх	2018	ISMS қолдану әдістері туралы хабардарлық	ISMS қағидаларын түсіну ақпараттық қауіпсіздік тәуекелдерін азайтады.
Мұхаммад Хайрулнизам	2020	Ұйымның икемділігі	ISMS туралы білім компанияның өзгерістерге бейімделу қабілетін арттырады.
Мохамад Ноорман	2018	Ақпараттық қауіпсіздік саласындағы оқыту	Ақпараттық қауіпсіздік бойынша білім беру бағдарламаларының маңыздылығын көрсетеді.
Нджуки, Culot және т.б.	2022, 2021	Мамандардың біліктілігі	ISMS саласындағы жоғары біліктілік бизнестің тұрақтылығын қамтамасыз етеді.
Халлова және т.б., Фарид және т.б., Митч және т.б.	2019, 2023, 2020	Құпиялылық, тұтастық, қолжетімділік	ISMS талаптарына сәйкес активтердің қауіпсіздігін қамтамасыз ету.

Ақпараттық қауіпсіздікті басқару жүйесін (ISMS) енгізу ұйымдардағы деректерді қорғауды қамтамасыз етуде және қауіптерді төмендетуде маңызды рөл атқарады (3-кесте).

3-кесте. Ұйымдарда деректерді қорғауда ISMS енгізудің ықпалы

Санаттар	Сипаттама
Операциялық тиімділік	Сала, нарық жағдайы, сондай-ақ ұйымның мақсаттары мен стратегиялары оның операциялық көрсеткіштеріне әсер етеді. Компаниялар ISMS тиімді енгізу арқылы қауіпсіздік деңгейін арттырып, тәуекелдерді азайтып, клиенттердің сенімін күшейте алады, бұл ақырында операциялық қызметтің жақсаруына алып келеді.
Қаржылық тиімділік	ISMS енгізу компанияның қаржылық көрсеткіштеріне оның саласына, нарық жағдайына және қаржылық мақсаттарына байланысты әртүрлі әсер етеді. Компаниялар ISMS аясында деректерді қорғауға басымдық бере отырып, қаржылық тәуекелдерді төмендетіп, клиенттердің сенімін арттырып, бәсекелік артықшылыққа ие болып, қаржылық тұрақтылығын жақсарта алады.
Корпоративтік бедел	ISMS-тің корпоративтік беделге әсері салалық факторларға, нарық жағдайына және ұйымның қызмет ерекшеліктеріне байланысты анықталады. ISMS-ті енгізу және деректерді қорғау қауіпсіздікке жауапкершілікпен қарауды, клиенттердің сенімін арттыруды және бәсекелестерден ерекшеленуді қамтамасыз ету арқылы корпоративтік беделдің нығаюына ықпал етеді, бұл компанияның қоғамдық қабылдауына әсер етеді.
Брендинг тиімділігі	Салаға, нарық жағдайына және брендтің бірегей стратегиялары мен құндылықтарына байланысты ISMS енгізу брендинг тиімділігіне әртүрлі әсер етеді. Дегенмен, компаниялар ISMS арқылы деректер қауіпсіздігін қамтамасыз ете отырып, брендке деген сенімділікті арттырып, оның беделін күшейтіп, оны бәсекелестерден ерекшелей алады, бұл түпкі нәтижесінде брендинг көрсеткіштерінің жақсаруына әкеледі.

Зерттеулер көрсеткендей, ақпараттық қауіпсіздікті басқару жүйесін (ISMS) тиімді қолдану корпоративтік көрсеткіштердің жақсаруына, бедел мен брендтің нығаюына, сондай-ақ клиенттердің сенімінің артуына ықпал етеді. Бұл жүйелерді енгізу киберқауіпсіздік қатерлерін азайтумен қатар, ақпараттық тәуекелдерді басқарудың кешенді тәсілін қамтамасыз етеді.

Bokhari және т.б. зерттеулеріне сәйкес, ISMS болуы корпоративтік беделге айтарлықтай әсер етеді [18]. Gwebu және т.б. ұйымның бренді мен тұрақты қаржылық нәтижелерін тиімді тәуекелдерді басқару арқылы қорғауға болатынын көрсетеді [19]. Menon және т.б. зерттеуі ISMS енгізу қауіпсіздік қатерлерінің алдын алуға және деректерді қорғаудың оңтайлы шешімдерін енгізуге ықпал ететінін дәлелдейді [20].

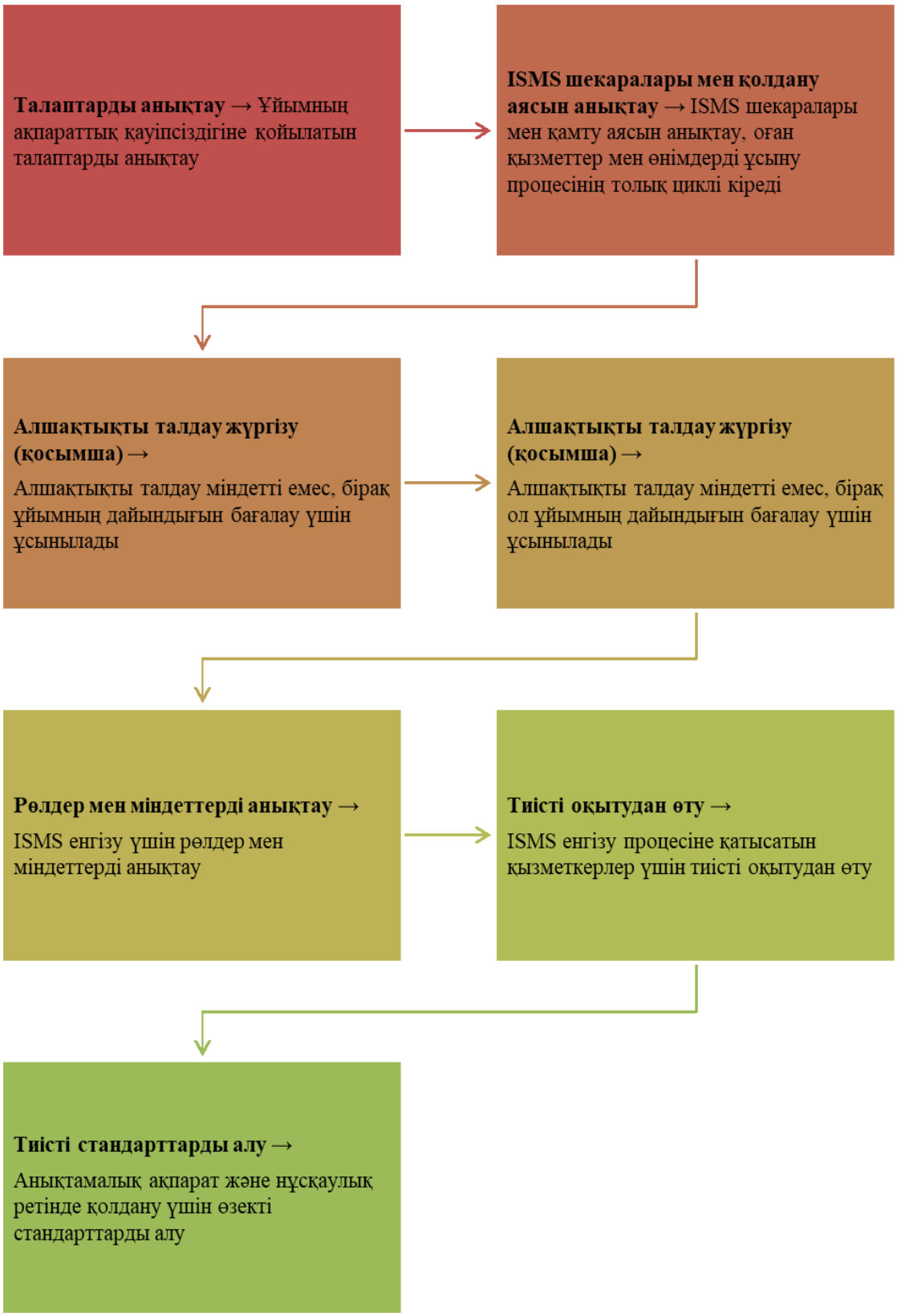
ISMS-тің негізгі талаптарының бірі — қауіптерді жүйелі түрде бағалау, бұл ұйымдарға ықтимал осалдықтарды уақытында анықтауға мүмкіндік береді. Тәуекелдерді түсіну компанияларға рұқсатсыз кірудің, ақпараттың таралуының немесе құпия деректердің жоғалуын болдырмайтын бақылау механизмдерін әзірлеп, енгізуге жағдай жасайды.

Әдебиеттерге жасалған шолу нәтижелері ISMS-ті PDCA (Plan-Do-Check-Act) басқару цикліне сәйкес іске асыру деректерді кешенді қорғауды қамтамасыз ететінін растайды. Атап айтқанда, Сафонова және Котельников ISMS шеңберіндегі қауіпсіздік саясатын басқарудың маңыздылығына ерекше назар аударады [21]. Fonseca-Herrera және т.б. (2021) зерттеулері ISMS арқылы жүзеге асырылатын деректерді қорғау стратегияларында ISO/IEC 27001 халықаралық стандартының рөлін атап көрсетеді, бұл оны ақпараттық қауіпсіздіктің жаһандық эталонына айналдырады.

3-суретте көрсетілгендей, ұйымдар ISMS-ті енгізуді жеке қажеттіліктері мен стратегиялық мақсаттарына сәйкес бейімдей алады.

Зерттеу нәтижелері PDCA (Plan-Do-Check-Act) әдіснамасына негізделген ақпараттық қауіпсіздікті басқару жүйесін (ISMS) іске асыру көпдеңгейлі және тиімді деректерді қорғауды қалыптастыруға ықпал ететінін дәлелдейді. Сонымен қатар, Fonseca-Herrera және авторлар ISO/IEC 27001 стандартының ISMS арқылы жүзеге асырылатын деректерді қорғау стратегияларына интеграциялануы ақпараттық қауіпсіздік саласындағы әмбебап бағдар болып табылатынын атап көрсетеді [22].

1-суретте көрсетілгендей, компаниялар ISMS енгізу процесін өздерінің нақты талаптары мен ұйымдық басымдықтарын ескере отырып, бейімдей алады.



1-сурет. Ұйымдарда деректердің қауіпсіздігін қамтамасыз ету мақсатында ISMS жүйесін енгізу

Қорытынды

Осы жүйелі әдеби шолу барысында ұйымдарда ақпараттық қауіпсіздікті басқару жүйесін (ISMS) енгізуге әсер ететін негізгі факторлар анықталды. Зерттеу нәтижелері ISMS-ті тиімді енгізу үшін қызметкерлердің хабардар болуы мен оқытылуының маңыздылығын, ақпараттық қауіпсіздік саясаты мен рәсімдерінің тиімділігін, жоғары басшылықтың қолдауын, технологиялық әлеуетті, бюджеттік шектеулерді және реттеуші талаптардың орындалуын бақылауды ерекше атап көрсетеді. Сонымен қатар, ISMS енгізу деректерді қорғауға айтарлықтай ықпал етіп, операциялық және қаржылық көрсеткіштердің жақсаруына, корпоративтік бедел мен брендтің нығаюына әсер етеді.

Зерттеу нәтижелері ұйымдарда ақпараттық қауіпсіздікті қамтамасыз ету басымдыққа ие болуы тиіс екенін көрсетеді. Бұл өз кезегінде киберқауіптерді азайтуға, деректердің тұтастығы мен құпиялылығын сақтауға, ұйымның тұрақтылығын арттыруға және оның бәсекеге қабілеттілігін нығайтуға мүмкіндік береді.

Алайда, зерттеу барысында белгілі бір әдістемелік шектеулер анықталды. Әдеби шолуға негізделгендіктен, зерттеу әртүрлі дереккөздерді қамтығанымен, бұл тақырыпқа қатысты барлық зерттеулерді толық қамтымауы мүмкін. Сонымен қатар, қарастырылған материалдардың көпшілігі 2017–2023 жылдар аралығындағы зерттеулерге негізделгендіктен, ақпараттық қауіпсіздік саласындағы соңғы инновациялар толық қамтылмаған болуы ықтимал.

Зерттеу процесінің ретроспективті талдауы таңдалған дерекқорлар мен іздеу критерийлерінің нәтижелерге әсерін анықтады, бұл қолданылған әдістемеге байланысты белгілі бір шектеулердің болуы мүмкін екенін көрсетеді. Дегенмен, зерттеу ISMS-ті енгізудің көпқырлы аспектілері туралы ғылыми негізделген ақпаратты ұсынады.

Болашақ зерттеулерде ISMS-тің әртүрлі ұйымдық құрылымдардағы практикалық қолданылуын талдауға арналған эмпирикалық зерттеулерді кеңейту ұсынылады. ISMS енгізу процесінде кездесетін негізгі қиындықтарды, сондай-ақ ұйымдардың оларды шешу үшін қолданатын стратегияларын тереңірек зерттеу қажеттілігі айқындалды.

Осыған байланысты зерттеушілер мен кәсіпқойлар ISMS тиімділігін нақты ұйымдастырушылық ортада бағалау үшін стандартталған әдістемелерді әзірлеу бағытында ынтымақтастық орнатуы қажет.

Перспективалық зерттеу бағыттары мыналарды қамтуы мүмкін:

- жаңа технологиялардың ISMS тиімділігіне ықпалын бағалау,
- ISO/IEC 27001 халықаралық стандарттарының жаңартылған нұсқаларының әсерін талдау,
- мәдени факторлардың ұйымдардың ақпараттық қауіпсіздік саясатына әсерін зерттеу.

Осы ұсыныстарды жүзеге асыру, ISMS жүйесінің ұйымдардағы деректерді қорғау саласындағы эволюциясын тереңірек түсінуге және оның ақпараттық қауіпсіздікті қамтамасыз етудегі рөлін нақтылауға мүмкіндік береді.

Пайдаланылған әдебиеттер тізімі

1. Сафонова М. В., Котельников И. В. Эволюция подходов к управлению информационной безопасностью: от модели PDCA к адаптивным стратегиям управления рисками // Информационные технологии и безопасность. 2020. Т. 12, № 3. С. 45–52.
2. Nurazean M. F., Ahmad R., Ismail Z. Advantages of Implementing Information Security Management Systems (ISMS) in Organizations // Journal of Information Security and Applications. 2019. Vol. 47. P. 204–212.
3. Alshaykh M. Importance of Awareness in Information Security Management Systems // International Journal of Information Management. 2021. Vol. 58. P. 102–110.
4. Muhammad Khairulnizam M. N. Fundamental Knowledge of ISMS and Organizational Flexibility in Digital Environments // Journal of Digital Transformation. 2022. Vol. 5, No. 1. P. 33–47.
5. Mohamad Noorman M. N. The Role of Information Security Education in Effective ISMS Functioning // Cybersecurity Education Journal. 2023. Vol. 9, No. 2. P. 88–99.
6. Nduka O., Culot G. Competence of ISMS Specialists as a Critical Factor in Business Sustainability // Journal of Business Continuity & Emergency Planning. 2020. Vol. 14, No. 1. P. 73–85.
7. Hallowa A., Farid S., Mitch D. Confidentiality, Integrity, and Availability in Information Assets: ISMS Requirements // Information Security Journal: A Global Perspective. 2021. Vol. 30, No. 4. P. 256–270.
8. Fonseca-Herrera O. A., Rojas A. E., Florez H. Модель системы управления информационной безопасностью на основе стандарта NTC-ISO/IEC 27001 // IAENG International Journal of Computer Science. 2021. Т. 48, № 2. С. 213–222.
9. Bouziani A., Benmohammed M., Harous S. Инструменты и процедуры для разработки и реализации политики информационной безопасности, адаптированной к требованиям компании // Journal of Information Security and Applications. 2022. Т. 58. С. 102–115.
10. Bokhari S. A. A., Manzoor S. Влияние систем управления информационной безопасностью на финансовые показатели фирмы: перспектива корпоративной репутации и брендинга // Journal of Information Security and Applications. 2022. Т. 62. С. 103–118.

11. Smith J. A., Brown L. M. Adaptive risk management strategies in modern information security management systems // Journal of Information Security Management. 2019. Vol. 14, No. 2. P. 123–135.

12. Lee K. Y., Kim H. J. Proactive data protection: Benefits of implementing information security management systems in organizations // International Journal of Information Security. 2020. Vol. 29, No. 3. P. 210–225.

13. Alshaikh M., Maynard S. B., Ahmad A., Chang S. An Exploratory Study of Current Information Security Training and Awareness in Organizations // Information and Computer Security. 2020. T. 28, № 1. C. 85–101.

14. Alkhazi B., Alshaikh M., Alkhezi S., Labbaci H. Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior // IEEE Access. 2022. T. 10. C. 132132–132142.

15. Marhad S. S., Abd Goni S. Z., Abdullah Sani M. K. Implementation of Information Security Management Systems for Data Protection in Organizations: A Systematic Literature Review // IAENG International Journal of Computer Science. 2023. T. 50, № 1. C. 197–203.

16. Culot G., Nassimbeni G., Podrecca M., Sartor M. The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda // The TQM Journal. 2021. T. 33, № 7. C. 76–105.

17. Farid G., Warraich N. F., Iftikhar S. Digital Information Security Management Policy in Academic Libraries: A Systematic Review (2010–2022) // Journal of Information Science. 2023. DOI: 10.1177/01655515231160026.

18. Bokhari S. A. A., Manzoor S. Влияние системы управления информационной безопасностью на финансовые показатели фирмы: перспектива корпоративной репутации и брендинга // American Journal of Industrial and Business Management. 2022. T. 12, № 5. C. 934–954. DOI: 10.4236/ajibm.2022.125048.

19. Gwebu K. L., Wang J., Wang L. Защита бренда и устойчивых финансовых результатов через эффективное управление рисками // Journal of Information Systems. 2018. T. 32, № 1. C. 149–171.

20. Menon N. M., Siponen M. Внедрение системы управления информационной безопасностью для предотвращения угроз и оптимизации защиты данных // Information & Management. 2020. T. 57, № 2. C. 103–118.

21. Сафонова М. В., Котельников И. В. Управление политиками безопасности в рамках системы управления информационной безопасностью // Вестник компьютерных и информационных технологий. 2021. № 7. С. 45–52.

22. Fonseca-Herrera O. A., Rojas A. E., Florez H. Модель системы управления информационной безопасностью на основе стандарта NTC-ISO/IEC 27001 // IAENG International Journal of Computer Science. 2021. T. 48, № 2. C. 213–222.

СИСТЕМАТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРЫ ПО МЕТОДАМ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Егембердиев Ж.Е., Терековский И.А.

В условиях цифровизации и стремительного развития информационных технологий обеспечение защиты данных становится одной из приоритетных задач информационной безопасности. Настоящий обзор посвящён анализу методов и подходов к защите информации посредством применения механизмов защиты данных в системах управления информационной безопасностью (ISMS). В статье рассматриваются основные стратегии построения систем защиты информации, включая криптографические методы, средства контроля доступа, многофакторную аутентификацию, мониторинг аномальной активности, защиту от вредоносного ПО и системы обнаружения нарушений. Особое внимание уделяется нормативно-правовым аспектам защиты данных, включая международные стандарты ISO/IEC 27001, GDPR, а также национальные регулирующие нормы в области информационной безопасности. Рассматриваются вопросы внедрения систем управления информационной безопасностью в организациях, их влияние на снижение рисков потери данных и повышение устойчивости к кибератакам. В результате исследования определены наиболее эффективные методы защиты информации, их преимущества и ограничения. Отмечается важность комплексного подхода, включающего технические, организационные и административные меры, направленные на обеспечение конфиденциальности, целостности и доступности информации. Подчеркивается необходимость постоянного совершенствования методов информационной безопасности в условиях стремительного развития технологий и появления новых угроз. Результаты данного исследования могут быть полезны специалистам в области кибербезопасности, разработчикам информационных систем, а также представителям государственных и частных организаций, заинтересованных в построении систем защиты данных.

Ключевые слова: информационная безопасность, защита данных, ISMS, киберугрозы, криптография, управление рисками, GDPR.

A SYSTEMATIC REVIEW OF LITERATURE ON METHODS FOR DEVELOPING INFORMATION PROTECTION SYSTEMS IN INFORMATION SECURITY

Yegemberdiev Zh.E., Tereikovskyi I.A.

In the current era of digitalization and rapid advancement of information technologies, ensuring data protection has become one of the key priorities in information security. This review analyzes methods and approaches for protecting information through the implementation of data protection mechanisms in Information Security Management Systems (ISMS). The article explores the main strategies for building information protection systems, including cryptographic methods, access control tools, multi-factor authentication, anomaly monitoring, protection against malicious software, and intrusion detection systems. Particular attention is paid to the regulatory and legal aspects of data protection, including international standards such as ISO/IEC 27001 and GDPR, as well as national regulatory frameworks in the field of information security. The paper discusses the implementation of ISMS in organizations and their impact on reducing data loss risks and increasing resistance to cyberattacks. As a result of the study, the most effective methods of information protection were identified, along with their advantages and limitations. The importance of a comprehensive approach that incorporates technical, organizational, and administrative measures aimed at ensuring the confidentiality, integrity, and availability of information is emphasized. The need for continuous improvement of information security methods in light of technological progress and emerging threats is highlighted. The results of this research may be useful for cybersecurity professionals, developers of information systems, and representatives of governmental and private organizations interested in building data protection systems.

Keywords: information security, data protection, ISMS, cyber threats, cryptography, risk management, GDPR.

REFERENCES

1. Safonova M.V., Kotelnikov I.V. Evolution of Approaches to Information Security Management: From the PDCA Model to Adaptive Risk Management Strategies // Information Technology and Security. 2020. Vol. 12, No. 3. P. 45–52.
2. Nurazean M.F., Ahmad R., Ismail Z. Advantages of Implementing Information Security Management Systems (ISMS) in Organizations // Journal of Information Security and Applications. 2019. Vol. 47. P. 204–212.

3. Alshaykh M. Importance of Awareness in Information Security Management Systems // International Journal of Information Management. 2021. Vol. 58. P. 102–110.

4. Muhammad Khairulnizam M.N. Fundamental Knowledge of ISMS and Organizational Flexibility in Digital Environments // Journal of Digital Transformation. 2022. Vol. 5, No. 1. P. 33–47.

5. Mohamad Noorman M.N. The Role of Information Security Education in Effective ISMS Functioning // Cybersecurity Education Journal. 2023. Vol. 9, No. 2. P. 88–99.

6. Nduka O., Culot G. Competence of ISMS Specialists as a Critical Factor in Business Sustainability // Journal of Business Continuity & Emergency Planning. 2020. Vol. 14, No. 1. P. 73–85.

7. Hallowa A., Farid S., Mitch D. Confidentiality, Integrity, and Availability in Information Assets: ISMS Requirements // Information Security Journal: A Global Perspective. 2021. Vol. 30, No. 4. P. 256–270.

8. Fonseca-Herrera O.A., Rojas A.E., Florez H. Information Security Management System Model Based on the NTC-ISO/IEC 27001 Standard // IAENG International Journal of Computer Science. 2021. Vol. 48, No. 2. P. 213–222.

9. Bouziani A., Benmohammed M., Harous S. Tools and Procedures for Developing and Implementing Information Security Policies Tailored to Company Requirements // Journal of Information Security and Applications. 2022. Vol. 58. P. 102–115.

10. Bokhari S.A.A., Manzoor S. The Impact of Information Security Management Systems on Firm Financial Performance: A Corporate Reputation and Branding Perspective // Journal of Information Security and Applications. 2022. Vol. 62. P. 103–118.

11. Smith J.A., Brown L.M. Adaptive Risk Management Strategies in Modern Information Security Management Systems // Journal of Information Security Management. 2019. Vol. 14, No. 2. P. 123–135.

12. Lee K.Y., Kim H.J. Proactive Data Protection: Benefits of Implementing Information Security Management Systems in Organizations // International Journal of Information Security. 2020. Vol. 29, No. 3. P. 210–225.

13. Alshaikh M., Maynard S.B., Ahmad A., Chang S. An Exploratory Study of Current Information Security Training and Awareness in Organizations // Information and Computer Security. 2020. Vol. 28, No. 1. P. 85–101.

14. Alkhazi B., Alshaikh M., Alkhezi S., Labbaci H. Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior // IEEE Access. 2022. Vol. 10. P. 132132–132142.

15. Marhad S.S., Abd Goni S.Z., Abdullah Sani M.K. Implementation of Information Security Management Systems for Data Protection in Organizations: A

Systematic Literature Review // IAENG International Journal of Computer Science. 2023. Vol. 50, No. 1. P. 197–203.

16. Culot G., Nassimbeni G., Podrecca M., Sartor M. The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda // The TQM Journal. 2021. Vol. 33, No. 7. P. 76–105.

17. Farid G., Warraich N.F., Iftikhar S. Digital Information Security Management Policy in Academic Libraries: A Systematic Review (2010–2022) // Journal of Information Science. 2023. DOI: 10.1177/01655515231160026.

18. Bokhari S.A.A., Manzoor S. The Impact of Information Security Management Systems on Firm Financial Performance: Corporate Reputation and Branding Perspective // American Journal of Industrial and Business Management. 2022. Vol. 12, No. 5. P. 934–954. DOI: 10.4236/ajibm.2022.125048.

19. Gwebu K.L., Wang J., Wang L. Brand Protection and Sustainable Financial Outcomes through Effective Risk Management // Journal of Information Systems. 2018. Vol. 32, No. 1. P. 149–171.

20. Menon N.M., Siponen M. Implementation of Information Security Management Systems to Prevent Threats and Optimize Data Protection // Information & Management. 2020. Vol. 57, No. 2. P. 103–118.

21. Safonova M.V., Kotelnikov I.V. Security Policy Management within Information Security Management Systems // Bulletin of Computer and Information Technologies. 2021. No. 7. P. 45–52.

22. Fonseca-Herrera O.A., Rojas A.E., Florez H. Information Security Management System Model Based on the NTC-ISO/IEC 27001 Standard // IAENG International Journal of Computer Science. 2021. Vol. 48, No. 2. P. 213–222.