МРНТИ 50.11.15 DOI 10.48501/2786.2023.43.91.010

Жумадилова М.Б.[1], Жұмажан Б.А.[1]
[1]Yessenov University
Қазақстан, Ақтау
e-mail: zhumazhanb@bk.ru

МЕМЛЕКЕТТІК МЕКЕМЕЛЕРДІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІНЕ ТӨНЕТІН ҚАТЕЛЕРДІ МОДЕЛЬДЕУ МӘСЕЛЕЛЕРІН ЗЕРТТЕУ

Аннотация. Мақалада мемлекеттік дерекқорлар мен автоматтандырылған ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз етудің қазіргі кездегі өзекті мәселесі қарастырылған. Ақпараттық қауіпсіздікті қамтамасыз етудің қолданыстағы тәсілдері талданды. Әр түрлі көрсеткіштерді талдау арқылы мемлекеттік деректер базасы мен автоматтандырылған ақпараттық жүйелердің ақпараттық қауіпсіздігіне қауіп төндіретін факторлардың үш блогы анықталды. Осы блоктардың ішінен қазақстандық ортаға тән деректердің қауіпсіздігіне төнетін қателерді модельдеу мәселелері зерттелді. Мәліметтер базасы мен ААЖ (автоматтандырылған ақпараттық жүйелер) ақпаратын қорғау жүйесін қалыптастыру кезінде кешенді тәсілдің қажеттілігі туралы қорытынды негізделген. Мемлекеттік сектор контекстінде ақпараттық қауіпсіздікке кешенді көзқарас құрылымының блок-схемасы әзірленді. Сондай-ақ малақада ақпараттық қауіпсіздік ұғымы, зерттеу салалары, әдіснамасы шеңбері қарастырылады, ресурстар ұсынылады және ақпараттық қауіпсіздік саласындағы қауіптердің мысалдары келтірілді.

Түйін сөздер: Ақпараттық қауіпсіздікті қамтамасыз ету, деректер базасы, автоматтандырылған ақпараттық жүйе, мемлекеттік сектор, ақпаратты қорғау.

Zhumadilova M.B[.1], Zhumazhan B.A.[1]
[1]Yessenov University
Kazakhstan, Aktau
e-mail: zhumazhanb@bk.ru

Research of problems of modeling errors of information security of public institutions

Annotation. The article discusses the current urgent problem of ensuring information security of state databases and automated information systems. The existing approaches to ensuring information security were analyzed. Through the analysis of various indicators, three blocks of factors that threaten the information security of state databases and automated information systems were identified. From these blocks, the problems of modeling errors that threaten the security of data inherent in the Kazakhstan environment were studied. The conclusion on the need for an integrated approach in the formation of a system for protecting information from databases and AIS (automated information systems) is justified. A block diagram of the structure of an integrated approach to information security in the context of the public sector has been developed. Also in Malaka, the concept of information security, research areas, the framework of the methodology are considered, resources are presented and examples of threats in the field of information security are given.

Keywords: Information Security, database, automated Information System, Public Sector, Information Protection.

Жумадилова М.Б.[1], Жумажан Б.А.[1]
[1]Yessenov University
Казахстан, Ақтау
e-mail: zhumazhanb@bk.ru

Исследование проблем моделирования ошибок информационной безопасности государственных учреждений

Аннотация. В статье рассмотрен актуальный на сегодняшний день вопрос обеспечения информационной безопасности государственных баз данных и автоматизированных информационных систем. Проанализированы существующие подходы к обеспечению информационной безопасности. Анализом различных показателей выявлены три блока факторов, представляющих угрозу информационной безопасности государственных баз данных и автоматизированных информационных систем. Из этих блоков исследованы проблемы моделирования ошибок безопасности данных, присущих Казахстанской среде. Обоснован вывод о необходимости комплексного подхода при формировании системы защиты информации базы данных и АИС (автоматизированных информационных систем). Разработана блок-схема структуры комплексного подхода к информационной

безопасности в контексте государственного сектора. Также будут рассмотрены понятие информационной безопасности, области исследований, рамки методологии, представлены ресурсы и приведены примеры угроз в области информационной безопасности.

Ключевые слова: обеспечение информационной безопасности, базы данных, автоматизированная информационная система, государственный сектор, защита информации.

Әр мемлекетте ақпараттық қауіпсіздік саласындағы міндеттерді қою және шешу үшін өзіндік және жиі ерекше жағдайлар қалыптасады. Осыған қарамастан, ақпараттық қауіпсіздік саласындағы мемлекеттік саясаттың идеалды моделін бөліп көрсетуге болады, оның негізінде қызметтің осы түрін жүзеге асырудың ұқсас міндеттері мен технологиялары бар. Ақпараттық салаға қатысты іс-қимыл стилін, мемлекеттік қауіпсіздік мәселелеріне жалпы қатынасты анықтайтын осындай мүдделерді түсіну сипаты деп айтуға болады.

Ұлттық мүдделерді түсіндіруді ескере отырып, ақпараттық қауіпсіздік саласындағы мемлекеттік саясатты қалыптастыру жолындағы келесі қадам – ақпараттық қорғауға жататын объектілерді анықтау. Әдетте, мұндай объектілерге мыналар жатады:

- жалпы елдің ақпараттық кеңістігі;
- қызметі мемлекетті басқару және оның ресурстық жабдықталуының өсуі үшін ерекше маңызы бар институттар, құрылымдар және жеке тұлғалар;
- жетекші экономикалық және әлеуметтік құрылымдар (мысалы, әуе кеңістігін басқару жүйелері, теміржол қозғалысы, басқа да жоғары жылдамдықты көлік жүйелері, Денсаулық сақтау жүйесі, мұнда өлім-жітімнің энергетикалық және электрондық желілердегі ақауларға тәуелділігі жоғары және т.б.);
- жетекші ақпараттық-техникалық жүйелер;
- ақпараттық-талдамалық құрылымдар;
- белгілі бір актордың қызметі туралы нақты ақпарат;
- ақпараттық ресурстар (мәліметтер базасы);
- жеке экономикалық және күштік құрылымдар.

Мемлекеттің іс-қимыл кешені оның ұлттық мүдделері туралы, тек ақпараттық ғана емес, сонымен бірге кең әлеуметтік-саяси саладағы идеялардан туындайды. Бұл мүдделер туралы айтпағанда, олар тек прагматикалық сипатта болуы мүмкін (мемлекетті қызметтің әртүрлі салаларында нақты пайда табуға талпындырады) және мифологиялық (осы институттың барлық қызметін басқаратын белгілі бір жетекші доктринаның, идеяның, идеологияның болуын болжайды). Ақпараттық салаға қатысты бұл осы түрді түсінудің сипаты деп айтуға болады

Мемлекеттік мекемелердегі ақпараттық қауіпсіздік ұғымын қарастыру қажеттілігі тұтастай қоғамдағы ақпарат ұғымының маңыздылығының артуына, атап айтқанда ұйым мен мемлекеттің мүдделерін қорғау қажеттілігіне байланысты.

Мемлекеттік мекемелердегі ақпараттық қауіпсіздік ұғымын, ең алдымен, мемлекет пен ұйымның қаржылық мүдделерін қорғау тұрғысынан қарастырады, ақпараттық қауіпсіздік жүйелерін енгізу және пайдалану құнын және тәуекелдер мен қауіптерден болатын шығындарды салыстырумен айналысады.

Мемлекеттік мекемелердегі ақпараттық қауіпсіздіктің рөлі ақпараттық қауіпсіздік құралдары мен әдістерінің мемлекет пен ұйымдардың экономикалық тұтастығына төтеп беру қабілетімен анықталады.

Сарапшылардың пікірінше, мемлекеттік мекемелердегі ақпараттық қауіпсіздік мәселелерін зерттеуде ойын теориясы мен әлеуметтік-экономикалық жүйелерді модельдеуді, факторлық талдауды және диалектикалық әдісті қамтитын әдіснаманы қолданады. Жалпы ғылыми әдістердің ішінде жүйелік тәсіл, салыстырмалы талдау, статистикалық және ситуациялық талдау және тарихи әдіс ерекше маңызға ие [1].

Ақпараттық қауіпсіздік бағыттарын зерттеу үшін математикалық әдістердің ішінде зерттеушілер математикалық

статистика теориясы мен ықтималдық теориясын, математикалық және корреляциялық талдауды, математикалық модельдеуді және графикалық теорияны бөліп көрсетеді.

Ақпараттық қауіпсіздік мәселелерін зерттеу кезінде ғылыми сала мамандары ақпараттық қауіпсіздікті ішкі және сыртқы бұзушылардың модельдерін құруды, ақпараттық қауіпсіздік жүйесін бағалау және оңтайландыру үшін бастапқы деректер жүйесін қалыптастыру моделін құруды және ақпараттық қауіпсіздік жүйесінің тиімділігін бағалаудың математикалық моделін жасауды қамтитын модельдеу әдістемесін қолданады.

Техникалық және технологиялық прогресс, сондай-ақ ақпараттық-телекоммуникациялық технологиялардың дамуы деректердің үлкен массивінің жинақталуына және айналымдағы ақпараттық массаның геометриялық өсуіне алып келеді [1].

Мәліметтер мен ақпараттардың алуан түрлілігінің артуына қарай оларды жүйелеу, құрылымдау, өңдеу және сақтау әдістері мен тәсілдері одан әрі тиімді пайдалану үшін пайда болды. Сонымен, жоғарыда аталған деректер жиынтығымен және ақпаратпен өзара әрекеттесу мақсаты жалпы концептуалды белгілерді құрайды, бұл «деректер базасы» және «автоматтандырылған ақпараттық жүйе» [2].

Бүгінгі таңда мемлекеттік деректер қоры мен автоматтандырылған ақпараттық жүйелер мемлекеттің жұмыс істеуі мен қоғамның қызмет ету жүйесінің негізгі элементтері болып табылады. Мемлекеттік органдар басқаратын дерекқорлар мен автоматтандырылған ақпараттық жүйелерде қамтылған ақпарат өте маңызды және құпия болып табылады, олар еркін айналымға арналмаған, сондықтан қол жеткізуді шектеу және қауіпсіз жұмыс істеуді қамтамасыз ету қағидасының сақталуы қатаң бақыланады. Мемлекеттік дерекқорлар мен автоматтандырылған ақпараттық жүйелерде қамтылған ақпарат пен деректердің жоғары құндылығы әртүрлі мүдделі субъектілер мен жеке тұлғалардың оларды өз мүдделері үшін алу және одан әрі пайдалану мақсатында қызығушылық тудырады [3]. Бұл құпия деректер мен ақпараттың қауіпсіздік проблемасын тудырады. Осылайша, құпия ақпараттың қауіпсіздігін талдауға маманданған компаниялардың соңғы есептерін талдай отырып, оқиғалар санының тұрақты өсу үрдісі байқалады деуге болады. 2019 жылы ақпараттың қауіпсіздігі бойынша қателер 2018 жылмен салыстырғанда 22%-ға көп тіркелді. InfoWatch аналитикалық орталығының мәліметіне сәйкес, 2006 жылы 157 жағдай болса, 2019 жылы 1276 оқиға тіркеліп, 8 еседен астам өсті [6].Сонымен қатар бұқаралық ақпарат құралдарында мемлекеттік деректер қорынан және автоматтандырылған ақпараттық жүйелерден ақпараттың қауіпсіздігі туралы фактілері бар жаңалықтар жиі шығады [7,8,9]. Жоғарыда аталған тезистер мемлекеттік мекемелердің ақпараттық қауіпсіздігіне төнетін мәселелердің өзектілігін растайды.

Мәліметтер қорының даму тарихын екі кезеңге бөлуге болады. Бірінші кезең, сөздің кең мағынасында, электрондық есептеуіш машиналарды қолданбай белгілі бір көлемдегі мәліметтерді құрылымдауға, ұйымдастыруға, өңдеуге және сақтауға бағытталған кез келген саналы әрекет деп сипаттауға болады. Мысалы, біздің дәуірімізге дейінгі 4000 жылы Оңтүстік Месопотамияның ежелгі халқы (шумерлер) өздерінің күнделікті өмірінде патша қазынасы мен халықтан алынатын салықтардың есебін жүргізуді әдетке айналдырған [4]. Бұл тарихи факт деректермен жұмыс істеудің пәндік саласының қалыптасуының басталуын белгіледі және ол электронды есептеуіш машиналар пайда болғанға дейін жалғасты. Бұл мысалда деректер қоры мен автоматтандыру ұғымы мұрағаттау мен жазу салаларының қиылысында жалпыланған түрде берілгенін атап өткен жөн. Деректер қоры туралы нақты ақпараттар л 1960 жылдардың ортасында пайда болды. General Electric корпорациясының негізінде компьютерлік бағдарламаларды жасау саласындағы американдық ғалым Чарльз Уильям Бахман әлемдегі бірінші IntegratedDataStore (IDS) өнімділігі жоғары желілік мәліметтер базасын жасады. 1964 жылы IDS жалпы кешенді операциялық

жүйемен (GCOS) жұмыс істейтін GE-200 компьютерінде жұмыс істейтін жалпы жұртшылыққа ұсынылды. Осы дамуы үшін 1973 жылы Бахман информатика саласындағы ең беделді марапат – Тьюринг сыйлығын алды [5]. Жоғарыда аталған факті пайда болған сәттен бастап бүгінгі күнге дейін бұл кезеңді мәліметтер қорының пәндік саласын дамытудың екінші кезеңі деп дұрыс белгілеуге болады.

Қазіргі ғылыми қоғамдастықта мәселенің зерттелу дәрежесін талдай отырып, авторлар ақпаратқа төнетін қауіптерлі екі негізгі топқа жіктейді: тікелей және жанама.

Жанамаларға мыналар жатады:

- сақтау құралдарын ұрлау немесе жоғалту;
- қашықтықтан суретке түсіру, тыңдау;
- электромагниттік сәулеленуді ұстау.

Тікелей мыналарды қамтиды:

- инсайдизм (адам факторы);
- тікелей көшіру.

Сонымен қатар, ақпараттың ағып кету арналарын физикалық қасиеттері мен жұмыс принциптеріне сәйкес бөлуге болады. Бұл бөлу 1-суретте көрсетілген.

Сурет 1. Ақпараттың ағып кету арналарын физикалық қасиеттері мен жұмыс істеу принциптері бойынша бөлу

Зерттеу пәні саласындағы ғылыми әдебиеттер мен нормативтік құқықтық актілерді талдау әдісін қолдана отырып, мемлекеттік деректер қоры мен автоматтандырылған ақпараттық жүйелердің ақпараттық қауіпсіздігіне қауіп төндіретін факторлардың үш блогын бөліп көрсетеміз:

- технологиялық,
- кадрлық,
- құқықтық қамтамасыз ету.

Технологиялық факторға техниканың, технологияның, инновацияның және ғылымның дамуымен байланысты құралдар жатады. Мысалы, өнертабыстар, машиналар, аппараттық және бағдарламалық қамтамасыз ету, жүйелер мен желілер. Қауіпсіздік қатерінің адам факторына дерекқормен және ААЖ-мен әрекеттесетін тірі субъектіге әсер етумен тікелей байланысты аймақтар жатады. Бұл жағдайда субъект сөздің кең мағынасында адам, жеке тұлға ретінде түсініледі. Ол бұрыннан рұқсат алған бар қызметкер, оператор, серіктес, контрагент, тіпті еріксіз иеленуші немесе дерекқорға және ААЖ-ға кіруге айналған жеке тұлға ретінде әрекет ете алады.

Ақпараттық қауіпсіздікке адам қауіпінің болуын анықтайтын негізгі шарттар жеке тұлғаның болуы және оның бар ақпараты немесе оны алу мүмкіндігі болып табылады. Бұл жағдайда ақпарат алу сценарийін іске асыру кезінде әсер ету объектісіне (адамға, жеке тұлғаға) көзқарас оның ұстанымы немесе мәртебесі емес, адамның табиғаты тұрғысынан әсер етудің психофизиологиялық әдістері мен

тәсілдеріне негізделеді. [10]. Сондай-ақ, біз бұл салаға жеке тұлғаның жеке басының ерекшеліктерімен және психологиялық ерекшеліктерімен негізделетін жеке материалдық қызығушылықты қосамыз [11]. Үшінші блок ақпараттық қауіпсіздік пен қорғау саласындағы құқықтық реттеуді және мемлекеттік саясатты әзірлеуді қамтиды. Бұған заңдар да, доктриналар да, Қазақстан Республикасы Президентінің жарлықтары да, республикалық деңгейде қабылданған халықаралық стандарттар да, сондай-ақ ішкі құжаттар, мәліметтер базасының немесе ААЖ операторы ретінде әрекет ететін мемлекеттік орган шеңберінде әзірленген шешімдер де жатады [12,13,14,15]. Адам факторы блогы бойынша ақпаратқа қауіп төндіретін мәселелер Қазақстан Республикасының мемлекеттік органдарына қатысты болуы мүмкін екенін атап өткен жөн. Осылайша, InfoWatch сараптамалық талдау орталығы зерттеу жүргізіп, 2020 жылдың 9 айында бүкіл әлем бойынша коммерциялық компаниялардан, мемлекеттік ұйымдардан және билік органдарынан шектеулі ақпаратқа төнетін қауіптердің 1 773 оқиғасы тіркелгенін көрсетті. Барлығы 9,93 миллиард жеке деректер мен төлем деректерінің жазбалары бұзылған. Қазақстанда зерттеу кезеңінде қолжетімділік шектелген ақпараттың 302 ағып кетуі тіркелді, бұл 2019 жылдың қаңтар-қыркүйек айларымен салыстырғанда 5,6%-ға көп. Зерттеу авторлары бүкіл әлем бойынша сыртқы шабуылдаушылардың әсерінен ақпаратқа төнетін қауіптердің артқанын атап өтті. Жоғарыда келтірілген мәліметтерге сүйене отырып, 2-суретте берілген блок-схеманы құрастырдық.

Сурет 2. Мемлекеттік ДБ және ААЖ ақпараттық қауіпсіздігіне қатер факторларының блок-схемасы

Қазақстан Республикасындағы мемлекеттік деректер базаларының және автоматтандырылған ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету мәселесін зерттеуді қорытындылай келе, негізгі қорытынды ақпараттық қауіпсіздік жүйесін құру және деректердің ағып кетуіне жол бермеу кезінде кешенді тәсілді қолдану қажеттілігі болып табылады. Мәліметтер қоры мен автоматтандырылған ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету құрылымының қаңқасын құрайтын үш блок анықталды – техникалық, адами және құқықтық. Ақпараттың ағып кетуінің ең көп пайызы болатын мемлекеттік деректер базасының қауіпсіздігін қамтамасыз ету тұрғысынан ең осал «адам факторы» блогы болып табылады. Бұл факторлар блогы үшін ең үлкен тәуекел қазақстандық мемлекеттік секторға тән екенін атап өткіміз келеді, басқа елдерде

техникалық блок басым, бұл бұрын жүргізілген зерттеулермен расталады. Сондықтан ең үлкен қауіпсіздік ресурстары осы блокта орналастырылуы керек. Айта кету керек, коммерциялық секторда жағдай керісінше және ең көп ресурстар «техникалық фактор» блогына жұмсалады. Бұл айырмашылық дерекқорлардағы ақпарат пен деректердің сипатына байланысты. Егер коммерциялық секторда бұл субъектінің экономикалық қызметіне қатысты ақпарат болса, мемлекеттік секторда бұл елдің қызметі мен өмірі туралы стратегиялық маңызды ақпарат болып табылады. Осыған сәйкес мұндай ақпаратты алу мақсаттары әртүрлі. Бірінші жағдайда, мақсат, әдетте, қаржылық пайда алумен шектелсе, екіншіден, алынған мәліметтерді саяси, әлеуметтік, экономикалық, ғылыми-техникалық және т.б. мақсаттарда қолдану болып табылады. Осы мақаладағы ақпарат мемлекеттік органдарға және басқа да мүдделі ұйымдарға олардың дерекқорлары мен автоматтандырылған ақпараттық жүйелерінің ақпараттық қауіпсіздігін қамтамасыз ету құрылымын іс жүзінде құруда пайдалы болады, сондай-ақ деректер базаларының және автоматтандырылған ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз етудің пәндік саласын әзірлеуге қосымша ғылыми үлес қосады.

Ақпараттық қауіпсіздік саласындағы зерттеушілердің пікірінше, ақпараттық қауіпсіздік мәселелерін зерттеудің негізгі міндеттеріне ақпаратты түсінудің жаңа тәсілдерін қалыптастыру және ақпарат құбылысын экономикалық ресурс ретінде зерттеу, ақпараттық қауіпсіздік теориясының негізгі ережелерін экономикалық зерттеу бағыттарына бейімдеу және өндірістік қатынастардың ақпараттық компонентін зерттеу, ақпараттың құнын бағалау әдістерін құру жатады [16].

Ақпараттық қауіпсіздік саласындағы қолданбалы зерттеулерге мамандар қаржылық дағдарыстар мен тұрақсыздыққа ақпараттық қауіпсіздік құралдарымен қарсы тұру, Қазақстанның ақпараттық қауіпсіздігі мәселесінің сыртқы экономикалық аспектілерін зерттеу және оның ақпараттық қауіпсіздігін қамтамасыз ету, жаһандану жағдайында Қазақстанның ақпараттық қауіпсіздігін күшейтудің перспективалары мен басымдықтарын анықтау және сыртқы экономикалық ақпараттың республикасын жүйесін құруды ұсынады. Басқа міндеттердің қатарында зерттеушілер Қазақстанның ұлттық мүдделеріне зиян келтіру үшін ақпараттық технологиялардың әлеуетін пайдалану қаупіне қарсы тұру және сыртқы экономикалық қатынастарға қазақстандық қатысушылардың ақпараттық қауіпсіздігін қамтамасыз ету мәселелерін зерттеу, Қазақстандағы ақпараттық-коммуникациялық технологияларды нормативтік-құқықтық қамтамасыз етуді басты нысанға қояды.

Зерттеушілер ақпараттық қауіпсіздікке төнетін тәуекелдер мен қауіп-қатерлерге қатысты міндеттерді бөлек санатқа бөледі, соның ішінде ақпараттық қауіпсіздікке төнетін қатерлерді жіктеу және ақпараттық тәуекелдерді жүйелеу, ақпараттық тәуекелдерді азайту, әртүрлі типтегі кәсіпорындар үшін ақпараттық қауіпсіздік қатерлерінің жіктелуін талдау және нақтылау, ақпараттық қауіпсіздікке төнетін қауіптердің арақатынасын талдау және жаңа ақпараттық тәуекелдерді анықтауды ұсынады. Осы салаға қатысты басқа міндеттердің қатарында ақпараттық тәуекелдерді бағалау әдістемелерін талдау және әзірлеу, ақпараттық қауіпсіздік шараларына салынған қаражатқа тәуекелдің тәуелділік қасиеттерін анықтау, ұйымның ақпараттық тәуекелдерін бағалауды автоматтандыру және ақпараттық тәуекелдерге байланысты шығындарды азайту, ақпараттық тәуекелдерді басқару бойынша ұсыныстар әзірлеу бөлінеді.

Мемлекеттік мекемелердегі ақпараттық қауіпсіздіктің қалған міндеттеріне мамандар ақпараттық-есептеу процесін ұйымдастырудың ерекшеліктерін анықтау және кәсіпорынның жекелеген объектілері бойынша ақпараттық қауіпсіздіктің жай-күйін бағалау, ақпараттық қауіпсіздікті арттыру үшін ақпараттық технологияларды пайдаланудың шетелдік тәжірибесін талдау және жүйелеу, іскерлік ақпараттың сапасы мен сенімділігіне қойылатын талаптарды

анықтау жатады, экономикалық қауіпсіздік деңгейін арттыру үшін ақпараттық технологияларды пайдалану тәжірибесін жүйелеу және ақпаратты қорғауды қамтамасыз ету міндеттеріне сәйкес мемлекет пен ұйымның қаржы ағындарын бөлуді негізге алады. Басқа міндеттер қатарында мемлекеттік мекемелердің ақпараттық қауіпсіздікті қорғауға қойылатын талаптар деңгейіне қарай жіктелуі, ақпараттық қауіпсіздік объектілерін статистикалық зерттеу көрсеткіштері мен әдістерін әзірлеу, ақпараттандыру процестерін жоспарлау және болжау, аймақтың ақпараттық қауіпсіздік объектілерінің тәсілдері мен жіктелуін әзірлеу, басқару объектілерінің ақпараттық қауіпсіздік саласын зерттеу, ақпараттық қауіпсіздік тұрғысынан қорғалған, өндірістік жүйелер және қолданыстағы жүйелердің тиімділігін талдау бар.

Ең перспективалы міндеттердің қатарында жеке және заңды тұлғалардың ақпараттық тәуекелдерін сақтандыру жүйесін құру және ақпараттық тәуекелдер бойынша тарифтік ставкаларды есептеу, сондай-ақ ақпараттық қауіпсіздік қатерлерін бейтараптандырудың экономикалық әдістерін зерттеуді бөліп көрсетуге болады.

Мемлекеттік мекемелердегі ақпараттық қауіпсіздік мәселелерін шешуде үлкен рөл атқаратынын атап өткен жөн, өйткені мемлекеттік мекемелер шеңберінде әзірленген әдістеме қауіпсіздік саласында және қауіптер мен тәуекелдердің экономикалық салдарын есептеуде, ақпаратты қорғау құралдарын сатып алуға және пайдалануға байланысты шығындарды жоспарлауда кеңінен қолданылды.

Екінші жағынан, ақпараттық қауіпсіздік және ақпарат теориясы саласындағы зерттеулер аясында жасалған әдістер мен әзірлемелер экономикалық саладағы бұзушылықтарға қарсы тұруда, ұйымның, мемлекеттің, жеке тұлғаның экономикалық қауіпсіздігін қорғауда кеңінен қолданылды.

Әдебиеттер

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994 г.
2. Кабанов А.С., Лось А.Б., Першаков А.С., Теоретические основы компьютерной безопасности, М: РИО МИЭМ, 2010 г.
3. Проскурин В.Г., Защита программ и данных, ИД «Академия», 2011 г.
4. Емельянов, В. В. ШУМЕР // Большая российская энциклопедия. — М., 2017. — Т. 35. – С. 153—155.
5. Andrew L. Russell. Oral-History:Charles Bachman. IEEE Oral History Network (April 9, 2011)
6. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года // INFOWATCH.RU – Официальный сайт аналитического центра InfoWatch. URL: infowatch.ru
7. Марютина Т. М., Ермолаев О. Ю. Введение в психофизиологию. – М., 2004. – 400 с.
8. Логинова Н.А. Психологическая наука – дело всей жизни Бориса Герасимовича Ананьева // Санкт-Петербургский университет. – 2007.
9. Доктрина информационной безопасности Российской Федерации // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document
10. И.Н.Кохтюлина «Информационная безопасность на внешнеэкономическом треке: современные методы анализа» // «Российский внешнеэкономический вестник» №2, 2009.
11. И.Н.Кохтюлина «Информационная составляющая внешнеэкономической безопасности Российской Федерации», М.: Полпред, 2008.
12. И.Н.Кохтюлина «Некоторые аспекты информационной безопасности на внешнеэкономическом треке» // «Бизнес и безопасность в России» №1, 2009.
13. А.Б.Табаков «На страже. Информационная безопасность бизнеса» // «Русский полис» № 5(61), 2005.
14. Д.И.Тараторин «Формирование системы исходных данных для оценки и оптимизации системы информационной безопасности» // Вестник ИНЖЭКОН № 3(12). СПб.: СПбГИЭУ, 2006.
15. А.С.Саввин «Проблемы обеспечения информационной безопасности страны» // Пятнадцатые международные плехановские чтения. М.: Изд-во Российской экономической академии, 2002.
16. В.В.Немиткина «Применение методов оптимизации при анализе и управлении информационными рисками» // «Экономика и математические методы» № 2, Т.44, 2008.

References

1. Gerasimenko V.A. Zashhita informacii v avtomatizirovannyh sistemah obrabotki dannyh. – M.: Jener-goatomizdat, 1994 g.
2. Kabanov A.S., Los' A.B., Pershakov A.S., Teoreticheskie osnovy komp'juternoj bezopasnosti, M: RIO MIJeM, 2010 g.
3. Proskurin V.G., Zashhita programm i dannyh, ID «Akademija», 2011 g.
4. Emel'janov, V. V. ShUMER // Bol'shaja rossijskaja jenciklopedija. — M., 2017. — T. 35. – S. 153—155.
5. Andrew L. Russell. Oral-History:Charles Bachman. IEEE Oral History Network (April 9, 2011)
6. Global'noe issledovanie utechek konfidencial'noj informacii v pervom polugodii 2019 goda // IN-FOWATCH.RU – Oficial'nyj sajt analiticheskogo centra InfoWatch. URL: infowatch.ru
7. Marjutina T. M., Ermolaev O. Ju. Vvedenie v psihofiziologiju. – M., 2004. – 400 s.
8. Loginova N.A. Psihologicheskaja nauka – delo vsej zhizni Borisa Gerasimovicha Anan'eva // Sankt-Peterburgskij universitet. – 2007.
9. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii // Spravochnaja pravovaja sistema «Kon-sul'tantPljus». URL: http://www.consultant.ru/document
10. I.N.Kohtjulina «Informacionnaja bezopasnost' na vneshnejekonomicheskom treke: sovremennye metody analiza» // «Rossijskij vneshnejekonomicheskij vestnik» №2, 2009.
11. I.N.Kohtjulina «Informacionnaja sostavljajushhaja vneshnejekonomicheskoj bezopasnosti Rossijskoj Fede-racii», M.: Polpred, 2008.
12. I.N.Kohtjulina «Nekotorye aspekty informacionnoj bezopasnosti na vneshnejekonomicheskom treke» // «Biznes i bezopasnost' v Rossii» №1, 2009.
13. A.B.Tabakov «Na strazhe. Informacionnaja bezopasnost' biznesa» // «Russkij polis» № 5(61), 2005.
14. D.I.Taratorin «Formirovanie sistemy ishodnyh dannyh dlja ocenki i optimizacii sistemy informa-cionnoj bezopasnosti» // Vestnik INZhJeKON № 3(12). SPb.: SPbGIJeU, 2006.
15. A.S.Savvin «Problemy obespechenija informacionnoj bezopasnosti strany» // Pjatnadcatye mezhduna-rodnye plehanovskie chtenija. M.: Izd-vo Rossijskoj jekonomicheskoj akademii, 2002.
16. V.V.Nemitkina «Primenenie metodov optimizacii pri analize i upravlenii informacionnymi riska-mi» // «Jekonomika i matematicheskie metody» № 2, T.44, 2008.

Сведения об авторе

Жумадилова Мереке Бапановна
Должность: К.т.н, доцент, заведующая кафедрой «Компьютерные науки» КГТИУ им. Ш. Есенова
Почтовый адрес: 130000, Республика Казахстан, г.Актау
Сот. тел: +7 (707) 689 33 66
E-mail: mereke.zhumadilova@yu.edu.kz
Zhumadilova Mereke Bapanovna
Position: candidate of technical sciences, associate professor, head of the "Computer Science" department CSUTE named after Sh. Yesenov
Mailing address: 130000, Republic of Kazakhstan, Aktau city
Mob.phone: +7 (707) 689 33 66
E-mail: mereke.zhumadilova@yu.edu.kz

Жұмажан Бекежан Амандықұлы
Лауазымы: ақпарттық жүйелер магистрі, Yessenov University
Пошталық мекен-жайы: 130000, Қазақстан Республикасы, Ақтау қаласы, 17 ш-а 92 үй 12 пәтер
Ұялы.тел 87788129531
E-mail: zhumazhanb@bk.ru
Жумажан Бекежан Амандыкулы
Должность: магистр информационных систем, Yessenov University
Почтовый адрес: 130000, Республика Казахстан, г. Актау, 17 мкр. 92, кв. 12
Сот. тел: 87788129531
E-mail: zhumazhanb@bk.ru
Zhumazhan Bekezhan
Position: master of Information system, Yessenov University
Mailing address: 130000, Republic of Kazakhstan, Aktau, 17 mkr. 92-12
Mob.phone: 87788129531
E-mail: zhumazhanb@bk.ru