ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

ҚазҰТЗУ ХАБАРШЫСЫ

ВЕСТНИК КазНИТУ

VESTNIK KazNRTU

№ 3 (139)

АЛМАТЫ 2020 ИЮНЬ

ISSN 1680-9211

Учредитель:

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Регистрация:

Министерство культуры, информации и общественного согласия
Республики Казахстан № 951 – Ж “25” 11. 1999 г.

Основан в августе 1994 г. Выходит 6 раз в год

Адрес редакции:

г. Алматы, ул. Сатпаева, 22,
каб. 609, тел. 292-63-46
Nina. Fedorovna. 52 @ mail.ru

УДК 004.056.53

S. Adilzhanova, G. Tyulepberdinova, G.Gaziz, M.Sakypbekova
(Al Farabi Kazakh National university, Almaty, Kazakhstan.
E-mail: asaltanat81@gmail.com)

ANALYSIS OF MATHEMATICAL METHODS FOR DYNAMIC MANAGEMENT OF CYBERSECURITY RESOURCES OF INFORMATIZATION OBJECTS

Abstract. This article discusses many threats, vulnerabilities, and risks information system. Communication models are offered information risks and resources that can reduce data risks. Based on these models, the optimal search is performed allocation of resources to reduce information security risks safety. As a result, the complexity of security systems and increase their cost. The development of issues is particularly relevant optimization of the performance of the system of information protection in terms of dynamic confrontation.

Key words: cyber defense, cybercrime, dynamic management, information space, information security.

С.А. Адилжанова, Г.А. Тюлепбердинова, Г. Ғазиз, М.Ж. Сақыпбекова
(Әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан)

АҚПАРАТТАНДЫРУ ОБЪЕКТІЛЕРІНІҢ КИБЕРҚАУІПСІЗДІК РЕСУРСТАРЫН ДИНАМИКАЛЫҚ БАСҚАРУДЫҢ МАТЕМАТИКАЛЫҚ ӘДІСТЕРІН ТАЛДАУ

Андатпа. Бұл мақалада ақпараттық жүйенің көптеген қатерлері, осалдықтары мен тәуекелдері қарастырылады. Ақпараттық тәуекелдер мен ресурстардың байланыс модельдері ұсынылады, олар осы тәуекелдерді төмендетуі мүмкін. Мұндай модельдер негізінде ақпараттық қауіпсіздік тәуекелдерін төмендетуге ресурстарды оңтайлы бөлуді іздестіру жүргізіледі. Нәтижесінде - қорғау жүйелерін күрделендіру және олардың құнын ұлғайту. Динамикалық қарсы тұру жағдайында ақпаратты қорғау жүйесінің көрсеткіштерін оңтайландыру мәселелерін әзірлеу ерекше өзектілікке ие болады.

Түйін сөздер*:* киберқорғау, киберқылмыс, динамикалық басқару, ақпараттық кеңістік, ақпаратты қорғау.

Кіріспе

Қазіргі уақытта ақпараттық қауіпсіздік саласындағы оқыс оқиғалардың күрт өсуі байқалады, олар кең таралған және қауіпті сипатқа ие. Мұндай шабуылдардың көпшілігі жеке, корпоративтік, сондай-ақ мемлекеттік мүдделердің кең ауқымын қозғайды. Қауіптерді дамытудың басты үрдістері мыналар болып табылады: көптеген шығындарға әкелетін шабуылдар санының өсуі; бірнеше кезеңді қамтитын және қарсы іс-қимылдың ықтимал әдістерінен қорғаудың арнайы әдістерін қолданатын шабуылдар күрделілігінің өсуі.; іс жүзінде барлық электрондық (цифрлық) құрылғыларға әсер ету, олардың ішінде соңғы уақытта мобильді құрылғылар барынша үлкен мәнге ие болады, ал олар ақпараттық қауіпсіздік саласындағы тәуекелдерге барынша бейім; ірі корпорациялардың, аса маңызды өнеркәсіптік объектілердің және тіпті мемлекеттік құрылымдардың ақпараттық инфрақұрылымына шабуыл жасаудың барынша жиі орын алуы; компьютерлік технологиялар саласында неғұрлым дамыған елдердің басқа мемлекеттерге киберқылмыс құралдары мен әдістерін қолдануы. Бұл ақпарат саласындағы қылмыскерлердің жаңа шабуылдары туралы хабарланатын күнделікті жаңалықтармен расталады.

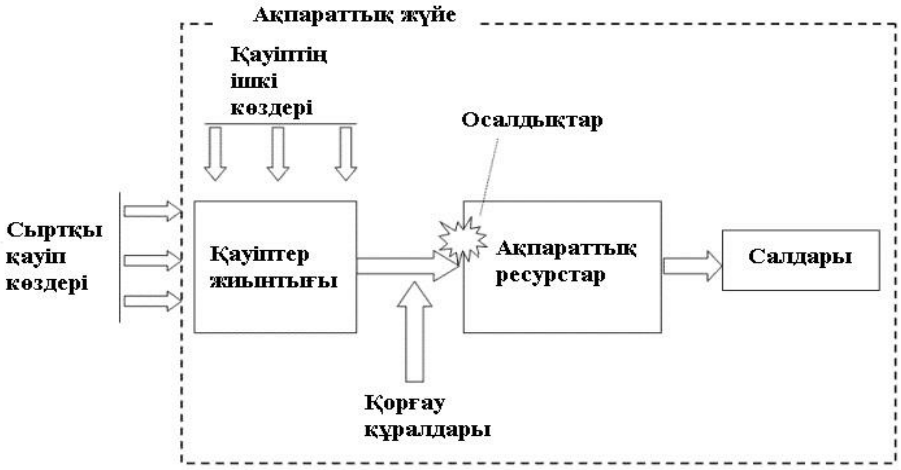
Зерттеу әдістері.

Ақпаратты тиімді қорғау-бұл ең маңызды заманауи проблемалардың бірі, өйткені ақпараттық ресурс Қазіргі әлемдегі экономикалық дамудың басты түйткілдерінің бірі болды. XXI ғасырдың жоғары ақпараттық технологияларын қолдану, бір жағынан, кәсіпорындар мен ұйымдардың қызметінде елеулі артықшылықтар береді, ал екінші жағынан – ақпараттық жүйенің ресурстары мен

деректеріне рұқсатсыз қол жеткізудің сапалы жаңа мүмкіндіктеріне алып келеді, бұл ақпараттың таралып кетуіне, жоғалуына, бұрмалануына, жойылуына, көшірілуіне және бұғатталуына, соның салдарынан экономикалық, әлеуметтік немесе басқа да залал түрлерін келтіруге әкеп соғады. Яғни, ұйымның ақпараттық технологияларын таратумен Ақпараттық жүйелер мен қызметтерге неғұрлым тәуелді, демек, қауіпсіздік қатерлеріне қатысты неғұрлым осал болып табылады. Сондықтан ақпаратты қорғау мәселесі бүгінгі күні өте маңызды болып тұр. Алайда ақпаратты қорғаудың қажетті деңгейін қамтамасыз ету өте күрделі міндет, өзінің шешімі үшін ұйымдастыру іс-шараларының тұтас жүйесін құруды және ақпаратты қорғау жөніндегі арнайы құралдар мен әдістерді қолдануды талап етеді.

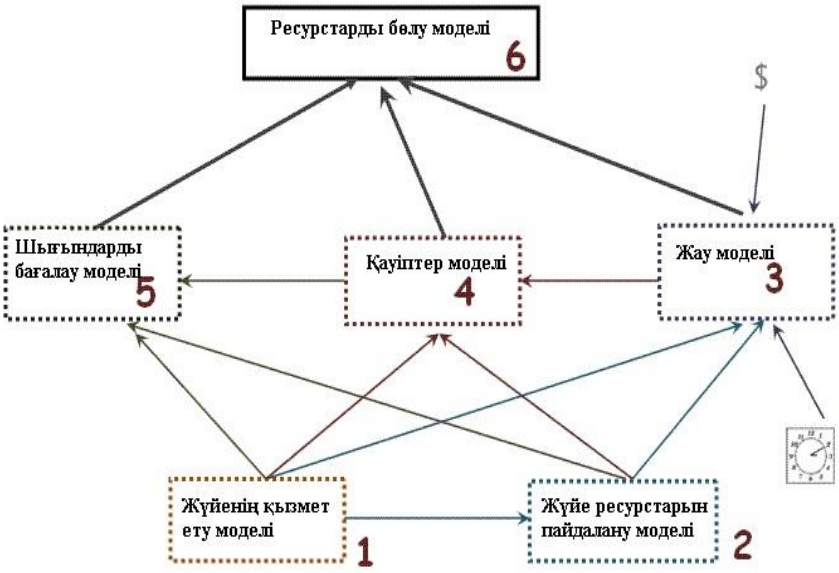
Негізгі бөлімі

Ақпаратты қорғау процесі-бұл ақпаратқа әсер ететін қауіп-қатерлердің және ақпаратты қорғау құралдарының олардың әсеріне кедергі келтіретін өзара іс-қимыл процесі. Жалпы түрде АЖ-да ақпаратты қорғау процесінің моделі 1-суретте көрсетілгендей ұсынылуы мүмкін.



1-сурет.

Ақпаратты қорғау процесін ақпаратты қорғайтын ресурстарды бөлу процесі ретінде де қарау қажет. Қорғау құралдарын оңтайлы таңдау ақпаратты қорғауға бөлінетін ресурстарды пайдалану мен бөлудің жетілдірілген моделін құру арқылы одан әрі шешу жоспарланып отырған күрделі міндет болып табылады [9]. Ресурстарды бөлу моделі 2-суретте көрсетілген [9].



2-сурет. Ақпаратты қорғау құралдарын таңдау процесінің жалпы моделі

Ресурстарды бөлу моделі қауіптер моделінің, сондай-ақ шығындарды бағалау моделінің негізінде қарсыластың және қорғалатын Тараптың мүмкіндіктеріне сүйене отырып құрылады, өйткені қорғау шараларын таңдауда экономикалық орындылыққа сүйене отырып, қорғау құралдарына жұмсалатын шығындар ақпараттық қауіпсіздікті бұзудан болатын болжамды шығыннан аспауы тиіс [8,9].

Ресурстарды бөлу моделін формальды түрде сипаттауға болады. Ол көптеген ақпараттық қауіп-қатерлерді қамтиды:;

* ақпарат қатерін сәтті іске асырған жағдайда, жүйенің шығындарына көптеген сандық бағалау;
* ақпаратты қорғау құралдарын қолданған жағдайда жүйе шығынының көптеген сандық бағалары;
* деструктивті әрекеттерді жүзеге асыру үшін көптеген құралдар;
* көптеген бұзушылар;
* ақпаратты қорғаудың көптеген құралдары;
* қауіп-қатерлерді іске асыру үшін шабуылдаушы жағы бар уақыт;
* қарсыласы бар қаржы қаражаты

Бұл модельді құру нәтижелері қарсылас моделін, қауіптер моделін, шығындарды бағалау моделін, сондай-ақ ресурстарды бөлу моделін құру үшін маңызды.

Қорғаудың ғылыми-әдістемелік базисінің негізгі элементтерінің бірі қаскүнемдердің іс-қимыл нұсқаларын ескере отырып, қорғау объектілері арасында ақпаратты қорғау ресурстарын оңтайлы бөлу есебінен ақпараттық жүйелердің қорғалу деңгейін арттыру болып табылады. Оларды құру үшін негіз ақпаратты қорғаудың жалпы мақсаттары (міндеттері) және қорғау жүзеге асырылатын шарттар болып табылады. Қорғау жүйесінің моделін құру міндетін шешу кезінде туындайтын мәселелердің бірі қорғаудың талап етілетін деңгейін қамтамасыз ету үшін қажетті ресурстар көлемін бағалау және оларды тиімді бөлу болып табылады және тиісінше осы модельде ресурстарды бөлу процестерін айқындаушы болуға тиіс.

Мемлекеттік басқару саласын ақпараттандырудың қол жеткізілген жоғары деңгейіне, қоғам мен жеке тұлғаның өмірінің түрлі салаларында, қорғаныс пен қауіпсіздікті қоса алғанда, АКТ-ны кеңінен пайдалануға қарамастан, Қазақстан АКТ-ның отандық секторы ұлттық экономиканы әртараптандыру бағдарламасына практикалық үлес қосатын ел болуы тиіс. Қазақстан, киберқауіпсіздікті қамтамасыз ету технологияларын қоса алғанда, айтарлықтай дәрежеде алдыңғы қатарлы IT технологияларға ие болған ел ретінде, кез келген сәтте эксперимент объектісі ретінде әрекет ететін немесе елдің ақпараттық-коммуникациялық инфрақұрылымының аса маңызды объектілеріне нақты әсер ететін қылмыстық ұйымдар мен жекелеген тұлғалар тарапынан күтпеген нәтижемен кез келген жағдайға тап болуы мүмкін. Ресей мен Украинада ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі мәселелердің тақырыптары мен шешімдері көптеген жұмыстар бір-бірімен қиылысады және көптеген ортақ және көп айырмашылықтар бар. Егер Украина мен Ресейде ақпараттық қауіпсіздіктің тұжырымдамалық және ғылыми-әдістемелік негіздері қоғамның бұрыннан емес ақпараттандырылуына және жоғары технологияларды қолдануға байланысты әзірлене бастаса, онда жаһандық контексте ақпараттық қауіпсіздік бұрыннан бері және өте белсенді дамып келеді, бұл туралы осы тақырыптағы ағылшын тіліндегі жұмыстардың үлкен саны мен шешілетін проблемалар шеңберін куәландырады.

Бұл мақалада егжей-тегжейлі қарау және зерттеу үшін шабуыл жасау және ақпараттық жүйеге қорғау тараптарының кезекпен шешім қабылдау салдарларын Имитациялық модельдеуді жүргізу әдістемесі таңдап алынды және ұсынылды. Динамикалық режимде бағалау пайдаланылады, бұл ресурстарды бөлуді оңтайландыру жөніндегі ұсыныстарды тұжырымдауға және ақпарат қатерін іске асырудан күтілетін зиянның мөлшерін бағалауға мүмкіндік береді. Ақпараттық қауіпсіздік жай-күйінің өзгеру динамикасын зерттеу үшін тараптардың әртүрлі бағыттағы қарсы тұру процестерін іске асыру моделін пайдалану жөніндегі практикалық ұсынымдар тұжырымдалады. Сондай-ақ, қорғау объектісінің ақпараттық қауіпсіздігінің кепілдігін бағалауға мүмкіндік беретін инвестициялық әдісті пайдалану тиімділігіне талдау жүргізу бойынша ұсынымдар тұжырымдалады. Болашақта киберқорғау ресурстарын динамикалық басқару процесін автоматтандыруға мүмкіндік беретін бағдарламалық кешенді әзірлеу жоспарлануда.

Ақпараттық қауіпсіздік тәуекелдерін төмендетуге ресурстарды бөлуді оңтайландыру кез келген ақпараттық жүйе үшін маңызды, ол жүйенің тәуекелдерін кешенді қарауға және оларды төмендетуге артық шығындарды болдырмауға көмектеседі. Құрылған модельдерде ақпараттық жүйеде болатын, осы проблеманы интуитивті шешу кезінде назар аудармауға болатын әртүрлі ерекшеліктер ескеріледі.

Ақпараттық саланы дамыту және оның көлемі мен құнының тиісті өсуі мемлекеттің қоғамдық өмірінің барлық салаларына озық ақпараттық технологияларды енгізумен сүйемелденеді, бұл шабуылдардың жиілігін және ақпараттың таралып кетуінен болатын ықтимал залалды арттыруға әкеп соғады. Нәтижесінде - қорғау жүйелерін күрделендіру және олардың құнын ұлғайту. Мұндай жағдайларда шектеулі қаржы ресурстарын шаруашылық қызмет субъектілерінің ақпаратын қорғауға тиімді бөлу міндеті неғұрлым маңызды болып табылады және едәуір дәрежеде мемлекеттің ақпараттық қауіпсіздік деңгейін айқындайды. Динамикалық қарсы тұру жағдайында ақпаратты қорғау жүйесінің көрсеткіштерін оңтайландыру мәселелерін әзірлеу ерекше өзектілікке ие болады. Мұндай көрсеткіштер қорғау жүйесінің тиімділігін, ақпаратты қорғауға инвестицияларды енгізуден түсетін пайданы, олардың рентабельділігін және тағы сол сияқтыларды анықтайтын жоғалған ақпараттың үлесі болуы мүмкін [7]

Қорытынды

Мақаланың ғылыми жаңалығы ақпараттық қауіпсіздік тәуекелдерін төмендетуге арналған ресурстарды бөлудің ең тиімді тәсілін табу әрекеті болып табылады және теориялық, әдіснамалық, эксперименталдық және ақпараттық-технологиялық негіздеме және мәселені шешу болып табылады. Ғылыми нәтижелердің маңыздылығы ұсынылған әдісті пайдалану тиімділігін бағалаудың әзірленген әдістемесі негізінде қазіргі заманғы инфокоммуникациялық технологияларды пайдалана отырып, динамикалық режимде күрделі ақпараттық жүйелерде ресурстарды бөлуді оңтайландыру процесін кешенді іске асыру үшін бағдарламалық өнімді құру болып табылады.

ӘДЕБИЕТТЕР

[1].Домарев В.В. Безопасность информационных технологий. - :ТИД Диа Софт, 2002 - с. 688

[2] Official ISACA site [Электронный ресурс]- Режим доступа к статье: http://www.isaca.org.

[3] Official ISACA site. The Business Model for Information Security [Электронный ресурс] — Режим доступа к статье: http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

[4] Nina Dobrinkova. Information Security – Bell-La Padula Model [Электронный ресурс] — Режим доступа к статье: http://www.iit.bas.bg/PECR/62/53-59.pdf

[5] Табаков А.Б. Разработка моделей оптимизации средств защиты информации для оценки страхования информационных рисков [Электронный ресурс] — Режим доступа к статье:http://ej.kubagro.ru/2005/04/02/

[6] Гроздов Г. Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса [Текст] / Г. Г. Гроздов // (Препринт/ НАН Украины. Отделение гибридных управляющих систем в энергетике ИПМЭ им. Г. П. Пухова НАН Украины; № 01/2005) – Киев : ЧП Нестреровой, 2005. – С. 66.

[7] Akhmetov, B., Lakhno, V., Akhmetov, B., Alimseitova, Z. (2019). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity, Advances in Intelligent Systems and Computing, 860, pp. 162-171.

[8] Lakhno, V., Zaitsev, S., Tkach, Y., Petrenko, T. (2019). Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs' clustering, Advances in Intelligent Systems and Computing, 754, pp. 673-682.

[9] Lakhno, V.A., Kravchuk, P.U., Malyukov, V.P., Domrachev, V.N., Myrutenko, L.V., Piven, O.S. (2017). Developing of the cyber security system based on clustering and formation of control deviation signs, Journal of Theoretical and Applied Information Technology, 95 (21), pp. 5778-5786.

Адилжанова С.А., Тюлепбердинова Г.А., Ғазиз Г., Сақыпбекова М.Ж.

Анализ математических методов динамического управления ресурсами кибербезопасности объектов информатизации

Резюме. Рассматриваются множества угроз, уязвимостей и рисков информационной системы. Предлагаются модели связи информационных рисков и ресурсов, которые могут снизить данные риски. На основе таких моделей производится поиск оптимального распределения ресурсов на снижение рисков информационной безопасности.. Как результат - усложнение систем защиты и увеличения их стоимости. Особую актуальность приобретает разработка вопросов оптимизации показателей системы защиты информации в условиях динамического противостояния.

Ключевые слова: киберзащита, киберпреступность, динамическое управления, информационное пространство, защита информации.

Технические науки