ИНТЕЛЛЕКТУАЛДЫ ТЕХНОЛОГИЯЛАР

Жайлхан Бахтияр Қожабергенұлы

магистрант, Қазақ ұлттық аграрлық университеті, Алматы қ., Қазақстан

Серикбаев А.У

научный руководитель, Ф.-м.ғ.д., профессор Қазақ ұлттық аграрлық университеті, Алматы қ., Қазақстан

Түйіндеме: Бұл мақалада қазіргі уақытта экономикалық субъектілердің ақпараттық қауіпсіздігін қамтамасыз ету үшін жасанды интеллект әдістерін қолдану қаншалықты негізделген екенін түсінуге әрекет жасалды. Жасанды интеллект әдістерінің тізімі келтірілген.

Шаруашылық жүргізуші субъектілердің ақпараттық қауіпсіздігін қамтамасыз ету үшін оларды ықтимал пайдаланудың негізгі салалары сипатталған. Авторлар шаруашылық жүргізуші субъектілердің ақпараттық қауіпсіздігінің вирусқа қарсы бағдарламалық қамтамасыз етуін әзірлеу үшін эвристикалық әдістер класын пайдалануды ұсынады. Зияткерлік жүйелер кәсіпорынның ақпараттық қауіпсіздігін дамытудың негізгі векторы болып табылады.

Abstract. The article attempts to understand how justified the use of artificial intelligence methods to ensure information security of economic entities at the present time. The list of artificial intelligence methods is given. The main areas of their possible use for information security of economic entities are described. The authors suggest using a class of heuristic methods for developing antivirus software for information security of economic entities. Intelligent systems are the main vector of enterprise information security development.

Кілт сөздер: жасанды интеллект, ақпараттық қауіпсіздік, жасанды интеллект әдістері, эвристикалық әдістер, киберқауіптер, вирусқа қарсы бағдарламалық қамтамасыз ету.

Keywords: artificial intelligence, information security, artificial intelligence methods, heuristic methods, cyber threats, antivirus software.

КІРІСПЕ

Елдің экономикалық дамуы жаңа ақпараттық технологияларды енгізумен және дамытумен тығыз байланысты.

Ел мен қоғамды тиімді дамытудың маңызды шарттарының бірі экономиканы цифрландыру болып табылады.

Ақпараттық қауіпсіздікті талдаудың жаңа құралдары мен мүмкіндіктері цифрлық экономика жағдайындағы аса маңызды технологиялар болып табылады.

Жақында компьютерлік жүйелердің қауіпсіздік деңгейін жоғарылату үшін де, хакерлік шабуылдарды тойтару үшін де жасанды интеллект әдістерін қолдану мүмкіндігі туралы

көптеген жарияланымдар пайда болды.

Жасанды интеллект, авторлардың көзқарасы бойынша, жүйенің дәстүрлі түрде адамның ақыл-ойымен байланысты бірқатар функцияларды орындау мүмкіндігі деп түсініледі.

Атап айтқанда, өздігінен білім алу, бұрын алынған тәжірибені, оның ішінде шаруашылық жүргізуші субъектілердің экономикалық қызметін зерттеуге негізделген шешімдер қабылдау қабілеті. Жасанды интеллект әдістерін қолдану аясы кеңейетініне күмән жоқ. Қазіргі уақытта бұл тәсіл кәсіпорынның автоматтандырылған жүйелерінің ақпараттық қауіпсіздігіне қатысты қандай артықшылықтар бере алатындығын бағалау қызықты, өйткені осы саладағы зерттеулер аяқталмаған және мүмкін аяқталған жоқ.

Ең алдымен, "жасанды интеллект" терминінің артында бірнеше гетерогенді технологиялар мен тәсілдер бар екенін атап өтеміз. Мысалы, дәстүрлі түрде жасанды интеллект әдістері [1]:

• ережелерге негізделген сараптамалық жүйелер. Мұндай жүйелер сараптамалық жүйені қолданар алдында тар бағытқа ие, ережелер "алынып", білім базасында сақталуы керек. Білімді алу процесі сараптамалық жүйені қолдану болжанатын саладағы ең білікті мамандарды тартуды қамтиды. Сарапшылар сараптамалық жүйелерді әзірлеу саласындағы маманның көмегімен өз тәжірибесі негізінде жүйенің мінез-құлық ережелерін тұжырымдауы керек;

* себеп-салдарлық желілер (Байес сенім желілері). Бұл желілер кездейсоқ оқиғалар себеп-салдарлық байланыстармен байланысқан белгісіздікке ие жағдайларды модельдеу үшін қолданылады. Математикалық тұрғыдан алғанда, Байес желісі графикалық модель болып табылады, онда түйіндер оқиғалар, ал доғалар оқиғалар арасындағы мүмкін байланыстар болып табылады;

* нейрондық желілер. Жасанды интеллекттің бұл бағыты адам миының жұмысын модельдеумен байланысты. Миды зерттеу оның нейрондық желілер негізінде жұмыс моделін құруға әкелді. Нейрондық желілер адамның оқу және өзін-өзі үйрену қабілетін түсіндіреді.

Нейрондық желілерді заманауи компьютерлерде сәтті модельдеуге болады, бұл өздігінен Үйренетін компьютерлік бағдарламаларды жасауға мүмкіндік береді;

* анық емес логика жүйелері. Бұл жүйелерде лингвистикалық айнымалыларды, яғни табиғи тілдегі мәлімдемелерді өңдеу модельденеді. Жүйе жұмысында алгебра аппараты және сарапшы белгілеген логикалық шығару ережелері қолданылады [1].

НӘТИЖЕЛЕР, ТАЛДАУ ЖӘНЕ ТАЛҚЫЛАУ

Машиналық оқытуды қолдануға негізделген вирусқа қарсы құралдар өзге қағидаттар бойынша жұмыс істей алады. Мысал ретінде "cylance" американдық фирмасының "Cylance Protect" антивирусын келтіруге болады [6]. "Cylance" компаниясы 2012 жылы стартап ретінде құрылды, ол сайтқа ие www.cylance.com. бұл компания алға қойған мақсаттардың бірі-вирусты немесе басқа қауіпті бағдарламалық жасақтаманы кем дегенде қандай да бір зиян келтірмес бұрын анықтайтын антивирус жасау.

"Cylance Protect" қолтаңба дерекқоры мен эвристикалық әдістерді пайдаланбайды. Оның орнына ол бағдарламалық жасақтаманың жұмысын сипаттайтын математикалық модельге сүйенеді. Код сипаттамаларын статистикалық талдау негізінде Бағдарламаның функциялары анықталады.

Егер олардың арасында қауіпті болса, онда бағдарламаны пайдалану бұғатталады.

Негізгі назар емдеуге емес, шабуылдардың алдын алуға бағытталған [6]. Модель жетілдірілуі мүмкін және антивирустық бағдарламалық жасақтама жаңа қауіпсіздік қатерлеріне бейімделу үшін өздігінен оқытылуы мүмкін. Жаңартуларды жиі орындау қажет емес, тек математикалық модельдер өзгерген кезде.

Жасанды интеллект орнатылған зиянды бағдарламалардың пайда болу мүмкіндігі туралы алаңдаушылық бар, бірақ олардың әрекет ету механизмі түсіндірілмейді. Бұл әлі мүмкін емес сияқты, бірақ әсіресе қажет емес. Жоғарыда айтылғандардың бәрі зияткерлік жүйелер ақпараттық қауіпсіздікті дамытудың айқындаушы векторы болып табылады деген қорытынды жасауға мүмкіндік береді [11].

Тәуекелдер мен қатерлердің барлық спектрін терең талдауды, болжауды, тануды және алдын алуды жүзеге асыруға мүмкіндік беретін жүйелерді енгізу қазіргі заманғы ақпараттық технологияларды пайдалануды ескере отырып, кәсіпорындардың бизнес-процестерін тиісті қайта құруды талап етеді.

ҚОРЫТЫНДЫ

Бұл ғылыми-зерттеу жұмысында қауіпсіздіктің белгілі бір деңгейін қамтамасыз ету мәселесін шешу екі нақты мәселені дәйекті шешумен байланысты: қауіпсіздік деңгейін сандық бағалау және АҚҚ ресурстарын қайта бөлу қажеттілігі туралы автоматтандырылған шешім қабылдау автоматтандырылған жүйе немесе АҚҚ қасиеттері мен параметрлерін өзгерту ақпараттың берілген деңгейін ұстап тұру үшін автоматтандырылған жүйе. Ақпараттың қорғалу деңгейін сандық бағалауды алу қажеттілігі автоматтандырылған жүйелер ақпаратының қорғалу деңгейін қолдауға бағытталған іс - шараларды жүргізу қажеттілігі туралы негізделген шешім қабылдау үшін жұмыс істеу жағдайларының өзгеруіне байланысты қорғалу деңгейінің өзгеру динамикасын жинақтау және талдау талап етілетіндігімен байланысты екені расталды.

Ақпараттың қорғалу деңгейін сандық бағалауды алудың ғылыми проблемасын шешу жолдарына жүргізілген теориялық зерттеулер таяу болашақта АС-да ақпараттың қорғалу деңгейін бағалаудың жалпыға бірдей танылған және ғылыми негізделген әдісін құру мүмкіндігі туралы айтуға мүмкіндік береді.

Екінші мәселені сәтті шешу, атап айтқанда, АҚҚ ресурстарын қайта бөлу немесе АҚҚ қасиеттері мен параметрлерін өзгерту қажеттілігі туралы автоматтандырылған шешім қабылдау міндеттері шешім қабылдау және АҚҚ қасиеттері мен параметрлерін қайта бөлу немесе өзгерту процесіне қатаң уақытша шектеулермен айтарлықтай қиындайды.автоматтандырылған жүйе, сондай-ақ осы процесс нәтижелерінің автоматтандырылған басқару жүйелерінің функционалдық міндеттерін толық көлемде орындау қабілетіне әсер ету мәселелерінің зерттелмегендігі.

Осы ғылыми мәселені шешудің тәсілдерін сипаттауға арналған жарияланымдарда, біріншіден, мамандандырылған автоматтандырылған жүйенің жұмыс істеу ерекшеліктерімен белгіленген уақыт шектеулері жағдайында оларды қолдану мәселелері аз зерттелген, екіншіден, қауіпсіздіктің белгілі бір деңгейін АҚҚ-да қолданылатын құралдармен қамтамасыз ету мүмкін болмаған жағдайларды зерттеу нәтижелері жоқ автоматтандырылған жүйе.

Осылайша, ҚР ақпараттық қауіпсіздігін қамтамасыз ету міндеттерінің бір бөлігі болып табылатын бөлінген мамандандырылған автоматтандырылған жүйелерде зияткерлік АҚҚ құру мен пайдаланудың өзекті ғылыми проблемасын шешу таратылған мамандандырылған автоматтандырылған жүйе ақпаратының қауіпсіздігін зияткерлік қамтамасыз ету теориясын жасау шеңберінде ғылыми негізделген және іс жүзінде мүмкін болатын әдістер мен әдіснамалар кешенін әзірлеу қажеттілігімен байланысты екендігі үйретілді.

Әдебиеттер тізімі:

1. Абрамова Я. Гонка вооружений: искусственный интеллект и кибербезопасность // Директор информационной службы. 2017. № 10. URL: https://www.osp.ru/cio/ archive/2017/10/ (дата обращения: 10.11.2019).

2. Потери банков от киберпреступности. Tadviser, 28.09.2019. URL: http://www.tadviser.ru/index.php (дата обращения: 10.01.2020).

3. Информационная безопасность в мультиплатформенную эру. Москва, 14.03.2019. URL: https://idcitsecurity.com/2019/moscow/#category_55/ (дата обращения: 21.08.2019).

4. Искусственный интеллект и кибербезопасность. URL: https://www.pandasecurity.com/mediacenter/adaptive-defense/artificial-intelligence-cybersecurity/ (дата обращения: 10.01.2020).

5. Олейникова Т. В. Применение методов искусственного интеллекта в задачах обеспе¬чения информационной безопасности. URL: http://dom8a.ru/seminar-ib/05.06.2014/oleinikova/paper.pdf (дата обращения: 17.12.2019).

6. Уэйн Рэш. Cylance выпускает продукт будущего для борьбы с вредоносным кодом // itWeek 28.04.2015 URL: https://www.itweek.ru/security/article/detail.php?ID=174219 (дата обращения: 10.11.2019).

7. Антивирус с искусственным интеллектом не требует обновления баз и не нагру¬жает систему. URL: https://www.osp.ru/news/2016/0614/13033043 (дата обращения: 12.11.2019)

8. Антивирус с искусственным интеллектом – выходец из России. URL: https://neuronus.com/news-tech/1132-antivirus-s-iskusstvennym-intellektom-vykhodets-iz-rossii. html (дата обращения: 10.11.2019).

9. «Антивирусная правДА!» 06.09.2017, ИИ против антивирусов. URL: https://www.drweb.ru/pravda/issue/?number=390 (дата обращения: 05.10.2019).

10. Георгиев Р. Искусственный интеллект научился писать трояны, невидимые для антивирусов. Платформа в открытом доступе. C-News 02.08.2017. URL: http://safe.cnews.ru/news/top/2017-08-02_iskusstvennyj_intellekt_nauchilsya_pisat_troyany (дата обращения: 21.11.2019).