6. A. Bourke, J. O'Brien, G. Lyons. Evaluation of a threshold-based tri-axial accelerometer fall detection algorithm. Gait & Posture 26(2) 2007:194–199.
7. M. Carfagni, R. Furferi, L. Governi, C. Santarelli, M. Servi, F. Uccheddu, Y.Volpe. Metrological and critical characterization of the Intel D415 stereo depth camera //Sensors. – 2019. – Т. 19. – №. 3. – p. 489-508.
8. Z. Zhang. Microsoft kinect sensor and its effect, IEEE MultiMed.19 (2) (2012) 04–10.
9. J. Shotton, A. Fitzgibbon, M. Cook, T. Sharp, M. Finocchio, R. Moore, A. Kipman, A. Blake, Real-time human pose recognition in parts from single depth images, in: Proceedings of IEEE Computer Vision and Pattern Recognition, CVPR, Colorado Springs, 2011.
10. J. Han, L. Shao, D. Xu, J. Shotton, Enhanced computer vision with Microsoft Kinect sensor: a review, IEEE Trans. Cybern. 43(5) (2013) 1318–1334.
11. R. Munoz-Salinas, R. Medina-Carnicer, F.J. Madrid-Cuevas, A. Carmona-Poyato, Depth silhouettes for gesture recognition, Pattern Recognit. Lett. 29 (3) (2008) 319–329.
12. F. Dominio, M. Donadeo, P. Zanuttigh, Combining multiple depth-based descriptors for hand gesture recognition, Pattern Recognit. Lett. 50 (2014) 101–111.
13. Holte M. B., Moeslund T. B., Fihl P. Fusion of range and intensity information for view invariant gesture recognition //2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. – IEEE, 2008. – С. 1-7.
14. Van den Bergh M. et al. Real-time 3D hand gesture interaction with a robot for understanding directions from humans //2011 Ro-Man. – IEEE, 2011. – Pp. 357-362.
15. Ren Z., Yuan J., Zhang Z. Robust hand gesture recognition based on finger-earth mover's distance with a commodity depth camera //Proceedings of the 19th ACM international conference on Multimedia. – 2011. – Pp. 1093-1096.
16. Wu D., Zhu F., Shao L. One shot learning gesture recognition from rgbd images //2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. – IEEE, 2012. – Pp. 7-12.
17. Keskin C., Kirac F., Kara Y., Akarun L. Randomized decision forests for static and dynamic hand shape classification //2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. – IEEE, 2012. – Pp. 31-36.
18. Liao, B., Li, J., Ju, Z., Ouyang, G. Hand gesture recognition with generalized hough transform and DC-CNN using realsense //2018 Eighth International Conference on Information Science and Technology (ICIST). – IEEE, 2018. – Pp. 84-90
19. Сатыбалдина Д.Ж., Калымова К.А. Разработка приложения, управляемого жестами, с использованием MICROSOFT KINECT SENSOR // «Цифровая обработка сигналов и ее применение – DSPA-2019»: Сборник докладов 21-й Международной конференции, Москва, Россия, 2019.- стр. 525-529.

ӘОЖ 001.378

ӨНЕРКӘСІП КӘСІПОРЫНДАРЫНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ

Касимов Асылбек Агыбаевич
a.kasimov-81@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Информатика және ақпараттық жүйе
магистранты, Астана, Қазақстан
Ғылыми жетекшісі – т.ғ.к., доц. Туребаева Р.Д.

Қазіргі уақытта өнеркәсіптік кәсіпорындардың ақпараттық ағындардың едәуір көлеміне тәуелділігі өсуде. Ақпараттық және коммуникациялық технологиялардың дамуымен субъектілер арасында әртүрлі ақпарат түрлерімен алмасу саласында өзгеріс болды, бұл ақпараттық технологиялардың көмегімен қазіргі қоғамның көптеген міндеттерін жедел шешуге мүмкіндік береді. Дегенмен, олардың негізінде ішкі ұйымдастыру, ұйымаралық,

ұлттық және әлемдік ақпараттық кеңістіктерде орналасқан есептеу жүйелері мен желілерінің тұрақты күрделенуі қазіргі заманғы қоғамның алдына ақпараттық қауіпсіздікті (АҚ) қамтамасыз ету міндетін қояды. Жыл сайын деректерді қорғау технологиялары жетілдірілуде, алайда қорғау осалдығы азаюда ғана емес, сонымен қатар үнемі өсуде. Сондықтан деректер ағынын қорғауға және ақпараттық қауіпсіздікке байланысты проблемалардың — оларды жинау, сақтау, өңдеу және беруге өзектілігі айқын.

Біздің ойымызша, ақпараттық қауіпсіздік - бұл ақпараттық-компьютерлік жүйелерде өңделетін кез-келген ақпараттың қорғалу жағдайы. Өйткені компьютерлік техника ақпараттық жүйенің бір бөлігі ғана. Жалпы ғылыми санат ретінде қауіпсіздік қарастырылып отырған жүйенің сыртқы және ішкі қауіп-қатерлердің әсеріне қарсы тұра алатын жай-күйі ретінде анықтауға болады, ал бұл жүйенің жұмыс істеуі оның құраушылары үшін, сондай-ақ сыртқы ортаға қауіп төндірмейді [1].

Бұл кәсіпорынның қаржы-экономикалық тұрақтылығын нығайту мақсатында ұйымның ақпараттық-технологиялық ресурсын неғұрлым тиімді пайдалану жағдайы, кәсіпорынның құпия ақпараты мен коммерциялық құпиясын қорғау, ішкі және сыртқы ортаның ақпаратты жинау және талдау [2].

Осы жерден АҚ-ны қамтамасыз етудің негізі өзара байланысты үш проблеманы шешу болып табылады: жүйедегі ақпаратты ішкі және сыртқы қауіптердің әсерінен қорғау мәселелері; ақпаратты ақпараттық қатерлерден қорғау проблемалары; ақпарат жүйесіндегі қауіп-қатерлерден сыртқы ортаны қорғау проблемалары.

"Ақпараттық қауіпсіздік" ұғымы практикалық өмірде және қызметте кеңінен қолданылады. Бұл ретте, тіпті мамандар бұл ұғымға әр түрлі мағынаны салады. Ол көбінесе "ақпаратты қорғау" ұқсас ұғымымен алмастырылады, соның нәтижесінде мәселе ақпаратты әртүрлі физикалық арналар арқылы оны есептеу техникасы құралдарымен өңдеу кезінде сыртқа шығудан қорғаудың жеке міндетіне түседі.

Ақпараттық қауіпсіздікті қамтамасыз ету күрделі және көп қырлы проблеманы білдіреді. Ол барлық экономикалық агенттер мен шаруашылық жүргізуші субъектілер, яғни негізгі ақпарат тасымалдаушы халық, кәсіпорындар мен ұйымдар үшін, сондай-ақ тұтастай мемлекет үшін қамтамасыз етілуі тиіс. Ең алдымен, АҚ-ға мүдделі субъектілерді қамтитын АҚ- ны қамтамасыз ету міндеттері мен деңгейлерін анықтаймыз.

Жария ету деп тиісті құқықтары жоқ субъектілердің ақпаратты алуға әдейі немесе ойдан тыс іс-әрекеттері нәтижесінде келтірілген оқиға түсініледі. Жария ету әртүрлі тәсілдермен жүзеге асырылуы мүмкін. Бұл хабарлама жіберу, жіберу, жариялау, жоғалту және т.б. болуы мүмкін. Бейресми арналар жеке кездесулер, хат алмасулар, көрмелер, конференциялар, бұқаралық ақпарат құралдары және т.б. болып табылады. Әдетте құпия ақпаратты жария ету қызметкерлердің біліксіздігі, құпия мәліметтерді қорғау ережелерін орындамау нәтижесінде болады.

Құпия ақпаратты кәсіпорын немесе белгілі бір тұлғалар шеңберінен тыс берудің бақылаусыз процесін түсінеміз. Ақпараттың таралып кету арнасы құпия мәліметтердің физикалық жолы деп аталады, оны пайдалана отырып, қаскүнем қорғалатын ақпараттық ресурстарға қол жеткізе алады. Ақпараттың таралып кету арналары ақпаратты материалдық-заттық, акустикалық, визуалды-оптикалық және электромагниттік заттарға тасымалдау тәсілі бойынша жіктеледі.

Рұқсат етілмеген қол жеткізу деп оған тиісті қол жеткізу құқығы жоқ тұлғаның құпия ақпаратты алуға бағытталған әдейі әрекет деп аталады. Қызметкерлерді сатып алу, ынтымақтастыққа күш қолдану, объектіге тікелей кіру және т. б. жататын түрлі әдістердің көмегімен рұқсатсыз қол жеткізу жүзеге асырылады.

Құпия ақпаратты заңсыз иеленуге ықпал ететін шарттар деп: қызметкерлерді сатып алу, айтып қою, бақылаудың болмауы, еңбек тәртібінің болмауы, қызметкерлерді жалдау кезіндегі кадр қызметтерінің нашар жұмысы, психологиялық үйлесімсіздік, еңбекақының төмендігі және т. б. болып саналады.

Сонымен қатар АҚ міндеттерінің бірі ақпараттың қолжетімділігін қамтамасыз ету болып табылады, өйткені Ақпараттық жүйелер (АЖ) әртүрлі ақпараттық қызметтерді (өнімдерді) ұсыну үшін құрылады және қызмет етеді. Байланысты бұзу, осындай қызметтерді алуға қол жеткізуден бас тарту мүдделі субъектілерге айтарлықтай залал келтіруге әкеп соғады. Қол жетімділіктің жетекші рөлі кәсіпорын қызметінің түрлі салаларында Басқару жүйелерінде көрінеді.

АҚ міндеті ретінде ақпараттың тұтастығы статикалық және динамикалық болып бөлінеді. Статикалық тұтастық деп ақпараттық ресурстардың өзгермеуі түсініледі, динамикалық күрделі операцияларды-транзакцияларды дәл жүргізуге жатады. Ақпараттың тұтастығын бұзу, яғни оның бұрмалануы, жоғалуы, адам қызметінің түрлі салаларындағы қателері болжанбаған нәтижелерге әкелуі мүмкін.

АҚ қамтамасыз ету деңгейін қарауға көшейік. Тұжырымдамалық-саяси деңгейде ақпараттық қауіпсіздіктің мемлекеттік саясатының бағыттарын айқындайтын құжаттар қабылданады, оларға қол жеткізудің мақсаттары мен міндеттері, жолдары мен құралдары тұжырымдалады.

Заң деңгейінде заңдар мен басқа да құқықтық актілерде (Президенттің жарлықтары, Үкіметтің Қаулылары және т.б.) көрсетілетін АҚ-ны құқықтық реттеу мен қамтамасыз етуге бағытталған шаралар кешені құрылады және қолдау көрсетіледі. Бұл деңгейдің маңызды міндеті ақпараттық технологиялар саласындағы прогреспен заңдарды әзірлеу процесін келісуге мүмкіндік беретін тетікті қалыптастыру болып табылады. Құқықтық шараларға ақпарат алу, өңдеу және пайдалану процесінде ақпараттық қатынастарға қатысушылардың құқықтары мен міндеттерін бекітетін, сондай-ақ осы Ережелерді бұзғаны үшін жауапкершілікті белгілейтін елде қолданылатын заңдар, жарлықтар және басқа да нормативтік құқықтық актілер жатады. Құқықтық шаралар негізінен алдын алу, профилактикалық сипатқа ие және пайдаланушылармен және қызмет көрсетуші қызметкерлермен үнемі түсіндіру жұмыстарын талап етеді. Бұл шаралар негізінен жасанды қауіп-қатерлерді жоюға бағытталған және басқа шараларды іске асыру үшін базис болып табылады.

Нормативтік-техникалық деңгейде стандарттар, басшылық және әдістемелік материалдар, сондай-ақ АҚ қамтамасыз ету құралдарын әзірлеу, енгізу және пайдалану, сондай-ақ жұмыс процестерін регламенттейтін басқа да құжаттар әзірленеді. Бұл деңгейдің басты міндеттерінің бірі ресейлік стандарттарды халықаралық стандарттарға сәйкестендіру болып табылады.

Кәсіпорын деңгейінде АҚ- ны қамтамасыз ету бойынша нақты шаралар жүзеге асырылады. Олардың құрамы мен мазмұны нақты ұйымның немесе кәсіпорынның ерекшеліктерімен анықталады. Осындай шаралардың негізінде мақсаты ақпаратты және онымен байланысты ресурстарды қорғауды қамтамасыз ету болып табылатын құжатталған басқару шешімдерінің жиынтығын білдіретін АҚ саясаты жатыр. Ол стратегияны, кәсіпорынның тиісті АҚ-ны қамтамасыз етуге бөлетін қаражат пен ресурстардың қажетті санын анықтайды. АҚ саясаты кәсіпорынның ақпараттық жүйесіне қауіп төндіретін қазіргі тәуекелдерге талдау жүргізу негізінде қалыптастырылады. Рәсімдік деңгейде адамдар жүзеге асыратын АҚ-ны қамтамасыз ету жөніндегі тікелей шаралар айқындалады. Оларға персоналды басқаруды, физикалық қорғауды және қалпына келтіру жұмыстарын жоспарлауды жатқызуға болады.

Бағдарламалық-техникалық деңгейде жабдықтарды, бағдарламалық құралдар мен ақпараттық ресурстарды қорғау жүзеге асырылады. Бұл шаралар АЖ құрамына кіретін және ақпаратты сақтау, өңдеу және беру процесімен тікелей байланысты қауіптерді жою мақсатында қорғау функцияларын орындайтын әртүрлі құрылғылар мен арнайы бағдарламаларды пайдалануға негізделген.

Бұл қауіпсіздік сервистерінің көмегімен іске асырылады (сәйкестендіру және аутентификация; қолжетімділікті шектеу; хаттамалау және аудит; шифрлеу; экрандау; тұтастықты қамтамасыз ету; қолжетімділікті қамтамасыз ету; бас тарту тұрақтылығын қамтамасыз ету).

Техникалық шаралар әлеуетті бұзушылардың жүйенің компоненттеріне және қорғалатын ақпаратқа кіруі және қол жеткізуі мүмкін жолдарда физикалық кедергілер жасау үшін арнайы арналған әртүрлі механикалық, электр және электронды - механикалық құрылғылар мен құрылыстарды, сондай-ақ визуалды бақылау, Байланыс және күзет сигнализациясы құралдарын қолдануға негізделген. Сондай-ақ АҚ талаптарын ескере отырып, ғимараттар, құрылыстар, инженерлік коммуникациялар желілері, көлік магистральдары және т.б. салуды оңтайландыруға байланысты инженерлік-техникалық шараларды бөліп көрсетуге болады.

Бүгінгі таңда қолданыстағы бағдарламалық-техникалық шешімдерді таңдаудың барлық байлығы кәсіпорынның АҚ-ын осы деңгейде қамтамасыз ету кезінде әлі күнге дейін күрделі міндет болып қала береді . Мұның себебі мынадай бағыттар бойынша ақпараттық технологиялардың қарқынды дамуы болып табылады : жүйелердің тез әрекет етуін арттыру; желілік технологиялардың дамуы және олардың өткізу қабілетінің өсуі; қысқа мерзімде құрылған және нарықта жоғары бәсекелестікке және пайда табуына байланысты тиісті түрде қорғалмаған бағдарламалық өнімдердің айтарлықтай өсуі; жаңа ақпараттық сервистерді құру және дамыту.

Ұйымдастыру шаралары АЖ АҚ-ін қамтамасыз етуде негізгі рөл атқарады. Ұйымдастыру шаралары - бұл басқа да қорғаныс әдістері мен құралдары жоқ немесе АҚ талап етілетін деңгейін қамтамасыз ете алмайтын жалғыз нәрсе. Ұйымдастыру шаралары адамдардың қызметін регламенттеуге қатысты басқа да шараларды тиімді қолдану үшін қажет. Сонымен қатар ұйымдастыру шараларын экономикалық, инженерлік-техникалық, техникалық және бағдарламалық-аппараттық құралдармен қолдау қажет.

Қолданылған әдебиеттер тізімі

1. Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы. М.: МЦПМО баспасы, 2002. 296 с.
2. Кастельс М. Информационная эпоха: экономика, общество и культура / пер. с англ. под научн. ред. О.И. Шкартана. М.: ГУ ВШЭ, 2000. 268 с.

УДК 004.56

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МОДЕЛЬ АНАЛИЗА, КОЛИЧЕСТВЕННЫЙ И КАЧЕСТВЕННЫЙ МЕТОДЫ ОЦЕНКИ

Ким Константин Станиславович
kkimseven@gmail.com
Магистрант специальности «6М070400 – Вычислительная техника и программное обеспечение», экспериментальная образовательная программа «Администратор по управлению и защите компьютерных систем и сетей на предприятиях», факультета Информационных технологий,
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Д.Ж. Сатыбалдина

Информационная безопасность, надежность и отказоустойчивость критических инфраструктур одна из основных и приоритетных задач любой страны [1]. Растущая зависимость важных инфраструктур и промышленной автоматизации от информационных систем управления привела к многочисленным угрозам кибербезопасности. Страны во всем мире сталкиваются со сбоями и инцидентами, вызванными различными причинами в секторе основной инфраструктуры [2]. Согласно аналитическому отчету «Kaspersky lab», с 2019 по 2020 год было обнаружено и отражено свыше **975** млн. атак по всему миру, найдено около 274 млн. уникальных вредоносных объектов, что в 1.5 раз больше по сравнению с предыдущим годом [3].