DOI: 10.53360/2788-7995-2023-4(12)-5

ҒТАХР: 81.93.29

Ж.М. Алимжанова, А.К. Байузакова*
Әл-Фараби атындағы Қазақ Ұлттық Университеті,
050040, Қазақстан Республикасы, Алматы, әл-Фараби даңғылы, 71
*e-mail: zhannamen@mail.ru, arailim107@mail.ru

АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕЛЕРДІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

Аңдатпа: *Орындалған мақалада бүгінде ақпараттық жүйелер аясында белсенді түрде қолданылып жүрген «автоматтандырылған жүйе және оның қауіпсіздігі» мәселесі жөнінде сөз қозғалады. Автоматтандырылған жүйелер қандай салаларда қолданылады, қауіпсіздік тұрғысынан беріктілігі және қорғаныс жағдайын талдау мәселесі шешіледі.*

Автоматтандырылған жүйелер қазіргі әлемде үлкен маңызға ие, өйткені олар күнделікті әртүрлі тапсырмаларды орындауды, деректер мен процестерді басқаруды айтарлықтай жеңілдетеді және жеделдетеді. Автоматтандырылған жүйелердің өзектілігі тиімділік және өнімділік, деректер сапасын жақсарту, масштабтау, аналитиканы дамыту сынды факторларға байланысты. Алайда, автоматтандырудың өсуімен деректер қауіпсіздігі мен құпиялылық саласындағы тәуекел де арта түсетінін түсіну маңызды. Автоматтандырылған жүйелер кибершабуылдардың нысанасына айналады және деректердің құпиялылығына, тұтастығына және қол жетімділігіне қауіп төндіруі мүмкін. Осылайша, автоматтандырылған жүйелердің қауіпсіздігі негізгі мәселелердің бірі болып қала бермек. Яғни, тиісті қауіпсіздік шараларының болмауы деректердің жоғалуына, құпиялылықтың бұзылуына және қаржылық шығындарға әкелуі мүмкін.

Сондықтан ұйымдар қол жетімділікті бақылау, шифрлау, инциденттерді анықтау тетіктерін енгізу және қызметкерлерді қауіпсіздік ережелеріне үйрету арқылы өздерінің атом электр станцияларын қорғауға және бақылауға белсенді түрде инвестиция салуы қажет.

Түйін сөздер: *автоматтандырылған жүйе, қауіпсіздік, компьютер, интернет, антивирус, технология.*

Кіріспе

Автоматтандырылған жүйелер қазіргі әлемнің ажырамас бөлігіне айналды [1,2], өнеркәсіптен бастап ақпараттық технологиялар мен электрондық коммерцияға дейінгі әртүрлі қызмет салаларына айтарлықтай әсер етті. Бұл жүйелер адамның минималды араласуымен күнделікті операциялар мен тапсырмаларды орындауға арналған бағдарламалық-аппараттық кешендер. Автоматтандырылған жүйелерді енгізу [2] тиімділіктің жоғарылауына, қателіктердің азаюына, шығындардың кемуіне және сапаның жақсаруына әкеледі.

Автоматтандырылған жүйелер әртүрлі салаларда шешуші рөл атқарады [3] :

– өндіріс және өнеркәсіп: өндірістік кәсіпорындарда автоматтандырлған жүйе өндірістік процестерді бақылайды және оңтайландырады, жабдықтар мен роботтарды басқарады және өнімнің сапасын арттырады.

– ақпараттық технологиялар: ақпараттық технологиялар саласында аталған жүйе серверлерді, желілік инфрақұрылымды, бұлтты есептеулерді басқаруды автоматтандыру және ақпараттың қауіпсіздігін қамтамасыз ету үшін қолданылады.

– электрондық коммерция: электрондық коммерциядағы процестерді автоматтандыру, тапсырыстарды, түгендеуді, логистиканы және тұтынушылардың өзара әрекеттесуін басқаруды оңтайландыруға мүмкіндік береді.

– денсаулық сақтау: автоматтандырылған жүйелер медицинада пациенттердің деректерін, медициналық жабдықтарды және зертханалық зерттеулерді басқару үшін қолданылады.

– қаржы және бухгалтерлік есеп: қаржылық есеп пен қаржыны басқарудың автоматтандырылған жүйелері фирмаларға бухгалтерлік есеп пен қаржылық талдауға көмектеседі.

Жоғарыда жіктелген бірнеше салалардың ішінде ақпараттық қауіпсіздік саласындағы автоматтандырылған жүйе жайлы кеңінен берілген мақалада көрсетіледі.

Автоматтандырылған жүйелер ақпараттық технологиялар әлемінде шешуші рөл атқарады және қазіргі қоғамға үлкен әсер етеді. Олар адамның айтарлықтай араласуынсыз күнделікті операциялар мен процестерді [3] орындауға арналған бағдарламалар мен жабдықтар кешені.

Ақпараттық технологиялар әлемінде автоматтандыру әсер ету салаларының кең ауқымын қамтиды:

– деректерді басқару: деректерді жинау, сақтау және талдау процестерін автоматтандыру ұйымдарға үлкен көлемдегі ақпаратты басқаруға көмектеседі. Деректер базасын басқару жүйелері (ДҚБЖ) және деректерді өңдеу құралдары әкімшілер мен деректерді талдаушылардың күнделікті тапсырмаларын автоматтандырады.

– бұлтты есептеу: бұлтты платформалар қолданбаларды сақтау, есептеу және масштабтау үшін автоматтандырылған ресурстарды ұсынады. Бұл ұйымдарға ат инфрақұрылымдарын жылдам масштабтауға және операциялық шығындарды азайтуға мүмкіндік береді.

– киберқауіпсіздік: автоматтандырылған киберқауіпсіздік оқиғаларын анықтау және алдын алу жүйелері қауіптерді анықтауға, сондай-ақ оларға нақты уақыт режимінде жауап беруге көмектеседі [4].

– желіні басқару: автоматтандырылған желіні басқару құралдары әкімшілерге трафикті оңтайландыру және жоғары қолжетімділікті қамтамасыз ету арқылы желілерді конфигурациялауға және бақылауға мүмкіндік береді.

– ақпараттық қауіпсіздік: қауіпсіздікті басқару және бақылау үшін ас оқиғалар журналын талдауды қамтамасыз етеді, кіруді анықтау, және кіру құқығын басқару.

– бағдарламалық жасақтаманы әзірлеу: үздіксіз интеграция/үздіксіз Деплоймент (CI/CD) сияқты даму орталары тестілеуді [4,5], құрастыруды және қосымшаларды орналастыруды автоматтандырады.

– табиғи тілді өңдеу: автоматтандырылған табиғи тілді өңдеу жүйелері мәтіндік ақпаратты, чатботтарды және машиналық аударманы автоматты түрде талдау үшін қолданылады.

– робототехника және жасанды интеллект: роботтар мен автономды жүйелер күнделікті физикалық тапсырмаларды орындау үшін қолданылады, ал жасанды интеллект деректерді талдау мен шешім қабылдауды автоматтандырады.

Ақпараттық технологияны автоматтандырудың көптеген артықшылықтары бар, соның ішінде өнімділікті арттыру, қателерді азайту және ресурстарды ұтымды пайдалану. Дегенмен, ұйымның ақпараттқ технология инфрақұрылымына автоматтандырылған жүйелерді енгізу кезінде қауіпсіздік мәселелерін есте ұстаған жөн. Киберқауіпсіздік автоматтандырудың ажырамас бөлігіне айналады және қауіпсіз жүйелерді әзірлеу және олардың жұмысын бақылау маңызды міндеттердің қатарына кіреді.

Материалдар мен тәсілдер

Ақпараттық қауіпсіздік саласындағы автоматтандырылған жүйелерді зерттеу маңызды міндет болып табылады, өйткені киберқауіптер мен тәуекелдер үнемі дамып отырады, соған орай уақыт өткен сайын жүйелерді қорғаудың жаңа әдістері мен шешімдерін жаңартып [6], әзірлеу қажет.

Міне, осы салада зерттеулер жүргізу кезінде қолдануға болатын кейбір материалдар мен тәсілдер тізімі төменде көрсетілген (кесте 1):

Кесте 1 – Автоматтандырылған жүйелердің қауіпсіздігін талдау әдістері мен тәсілдері

Атауы	Сипаты
Қолданыстағы әдебиеттерді талдау	Ақпараттық қауіпсіздік саласындағы автоматтандырылған жүйелерді зерттеудің алғашқы қадамы – бар әдебиеттерге шолу жасау. Зерттеулер, ғылыми мақалалар, кітаптар және киберқауіпсіздік туралы есептер зерттеуге ерекше назар беру.
Эмпирикалық зерттеулер	Зерттеушілер нақты әлемдегі автоматтандырылған жүйелердің жұмысын талдау үшін эксперименттер мен бақылаулар жүргізе алады. Бұл қауіптерді сынау үшін құм жәшіктерін құруды, сондай-ақ кибершабуылдарды бақылауды және жүйелердің оларға реакциясын қамтуы мүмкін.
Модельдеу және симулация	Модельдер мен симуляция жасау зерттеушілерге әртүрлі шабуыл сценарийлерін зерттеуге және автоматтандырылған жүйелердің қауіпсіздік деңгейін бағалауға көмектеседі. Бұл нақты жүйелер үшін қауіп-қатерсіз эксперименттер жүргізуге мүмкіндік береді.
Деректерді талдау және статистика	Кибершабуылдар, оқиғалар және қауіпсіздіктің бұзылуы туралы деректерді жинау және талдау зерттеу үшін құнды ақпарат бере алады. Бұл деректерді жүйелердегі кедергілерді анықтау және болашақ шабуылдарды болжау үшін пайдалануға болады.
Жаңа әдістер мен құралдарды әзірлеу	Зерттеушілер киберқауіптерді анықтау, алдын алу және оларға жауап беру үшін жаңа әдістер мен құралдарды жасай алады. Бұл аномалияларды анықтауға арналған жаңа алгоритмдер мен қол жетімділікті басқаруға арналған жүйелерді әзірлеуді қамтуы мүмкін.
Нарық пен индустрияға шолу	Зерттеушілер автоматтандырылған жүйелерді қорғау үшін пайдаланылуы мүмкін жаңа өнімдер мен технологияларды қоса алғанда, ақпараттық қауіпсіздіктің ағымдағы тенденциялары мен әзірлемелерін талдай алады.

Ақпараттық қауіпсіздік саласындағы автоматтандырылған жүйелердің материалдары мен тәсілдерін пайдалану ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету процестерін едәуір жеңілдетуге және жақсартуға, қауіптердің ықтималдығын азайтуға және оқиғаларға реакцияны жеделдетуге мүмкіндік береді:

– тиімділік: автоматтандырылған жүйелер көптеген тапсырмалар мен процестерді адамға қарағанда тезірек және тиімдірек орындай алады. Бұл уақыт пен ресурстарды үнемдейді.

– үздіксіздік: автоматтандырылған жүйелер тәулік бойы жұмыс істейді, соған орай ақпараттық жүйелер мен деректерді қорғаудың үздіксіздігін қамтамасыз етеді.

– реакция жылдамдығы: автоматтандырылған жүйелер анықтау мен реакция арасындағы уақыт аралығын азайту арқылы қауіптер мен оқиғаларға бірден жауап бере алады.

– дәлдік: жүйелер қателіктердің ықтималдығын азайту арқылы адам факторын жоққа шығарады. Бұл әсіресе үлкен көлемдегі деректерді талдау кезінде өте маңызды.

– масштабтау: автоматтандырылған жүйелер қажеттіліктерге байланысты масштабталуы мүмкін [7], бұл шағын компанияларды да, ірі корпорацияларды да қорғауды қамтамасыз етеді.

Жоғарыда сипатталған ақпараттық қауіпсіздік саласындағы автоматтандырылған жүйелерді зерттеудегі материалдар мен тәсілдер келесі міндеттер мен мақсаттарды шешуде шешуші рөл атқарады (диаграмма 1):

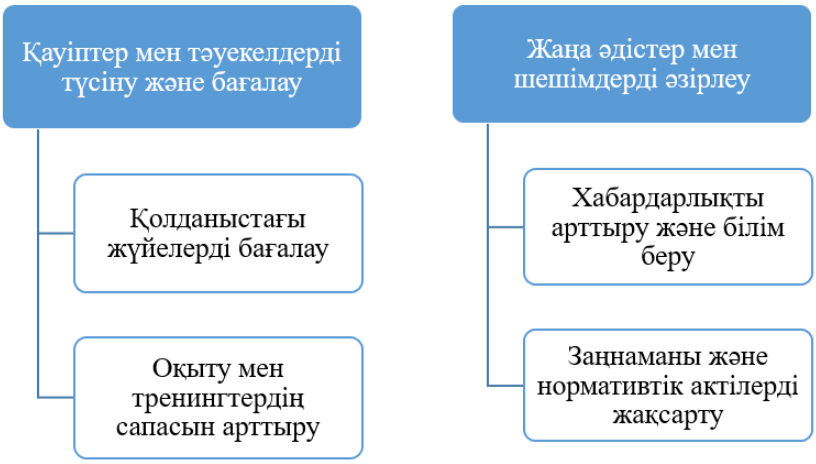

Диаграмма 1 – Автоматтандырылған жүйелердің қауіпсіздігін шешудің негізгі кезеңдері

Сипаттама

Қауіптер мен тәуекелдерді түсіну және бағалау: зерттеу материалдары мен тәсілдері зерттеушілер мен сарапшыларға автоматтандырылған жүйелермен байланысты бар және ықтимал қауіптерді түсінуге және бағалауға мүмкіндік береді [7]. Бұл тиімді қорғаныс стратегияларын әзірлеу үшін маңызды.

Жаңа әдістер мен шешімдерді әзірлеу: зерттеу автоматтандырылған жүйелердің қауіпсіздігін нығайтуға көмектесетін жаңа әдістерді, алгоритмдерді, құралдар мен технологияларды әзірлеуге негіз береді.

Қолданыстағы жүйелерді бағалау: зерттеу материалдары мен тәсілдерінің көмегімен қолданыстағы автоматтандырылған жүйелердің қауіпсіздігін талдауға, осалдықтарды анықтауға және жақсартуларды ұсынуға болады.

Хабардарлықты арттыру және білім беру: зерттеу материалдары мен нәтижелері мамандар арасында да, қарапайым пайдаланушылар арасында да ақпараттық қауіпсіздік туралы білім мен түсінік деңгейін арттыруға ықпал етеді.

Оқыту мен тренингтің сапасын арттыру: зерттеулер ақпараттық қауіпсіздік бойынша неғұрлым тиімді білім беру бағдарламалары мен тренингтерін әзірлеуге негіз бола алады.

Инциденттерге жауап беруге дайындық: зерттеулер киберинциденттер мен қауіпсіздік оқиғаларына жауап беру стратегиялары мен процедураларын әзірлеуге көмектеседі.

Нәтижелер

Автоматтандырылған жүйелердің қауіпсіздігі бойынша алдыңғы бөлімде қарастырылған талдау нәтижесінде бүгінгі күні кең етек жайған бірнеше маңызды мәселелері және олардың негізгі шешу жолдары анықталды.

Осы саладағы негізгі қиындықтардың ішінде мыналарды бөліп көрсетуге болады:

– киберқауіптер мен шабуылдар: вирустар, трояндық кон, хакерлік шабуылдар, фишинг және басқалары сияқты киберқауіптердің тоқтаусыз өсуі автоматтандырылған жүйелердің қауіпсіздігіне тұрақты қауіп төндіреді.

– бағдарламалық жасақтамадағы осалдықтар мен қателер: бағдарламалық жасақтама өнімдері мен қосымшаларында шабуылдаушылар жүйеге енгізу үшін қолдана алатын осалдықтар жиі кездеседі.

– дизайндағы кемшіліктер: жүйелерді дұрыс емес жобалау және архитектурадағы кемшіліктер жүйеге шабуыл жасау үшін әлсіз жақтарды тудыруы мүмкін.

– адам факторы: қызметкерлердің қателіктері мен бақылаулары жүйенің бұзылуына әкелуі мүмкін. Бұған парольдерді кездейсоқ ашу, кіру құқығын дұрыс орнатпау және тіпті әлеуметтік инженерия кіруі мүмкін [8].

– қол жеткізуді басқарудағы кемшіліктер: деректер мен ресурстарға қол жеткізуді басқарудың жеткіліксіздігі рұқсатсыз кіруге және ақпараттың ағып кетуіне әкелуі мүмкін.

– қызметкерлердің білімі мен хабардарлығының жеткіліксіздігі: ақпаратсыз қызметкерлер қауіпсіздік тізбегінің әлсіз буыны болуы мүмкін.

– желілер мен жүйелердің күрделілігі: қазіргі заманғы желілер мен жүйелер барған сайын күрделі және өзара байланысты болып [8,9], қауіпсіздікті қамтамасыз етуді қиындатады.

– нормативтер мен заңнаманы сақтау: ұйымдар ақпараттық қауіпсіздік нормативтері мен заңнамаларын сақтауда жиі қиындықтарға тап болады.

– масштабтау және икемділік: бизнестің өсуімен және талаптардың өзгеруімен жүйелерді масштабтау және қоршаған ортаға өзгерістер енгізу қажеттілігі туындауы мүмкін [9], бұл қауіпсіздікті қамтамасыз етуді қиындатады.

– құпиялылық пен деректерді қорғауды қамтамасыз ету: құпиялылық пен деректерді қорғау, әсіресе деректерді реттеу және құпиялылықты қорғау заңдары контекстінде бірінші кезектегі міндет болып табылады.

Бұл мәселелерді шешу және автоматтандырылған жүйелердің қауіпсіздігін қамтамасыз ету үшін техникалық, ұйымдастырушылық және адами шараларды қоса алғанда, көп қырлы және көп деңгейлі тәсіл, сондай-ақ ақпараттық қауіпсіздік саласындағы жаңа қауіптер мен сын-қатерлерге үнемі жаңару және бейімделу қажет [10]. Жоғарыда сипатталған негізгі мәселелерді шешумен бірнеше жылдар бойы арнайы ғаламдар тобы жұмыс жасады. Жұмыс нәтижесінде, автоматтандырылған жүйелердің қауіпсіздігін қамтамасыз ету мәселелері бойынша келесідей негізгі аспектілер тізімі қалыптасты:

1. қауіптердің үздіксіз эволюциясы: ғалымдар киберқауіптер мен шабуыл әдістері үнемі дамып келе жатқанын мойындайды. Бұл қауіпсіздік шараларын үнемі жаңартуды және бейімдеуді қажет етеді.

2. кешенді тәсіл: қауіпсіздік мамандары техникалық, ұйымдастырушылық және адами қауіпсіздік шараларын қамтитын кешенді тәсілге шақырады.

3. қызметкерлерді оқытудың маңыздылығы: ғалымдар адам факторы көбінесе жүйелердің қауіпсіздігіне шешуші әсер ететінін атап көрсетеді. Сондықтан қызметкерлерді қауіпсіздік бойынша оқыту басымдық болып табылады.

4. жасанды интеллект пен машиналық оқытудың интеграциясы: соңғы жылдары жасанды интеллект пен машиналық оқыту қауіпті анықтау мен талдауда шешуші рөл атқарды. Ғалымдар оларды қауіпсіздік жүйелеріне біріктіруді ұсынады.

5. нормативтер мен заңнаманы сақтау: зерттеу нәтижелері ақпараттық қауіпсіздік саласындағы нормативтер мен заңнаманы сақтаудың маңыздылығын көрсетеді.

6. инциденттерге жауап беру: ғалымдар инциденттерге жауап беру жоспарларын әзірлеуге және үнемі жаңартуға шақырады. Оқиғаларға реакция тез және үйлестірілген болуы керек.

7. қауіптер туралы ақпаратты талдау және бөлісу: ғалымдардың тұжырымдары ұйымдар мен институттар арасындағы қауіптер туралы ақпаратты жинау, талдау және бөлісудің маңыздылығын көрсетеді.

8. саналы қауіпсіз мәдениетті құру: ғалымдар ұйымдарда қауіпсіздік мәдениетін құруды ұсынады, мұнда әр қызметкер қауіпсіздікті қамтамасыз етудегі өз рөлін түсінеді.

9. жаңа технологияларды зерттеу және дамыту: ғалымдар киберқауіптермен күресу үшін жаңа технологияларды зерттеуге және дамытуға инвестиция салуға шақырады.

10. ынтымақтастық және серіктестік: зерттеу нәтижелері тәжірибе мен ресурстармен алмасу үшін ұйымдар мен секторлар арасындағы ынтымақтастықтың маңыздылығын көрсетеді.

Жалпы, ғалымдардың тұжырымдары автоматтандырылған жүйелердің қауіпсіздігін қамтамасыз ету өзгерістерге, оқытуға, ынтымақтастыққа және заманауи әдістер мен технологияларды енгізуге үнемі дайындықты қажет ететіндігін растайды. Қауіпсіздік мәселелерін шешу – бұл барлық қатысушылардың назарын және күш-жігерін қажет ететін үздіксіз және көп қырлы процесс.

Талдау

Автоматтандырылған жүйелердің қауіпсіздігін қамтамасыз ету негізінде бірнеше талдау жұмыстары сан ғасырлардан бері жүргізіліп келеді [11]. Атап айтатын болсақ, жасанды интеллект және машиналық оқыту, киберфизикалық жүйелер, кванттық криптография, заттар интернеті (IoT), блокчейн және криптовалюта, қауіпсіздікті басқару жүйелері (Security Information and Event Management, SIEM), кибергигиеналық зерттеулер және т.б. зерттеулер

мен талдаулар жүйесі ұсынылды. Көрсетілген, еңбектер мен талдауларға сүйене отырып, төмендегідей қорытынды жасалды (кесте 2):

Кесте 2 – Ұйымдар автоматтандырылған жүйелер мен деректерді қорғауды қамтамасыз ету үшін қолдана алатын стратегиялар мен шаралар

Атауы	Сипаттама
Көп факторлы аутентификация (MFA)	құпия сөз және бір реттік код сияқты пайдаланушының жеке басын тексерудің екі немесе одан да көп әдістерін қажет ететін MFA енгізу қосымша қауіпсіздік деңгейін қамтамасыз етеді.
Желі қауіпсіздігі	брандмауэрді орнату, кіруді анықтау, желілік шифрлау және желіге кіруді басқару желілік инфрақұрылымды қорғауға көмектеседі.
Деректерді шифрлау	деректерді тасымалдау және сақтау кезінде шифрлау ақпараттың құпиялылығын қамтамасыз етеді.
Желілік сегментация	желіні қол жетімділік пен қауіпсіздіктің әртүрлі деңгейлері бар сегменттерге бөлу, бұл шабуылдың таралуын шектеуге көмектеседі.
Антивирустық және антималварлық шешімдер	зиянды бағдарламаларды анықтау және жою үшін антивирустық және антималварлық бағдарламаларды қолдану.
Оқиғалар журналын талдау	қалыптан тыс белсенділік пен ықтимал оқиғаларды анықтау үшін оқиғалар журналын жүргізу және талдау.
Физикалық қауіпсіздік	серверлер мен инфрақұрылымды физикалық қорғауды қамтамасыз ету.
Қауіпсіздік саясаты	құпия сөз саясатын, кіруді басқару ережелерін және т.б. қоса алғанда, қатаң қауіпсіздік саясатын әзірлеу және енгізу.

Бұл шаралар мен стратегияларды ұйымның ерекшеліктеріне және оның қауіпсіздік қажеттіліктеріне бейімдеуге болады. Сонымен қатар, пайда болған қауіптерге жауап ретінде қауіпсіздік жүйелерін үнемі жаңартып отыру және жетілдіру маңызды.

Қорытынды

Автоматтандырылған жүйелерді пайдалану және жұмыс жасау өмірде болып жатқан оқиғалар мен процестерді қаншалықты оңтайлатып, атқарылатын іс-шаралар тізімін барынша қысқартқандығы сияқты, жүйелердің қауіпсіздік мәселесімен айналысу да аса маңызды аспект екендігі айқындалды. Талдау барысында автоматтандырылған жүйелердің негізгі қауіпсіздік мәселелері, туындау себептері мен алдын алу шаралары көрсетілді. Яғни, автоматтандырылған жүйелердің қауіпсіздігі қазіргі цифрлық дәуірдің ажырамас бөлігі болып табылады. Автоматтандырылған жүйелердің қауіпсіздігі туралы мақаланың қорытындысы киберқауіптер барған сайын күрделі және жойқын болып жатқан әлемде деректерді қорғау мен функционалдылықты қамтамасыз етудің маңыздылығын көрсетеді.

Қорытынды келесі негізгі ойларды негіздеді:

– қауіпсіздіктің ұзақ мерзімді рөлі: автоматтандырылған жүйелердің қауіпсіздігі бір реттік міндет емес. Бұл тұрақты назар мен инвестицияны қажет ететін ұзақ мерзімді міндеттеме.

– заманауи қиындықтар: жасанды интеллект және Заттар интернеті сияқты заманауи технологиялар жаңа мүмкіндіктер береді, сонымен қатар жаңа қауіптер. Ұйымдар осы қиындықтарға бейімделуі керек.

– қауіпсіздік мәдениеті: ұйымда қауіпсіздік мәдениетін құру маңызды аспект болып табылады. Қызметкерлерді оқыту және қауіпсіздік ережелерін сақтау тәуекелді азайтуға көмектеседі.

– ынтымақтастық және ақпарат алмасу: ұйымдар арасындағы ынтымақтастық және қауіп-қатер туралы ақпарат алмасу киберқылмыспен тиімді күресу үшін маңызды бола түсуде.

– міндетті сәйкестік: ұйымдар деректер мен ақпараттық технологиялардың қауіпсіздігі саласындағы нормативтер мен заңнаманы сақтауы керек.

Автоматтандырылған жүйелердің қауіпсіздігі тек техникалық міндет қана емес, сонымен қатар қазіргі әлемдегі ұйымдардың табысты қызметінің стратегиялық аспектісі.

Деректер мен инфрақұрылымды сенімді қорғау ұзақ мерзімді табыстың негізгі факторы болып табылады.

Әдебиеттер тізімі

1. Мезенцев К.Н. Автоматизированные информационные системы / К.Н. Мезенцев. – М.: Academia. – 2021. – 176 с.
2. Мезенцев К.Н. Автоматизированные информационные системы / К.Н. Мезенцев. – М.: Академия. – 2019. – 176 с.
3. Солодянников А.В. Информационная безопасность автоматизированных систем – М.: СПбГЭУ, 2020. – 109 с.
4. Чипига А.Ф. Информационная безопасность автоматизированных систем – М.: Гелиос АРВ, 2017. – 336 с.
5. Лозовецкий В.В., Комаров Е.Г., Лебедев В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей – М.: учебник для вузов, 2023. – 488 с.
6. Awad A., Furnell S., Paprzycki M., Sharma S. (Eds.) Security in Cyber-Physical Systems: Foundations and Applications – M.: Springer, 2021. – 273 с.
7. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
8. Ивлев В.А. ABIS. Информационные системы на основе действий / В.А. Ивлев, Т.В. Попова. – М.: 1С-Паблишинг, 2019. – 248 с.
9. Michael E. Whitman, Herbert J. Mattord Principles of Information Security 6th Edition – M.: Cengage Learning, 2017. – 656 с.

References

1. Mezentsev K.N. Automated information systems / K.N. Mezentsev. – M.: Academia. – 2021. – 176 p. (In Russian).
2. Mezentsev K.N. Automated information systems / K.N. Mezentsev. – M.: Academy. – 2019. – 176 p. (In Russian).
3. Solodyannikov A.V. Information security of automated systems – Moscow: SPbGEU, 2020. – 109 p. (In Russian).
4. Chipiga A.F. Information security of automated systems – M.: Helios ARV, 2017. – 336 p. (In Russian).
5. In Lozovetsky.V., Komarov E.G., V. Lebedev. V. Protection of automated information processing systems and telecommunication networks – M.: textbook for universities, 2023. – 488 p. (In Russian).
6. Awad A., Fernell S., Papshicki M., Sharma S. (eds.) Security in cyberphysical systems: fundamentals and applications – Moscow: Springer, 2021. – 273 p. (In English).
7. Zapechnikov S.V. Information security of open systems. In 2 t. t.2 – Means of protection in networks / S.V. Zapechnikov, N.G. Miloslavskaya, A.I. Tolstoy, D.V. Ushakov. – M.: GLT, 2018. – 558 p. (In Russian).
8. Ivlev V. A. ABIS. Information systems based on actions / V.A. Ivlev, T.V. Popova. – M.: 1C-Publishing, 2019, – 248 p. (In Russian).
9. Michael E. Whitman, Herbert J. Mattord Principles of Information Security, 6th edition – Moscow: Cengage Learning, 2017. – 656 p. (In English).

Ж.М. Алимжанова, А.К. Байузакова*

Казахский национальный университет имени аль-Фараби,
050040, Республика Казахстан, г. Алматы, пр. аль-Фараби, 71
*e-mail: zhannamen@mail.ru, arailim107@mail.ru

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

В данной статье речь идет о проблеме «автоматизированная система и ее безопасность», которая сегодня активно используется в рамках информационных систем. В каких отраслях применяются автоматизированные системы, решается проблема

надежности с точки зрения безопасности и анализа состояния защиты. Автоматизированные системы имеют большое значение в современном мире, поскольку значительно упрощают и ускоряют выполнение различных повседневных задач, управление данными и процессами. Актуальность автоматизированных систем зависит от таких факторов, как эффективность и производительность, улучшение качества данных, масштабирование, развитие аналитики. Однако важно понимать, что с ростом автоматизации возрастает и риск в области безопасности данных и конфиденциальности. Автоматизированные системы становятся мишенью для кибератак и могут угрожать конфиденциальности, целостности и доступности данных. Таким образом, безопасность автоматизированных систем остается одной из основных проблем. То есть отсутствие надлежащих мер безопасности может привести к потере данных, нарушению конфиденциальности и финансовым потерям. Поэтому организациям необходимо активно инвестировать в защиту и мониторинг своих атомных электростанций, контролируя доступ, шифруя, внедряя механизмы обнаружения инцидентов и обучая сотрудников правилам безопасности.

Ключевые слова: *автоматизированная система, безопасность, компьютер, интернет, антивирус, технология.*

Z.M. Alimzhanova, A.K. Baiuzakova*
Kazakh National University named after Al-Farabi,
050040, Republic of Kazakhstan, Almaty, 71 al-Farabi Avenue
*e-mail: zhannamen@mail.ru, arailim107@mail.ru

PROBLEMS OF ENSURING THE SAFETY OF AUTOMATED SYSTEMS

The article discusses the issue of "automated system and its security", which is actively used today in the framework of Information Systems. In what areas are automated systems used, the problem of strength in terms of safety and analysis of the state of protection is solved.

Automated systems are of great importance in the modern world, as they greatly simplify and speed up the implementation of various daily tasks, data and process management. The relevance of automated systems depends on such factors as efficiency and productivity, improving data quality, scaling, and developing analytics. However, it is important to understand that with the growth of automation, the risk in the field of data security and privacy will also increase. Automated systems become targets of cyber attacks and can threaten the confidentiality, integrity and availability of data. Thus, the safety of automated systems remains one of the main issues. That is, the lack of appropriate security measures can lead to data loss, privacy violations and financial losses. Therefore, organizations need to actively invest in the protection and control of their nuclear power plants by implementing access control, encryption, incident detection mechanisms, and training employees in safety regulations.

Key words: *automated system, security, computer, internet, antivirus, technology.*

Авторлар туралы мәліметтер

Жанна Муратбековна Алимжанова – физика-математика ғылымдарының докторы, әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан, e-mail: zhannamen@mail.ru.

Арайлым Қайратқызы Байузакова – магистрант, әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан, e-mail: arailim107@mail.ru.

Сведения об авторах

Жанна Муратбековна Алимжанова – доктор физико-математических наук, профессор, Казахский Национальный Университет имени Аль-Фараби, Алматы, Казахстан, e-mail: zhannamen@mail.ru.

Арайлым Қайратқызы Байузакова – магистрант, Казахский Национальный Университет имени аль-Фараби, Алматы, Казахстан, e-mail: arailim107@mail.ru.

Information about the authors

Zhanna Muratbekovna Alimzhanova – doctor of physical and mathematical sciences, professor, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: zhannamen@mail.ru.

Arailym Baiuzakova – master's degree, Al-Farabi Kazakh National University, Almaty, Kazakhstan, arailim107@mail.ru.

Материал 24.10.2023 ж. баспаға түсті.

DOI: 10.53360/2788-7995-2023-4(12)-6

ISTIR: 20.53.17

A.T. Manap*, G.A. Abitova
Astana IT University,
010000, Republic of Kazakhstan, Astana, Mangilik El Avenue, 55/11
*e-mail: abusaid.manap@gmail.com

DEVELOPMENT OF INFORMATION TECHNOLOGY FOR SECURE FILE STORAGE BASED ON HYBRID CRYPTOGRAPHY METHODS

Abstract: *This article explores the development of information technology for secure file storage based on hybrid cryptography methods. It highlights the importance of secure file storage in the digital age and introduces hybrid cryptography as a solution for enhanced data security. The purpose of the article is to provide a comprehensive understanding of the benefits and advancements in hybrid cryptography for secure file storage.*

The article discusses the differences between symmetric and asymmetric encryption algorithms and introduces hybrid cryptography as a combination of both. It delves into the advantages of hybrid cryptography, emphasizing its ability to provide robust security and efficient data protection. The use of hybrid cryptography in encryption at rest and encryption in transit is examined, highlighting its role in securing stored data and ensuring secure data transmission.

Moreover, the article explores the authentication, integrity, and reliability features provided by hybrid cryptography. It discusses the importance of key management and its impact on secure file storage.

Key words: *cryptography; analysis; secure storage; secure transmission; encryption.*

Introduction

In the digital age, where vast amounts of data are generated and exchanged daily, the importance of secure file storage cannot be overstated. Protecting sensitive information from unauthorized access, tampering, or loss has become a critical concern for businesses, organizations, and individuals alike. To address this challenge, the concept of hybrid cryptography has emerged as a powerful solution for enhanced data security. This chapter aims to explore the development of information technology for secure file storage based on hybrid cryptography methods, highlighting its significance in the digital landscape.

The purpose of this article is to delve into the development of information technology for secure file storage based on hybrid cryptography methods. By exploring the importance of secure file storage in the digital age and introducing the concept of hybrid cryptography, we aim to highlight the significance of this approach in enhancing data security. The article will provide insights into the benefits of secure file storage and the role of hybrid cryptography in ensuring confidentiality, integrity, and availability of stored data.

In today's interconnected world, where data breaches and cyber threats are prevalent, secure file storage is crucial for several reasons:

1. **Confidentiality:** Secure file storage ensures that sensitive information remains confidential by employing encryption techniques that render data unreadable to unauthorized