ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ҚАЙЫРЫМДЫЛЫҚ ҚОРЫ HALYK CHARITY FOUNDATION

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ
«ХАЛЫҚ» ЖҚ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»
ЧФ «Халық»

NEWS

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
«Halyk» Private Foundation

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

1 (349)

JANUARY – MARCH 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

ЧФ «ХАЛЫҚ»

В 2016 году для развития и улучшения качества жизни казахстанцев был создан частный Благотворительный фонд «Халык». За годы своей деятельности на реализацию благотворительных проектов в областях образования и науки, социальной защиты, культуры, здравоохранения и спорта, Фонд выделил более 45 миллиардов тенге.

Особое внимание Благотворительный фонд «Халык» уделяет образовательным программам, считая это направление одним из ключевых в своей деятельности. Оказывая поддержку отечественному образованию, Фонд вносит свой посильный вклад в развитие качественного образования в Казахстане. Тем самым способствуя росту числа людей, способных менять жизнь в стране к лучшему – профессионалов в различных сферах, потенциальных лидеров и «великих умов». Одной из значимых инициатив фонда «Халык» в образовательной сфере стал проект Ozgeris powered by Halyk Fund – первый в стране бизнес-инкубатор для учащихся 9-11 классов, который помогает развивать необходимые в современном мире предпринимательские навыки. Так, на содействие малому бизнесу школьников было выделено более 200 грантов. Для поддержки талантливых и мотивированных детей Фонд неоднократно выделял гранты на обучение в Международной школе «Мирас» и в Astana IT University, а также помог казахстанским школьникам принять участие в престижном конкурсе «USTEM Robotics» в США. Авторские работы в рамках проекта «Тәлімгер», которому Фонд оказал поддержку, легли в основу учебной программы, учебников и учебно-методических книг по предмету «Основы предпринимательства и бизнеса», преподаваемого в 10-11 классах казахстанских школ и колледжей.

Помимо помощи школьникам, учащимся колледжей и студентам Фонд считает важным внести свой вклад в повышение квалификации педагогов, совершенствование их знаний и навыков, поскольку именно они являются проводниками знаний будущих поколений казахстанцев. При поддержке Фонда «Халык» в южной столице был организован ежегодный городской конкурс педагогов «Almaty Digital Ustaz.

Важной инициативой стал реализуемый проект по обучению основам финансовой грамотности преподавателей из восьми областей Казахстана, что должно оказать существенное влияние на воспитание финансовой грамотности и предпринимательского мышления у нового поколения граждан страны.

Необходимую помощь Фонд «Халык» оказывает и тем, кто особенно остро в ней нуждается. В рамках социальной защиты населения активно проводится работа по поддержке детей, оставшихся без родителей, детей и взрослых из социально уязвимых слоев населения, людей с ограниченными возможностями, а также обеспечению нуждающихся социальным жильем, строительству социально важных объектов, таких как детские сады, детские площадки и физкультурно-оздоровительные комплексы.

В копилку добрых дел Фонда «Халык» можно добавить оказание помощи детскому спорту, куда относится поддержка в развитии детского футбола и карате в нашей стране. Жизненно важную помощь Благотворительный фонд «Халык» оказал нашим соотечественникам во время недавней пандемии COVID-19. Тогда, в разгар тяжелой борьбы с коронавирусной инфекцией Фонд выделил свыше 11 миллиардов тенге на приобретение необходимого медицинского оборудования и дорогостоящих медицинских препаратов, автомобилей скорой медицинской помощи и средств защиты, адресную материальную помощь социально уязвимым слоям населения и денежные выплаты медицинским работникам.

В 2023 году наряду с другими проектами, нацеленными на повышение благосостояния казахстанских граждан Фонд решил уделить особое внимание науке, поскольку она является частью общественной культуры, а уровень ее развития определяет уровень развития государства.

Поддержка Фондом выпуска журналов Национальной Академии наук Республики Казахстан, которые входят в международные фонды Scopus и Wos и в которых публикуются статьи отечественных ученых, докторантов и магистрантов, а также научных сотрудников высших учебных заведений и научно-исследовательских институтов нашей страны является не менее значимым вкладом Фонда в развитие казахстанского общества.

С уважением,
Благотворительный Фонд «Халык»!

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1. Namber 349 (2024). 7–20
https://doi.org/10.32014/2024.2518-1726.238

МРНТИ- 81.93.29
УДК 372.851.02

© K.S. Aldazharov, S.K. Batyrkhan*, 2024
Narxoz University, Almaty, Kazakhstan.
E-mail: serik.batyrkhan@narxoz.kz

ANALYSIS OF THE MODERN MODEL OF INFORMATION SECURITY

Aldazharov K.S. — Candidate of Economic Sciences, Associate Professor at the School of Digital Technologies, Narxoz University, Almaty, Kazakhstan
E-mail kanagat.aldazharov@narxoz.kz, https://orcid.org/0000-0002-3181-4539;
Batyrkhan S.K. – Master of Technical Sciences, Senior Lecturer at the School of Digital Technologies, Narxoz University, Almaty, Kazakhstan
E-mail serik.batyrkhan@narxoz.kz, https://orcid.org/my-orcid?orcid=0000-0002-4726-5626.

Abstract. The current situation related to the spread of the virus pandemic shows a sharp increase in cyber attacks, which negatively affects the preservation of corporate and personal data. In this regard, studies aimed at studying the problems of information security are relevant. The article is devoted to the analysis of the problems of using the Zero Trust information protection model (zero trust). It attempts to reveal the concept of this model, as a result of which it considers the possibility of moving from the traditional method of protection "perimeter protection" to the "zero trust" model. At the same time, since this concept is just a theory, we did not offer practical steps for its implementation, so different companies may act differently. In this article, we provide information on the practical implementation of steps to mitigate the risk of Zero Trust Network Access (ZTNA). Its purpose is that at some point a company may realize that the network infrastructure includes outdated devices and software that cannot implement modern security standards. At the same time, a trusted zone is formed within the corporate network, which allows users, devices and applications to carry out certain actions, taking into account data security. At the same time, the ways of this transition are given on the examples of Microsoft and Google. The issues under study will be of interest to specialists in the field of cybersecurity.

Keywords: Zero trust, security, information, information security, general control, data analysis

© К.С. Алдажаров, С.К. Батырхан*, 2024
Narxoz Университеті, Алматы, Қазақстан.
E-mail: serik.batyrkhan@narxoz.kz

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ҚАЗІРГІ ЗАМАНҒЫ МОДЕЛІН ТАЛДАУ

Алдажаров К.С. — э.ғ.к., Цифрлық технология мектебінің қауымдастырылған профессоры, Нархоз университеті, Алматы, Қазақстан
E-mail kanagat.aldazharov@narxoz.kz, https://orcid.org/0000-0002-3181-4539;
Батырхан С.К. — т.ғ.м., Цифрлық технология мектебінің аға оқытушысы, Нархоз университеті, Алматы, Қазақстан
E-mail serik.batyrkhan@narxoz.kz, https://orcid.org/my-orcid?orcid=0000-0002-4726-5626.

Аннотация. Вирус пандемиясының таралуымен байланысты болып отырған қазіргі жағдай кибершабуылдардың күрт өсуін көрсетуде, бұл корпоративтік және дербес деректердің сақталуына теріс әсерін тигізуде. Осыған байланысты ақпараттық қауіпсіздік мәселелерін зерттеуге бағытталған зерттеулер өзекті болып табылады. Мақала Zero Trust (нөлдік сенім) ақпараттық қауіпсіздік моделін қолдану мәселелерін талдау тақырыбына арналған. Мақала осы модельдің тұжырымдамасын талдауды білдіреді, осының нәтижесінде дәстүрлі «периметрді қорғау» қорғаныс әдісінен «нөлдік сенім» моделіне көшу мүмкіндіктерін қарастырады. Сонымен қатар бұл тұжырымдаманың өзі тек теория болғандықтан, оны іске асырудың практикалық қадамдарын ұсынбадық, сондықтан әртүрлі компаниялар әртүрлі әрекет ете алады. Мақалада Zero Trust Network Access (ZTNA) тәуекелдерді азайту қадамдарының практикалық орындалуы туралыда ақпаратты береміз. Оның мақсаты, бір сәтте компания желілік инфрақұрылымның ескірген құрылғылар мен бағдарламалық қамтамасыз етуді қамтитынын білуі мүмкін, оларда заманауи қауіпсіздік стандарттарын енгізу мүмкін емес. Оларды ауыстыру көп ресурстарды және уақытты қажет етеді. Бұл ретте корпоративтік желі ішінде сенімді аймақ қалыптасады, ол пайдаланушыларға, құрылғылар мен қолданбаларға деректер қауіпсіздігін ескере отырып, белгілі бір әрекеттерді орындауға мүмкіндік береді. Бұл ретте Microsoft және Google компанияларының мысалдарында осы көшудің амал-тәсілдері келтірілген. Зерттелетін мәселелер киберқауіпсіздік саласындағы мамандарды қызықтыруы мүмкін.

Түйін сөздер: Нөлдік сенім, қауіпсіздік, ақпарат, ақпараттық қауіпсіздік, жалпы бақылау, деректер талдау

© К.С. Алдажаров, С.К. Батырхан*, 2024
Университет Нархоз, Алматы, Казахстан.
E-mail: serik.batyrkhan@narxoz.kz

АНАЛИЗ СОВРЕМЕННОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Алдажаров К.С. — к.э.н., ассоциированный профессор Школы цифровых технологий, Университет Нархоз, Алматы, Казахстан
E-mail kanagat.aldazharov@narxoz.kz, https://orcid.org/0000-0002-3181-4539;
Батырхан С.К. — м.т.н., старший преподаватель Школы цифровых технологий, Университет Нархоз, Алматы, Казахстан
E-mail serik.batyrkhan@narxoz.kz, https://orcid.org/my-orcid?orcid=0000-0002-4726-5626.

Аннотация. Современная ситуация, связанная с распространением пандемии вируса показывает резкий рост кибератак, что негативно сказывается на сохранении корпоративных и персональных данных. В этой связи исследования, направленные на изучение вопросов безопасности информации являются актуальными. Статья посвящена анализу проблем использования модели защиты информации Zero Trust (нулевое доверие). В ней предпринята попытка раскрытия концепции данной модели, в результате которой рассматриваются возможности перехода от традиционого метода защиты «защите периметра» к модели "нулевое доверие". В то же время, поскольку данная концепция является всего лишь теорией, практических шагов по ее реализации мы не предлагали, поэтому компании могут действовать по-разному. В этой статье мы предоставляем информацию о практической реализации шагов по снижению риска доступа к сети с нулевым доверием (ZTNA). Цель состоит в том, что в какой-то момент компания может осознать, что сетевая инфраструктура включает в себя устаревшие устройства и программное обеспечение, в которых невозможно реализовать современные стандарты безопасности. При этом внутри корпоративной сети образуется доверенная зона которая позволяет пользователям, устройствам и приложениям проводить определенные действия с учетом безопасности данных. Авторами приведены способы этого перехода на примерах компаний Microsoft и Google. Изучаемые вопросы заинтересуют специалистов в области кибербезопасности.

Ключевые слова: нулевое доверие, безопасность, информация, информационная безопасность, общий контроль, анализ данных

Кіріспе

Қазіргі уақытта бизнес үшін басты проблема ақпараттық қауіпсіздік тәуекелдері болып отыр. Мәселен, Positive Technologies (ақпараттық қауіпсіздік саласындағы бағдарламалық жасақтаманы әзірлеуге маманданып отырған халықаралық компания) бағалаулары бойынша, COVID-19 тақырыбымен

жаппай шабуылдар да, APT шабуылдар да байланысты болды. 2020 жылдың ішінде шифрлаушылардың шабуылдар санының үнемі өсіп отырғандығы байқалды. Қашықтан жұмыс істеудің жер-жерде кеңінен енгізілуіне орай, ақпараттық қауіпсіздіктің жаңа тәуекелдері пайда болды, әлеуметтік инженерия ұйымдардың желісіне ену үшін жиі қолданыла бастады. Жаһандық жаңалықтардың себебін — эпидемияны — хакерлік топтардың барлық түрлері қолданды. Бұл ретте, 2019 жылы болжанғандай, 2020 жылы APT-шабуылдардың саны өсуін жалғастырды («Өзекті киберқауіптер: 2020 жылдың III тоқсаны», 2020). Сондықтан қазіргі таңда ақпаратты қорғау өте өзекті мәселе болым табылады. Мақаланың тақырыбы осыған орай таңдалды.

Зерттеудің мақсаты – ақпараттық қауіпсіздігін қамтамасыз етуге қолданылатын заманауи әдістердің, яғни Zero Trust моделін талдау болып табылады.

Әдеттегідей, инфрақұрылымды қорғаған кезде, компаниялар «периметрді қорғау» ұғымын пайдаланады. Бұл қағида компанияның ресурстарына сырттан қосылуға тырысатын барлық нәрсені мұқият тексеруді көздейді. Бұл ретте периметрдің ішінде (яғни корпоративтік желіде) осында пайдаланушылар, құрылғылар мен қосымшалар белгілі бір іс-қимыл еркіндігіне ие болатын сенім білдірілген аймақ құрылады.

Әдістер мен материалдар

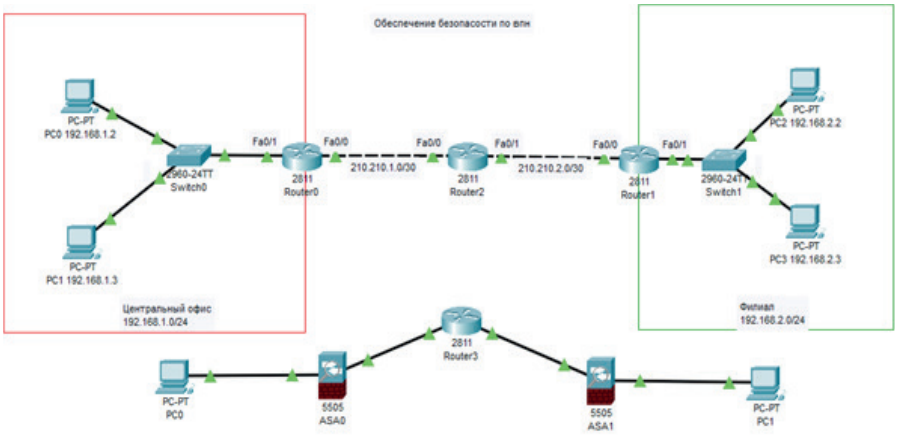
Қауіпсіздікті виртуалды VPN желісін құру кезінде ақпараттық қауіпсіздікті қамтамасыз ету міндеті өте маңызды болып келеді. Жалпы қабылданған анықтамаға сәйкес деректердің қауіпсіздігі олардың құпиялылығын, тұтастығын және қол жетімділігін білдіреді. VPN міндеттеріне қатысты деректер қауіпсіздігінің критерийлері келесідей анықталуы мүмкін:

a) Құпиялылық - деректерді қауіпсіз VPN арналары арқылы беру процесінде бұл мәліметтер заңды жөнелтуші мен алушыға ғана белгілі бола алатындығына кепілдік;

b) Тұтастық туралы - қауіпсіз VPN арнасы арқылы өту кезінде берілетін деректердің қауіпсіздігінің кепілі. Жаңа деректерді өзгерту, жою немесе құру әрекеттері анықталып, заңды пайдаланушыларға белгілі болады;

c) Қол жетімділік - VPN функцияларын орындайтын құралдардың заңды пайдаланушыларға үнемі қол жетімді екендігінің кепілі. VPN құралдарының қол жетімділігі - бұл бірқатар факторларға тәуелді болатын күрделі көрсеткіш: іске асырудың сенімділігі, қызмет көрсету сапасы және құралдың өзін сыртқы шабуылдардан қорғау дәрежесі.

VPN (Virtual Private Network) - виртуалды жеке желі. VPN технологиясы қашықтағы пайдаланушыларға жалпыға ортақ желілер арқылы (мысалы, Интернет) қауіпсіз байланыс арналарын қолдана отырып, жергілікті желіге қосылуға мүмкіндік береді. Қазіргі таңда локалды желіні қолдана отырып алыс қашықтағы офистарды қауіпсіз басқаруға осы моделді қолданып іске асыруға болады. Осы қауіпсіздікті қамтамасыз ету барысында жаңа технологияны қолдана отырып қашықтан пайдаланушыларға арналған VPN құрылымдық диаграммасы құрылды. Осы тақырып негізінде VPN құрылымдық қауіпсіздік моделін 1-суретте көруге болады.



1-сурет. VPN құрылымдық диаграммасы
Figure 1. VPN structural diagram

Сенім білдірілген аймақ жергілікті желімен және оған қосылған стационарлық құрылғылармен шектеліп келген кезде, периметрді қорғау тиімді болған еді. Алайда, ұйымдар мен олардың қызметкерлері пайдаланатын мобильді гаджеттер мен бұлттық сервистердің санының өсуімен, периметр ұғымы бұлыңғыр болып кетті. Қазіргі заманғы компаниялардың көпшілігінде корпоративтік ресурстардың ең аз дегенде бір бөлігі кеңседен, ал кей кездері елден де тыс жерде орналасқан. Тиісінше, оларды бір үлкен қабырғаның артына жасырып қою мүмкін емес. Ал енді сенім білдірілген аймақтың ішіне өтіп, онда еш кедергісіз жүріп-тұру анағұрлым оңайырақ бола бастады.

Сондықтан, 2010 жылы Forrester Research жобасының талдаушысы Джон Киндерваг (John Kindervag) «периметрді қорғауға» балама ретінде «нөлдік сенім» тұжырымдамасын ұсынды. Ол ресурстарды сыртқы және ішкі деп бөлуден бас тартуды ұсынды. Zero Trust тұжырымдамасы — бұл шын мәнінде қандай да болсын сенім білдірілген аймақтардың толық болмауы. Осы модельдің аясында пайдаланушылар, құрылғылар және қосымшалар қандай да бір корпоративтік ресурске кіруді талап еткен әрбір ретте тексерілуге тиіс болады (Peters, 2019).

Нәтижелер және оларды талқылау

«Нөлдік сенімге» негізделген қауіпсіздік жүйесін өрістетуге деген бірыңғай көзқарас, амал-тәсіл жоқ. Алайда, мұндай жүйені құруға мүмкіндік беретін бірнеше негізгі принципті бөліп көрсетуге болады (Golubev, 2020).

1. «Нөлдік сенім» моделінің контекстінде *«қорғаныс беті» (protect surface)* туралы айту қабылданған. Оған ұйым рұқсатсыз кіруден қорғауы керек болатын барлық нәрсе: құпия деректер, инфрақұрылым элементтері және т.б. кіреді. Қорғаныс беті бұған барлық ықтимал осал инфрақұрылым объектілері, процестер мен оларға қатысушылар кіретін шабуыл бетінен әлдеқайда азырақ. Ал демек, шабуыл бетін нөлге келтіруден гөрі, қорғаныс бетінің қауіпсіздігін қамтамасыз ету жеңілірек болады.

2. Микросегменттеу. Сыртқы периметрді қорғауды тұспалдайтын классикалық тәсілден айырмашылығы, Zero Trust моделі корпоративті желіні және басқа да ресурстарды тіптен жалғыз ғана құрылғыдан немесе қосымшадан тұратын шағын тораптарға бөлуді шамалайды. Шығатын жерде өздерінің қауіпсіздік саясаттары мен қол жетімділік құқықтары бар көптеген микроскопиялық периметрлер алынады. Бұл қол жеткізуді икемді басқаруға және желінің ішінде қатердің бақылаусыз таралуын болдырмауға мүмкіндік береді.

3. *Ең аз артықшылықтар принципі*. Әрбір пайдаланушыға өзінің міндеттерін орындау үшін қанша қажет болса, дәл сонша құқық беріледі. Тиісінше, егер жекелеген пайдаланушының аккаунты бұзылса, бұл бүкіл инфрақұрылымның емес, тек ресурстардың бір бөлігінің әшкереленуіне алып келуі мүмкін.

4. «Жаппай сенімсіздік» доктринасы, кері нәрсе дәлелденбейінше, корпоративті ақпаратқа қол жеткізудің кез-келген әрекетінен ықтимал қауіп-қатерді көруге кеңес береді. Яғни, әрбір нақты сессия үшін пайдаланушы (құрылғы, қосымша) *анықтап танып, сәйкестендіру рәсімінен* өтуге және өзінің қандай да бір деректерге қол жеткізу құқығын растауға тиіс.

5. *Жаппай бақылау*. «Нөлдік сенім» моделін тиімді енгізу үшін, IT-бөлімі барлық жұмыс құрылғылары мен қосымшаларын басқару мүмкіндігіне ие болуы керек. Сондай-ақ, соңғы нүктелердегі және инфрақұрылымның басқа элементтеріндегі барлық оқиғалар туралы ақпаратты жазып алып, талдаған маңызды.

Жалпы алғанда, «нөлдік сенім» қауіпсіздік моделін 2-сурет түрінде көрсетуге болады.

2-сурет. Нөлдік сенім қауіпсіздік моделі
Figure 2. Zero trust security model

Осы модель бойынша деректерді қорғау бірінші орынға қойылады. Сондықтан корпорация үшін өзінің деректерін талдай, қорғай, жіктей, қадағалай және қолдай білу қажеттігі туындайды. Бұл модельдің екінші саласы – корпо-

ративті желі. Ол қаскүнем осы желінің ішіне кіре алмайтындай етіп жобалануға тиіс. Бұл үшін заманауи желілік технологияларды пайдалану қажет.

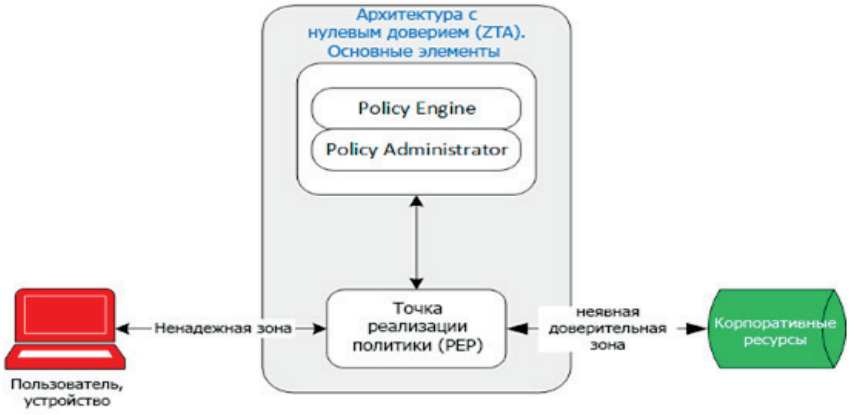
Ақпараттық қауіпсіздік жүйесіндегі адамдардың әлсіз буын болып табылатындығы белгілі. Сондықтан, бұл модельде желі мен интернеттің ішіндегі ресурстарға қол жеткізуді шектеу принципі қолданылады. Бұл ретте шектеулерге VPN, CASB (Cloud access security broker) және қызметкерлерді қорғау үшін қолжетімділіктің басқа да нұсқаларын баптау арқылы қол жеткізіледі.

Бұл модельде «Жүктеме» компоненті ерекшеленеді, ол сервистің вебсайттың ішкі бөлігінің жұмыс істеуіне жауап беретін бағдарламалық-аппараттық бөлігін білдіреді.

Заттар интернетінің таралуына байланысты, корпоративті желінің құрамында бола алатын құрылғылардың саны желінің қауіпсіздігін күрт арттырды. Бұл құрылғылар да шабуылдың ықтимал векторы болып табылады, сондықтан олар, желідегі кез-келген басқа компьютер сияқты, сегменттеуге және мониторингке ұшыратылуға тиіс. Мұның бәрі осы модельде «Құрылғылар»компоненті ретінде ескеріледі.

Осылайша, Zero Trust моделі келесі компоненттерге: сәйкестендіруді және активтерді басқаруға, қосымшаларды анықтап танып, сәйкестендіруге, желіні сегменттеуге және қауіп-қатерлерді талдауға сүйенеді.

Нөлдік сенімі бар архитектураның жоғарғы деңгейі 3-суретте көрсетілген (Наливайко, 2020).



3-сурет. Нөлдік сенімі бар архитектураның жоғарғы деңгейі

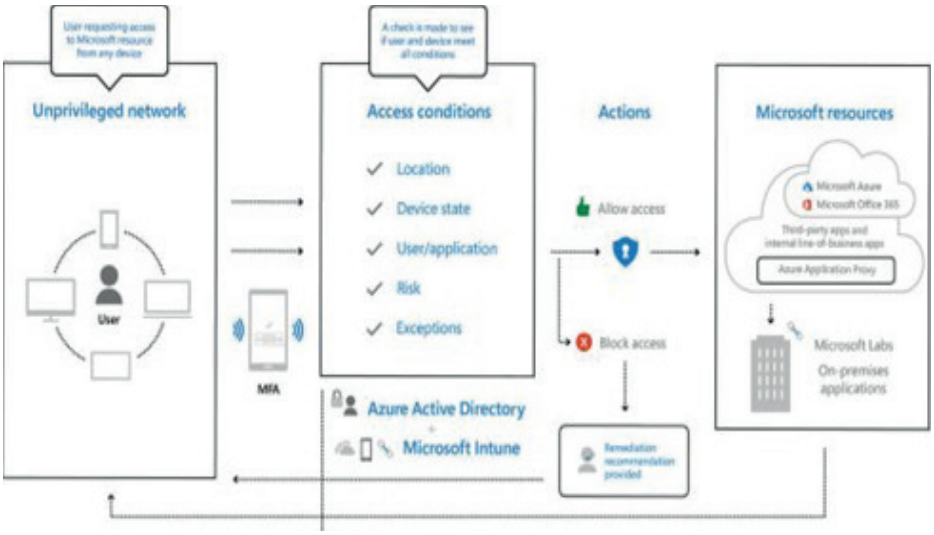
Figure 3. The top level of architecture with zero trust

Бұл деңгейде саясаттар ядросы (Policy Engine, PE) және әкімшілік ету агенті (Policy Administrator, PA) архитектураның негізін көрсетеді. Олар бірлесе саясатты жүзеге асыру нүктесін (Policy Enforcement Point, PEP) жасайды. PE қауіпсіздік саясаттарын іске қосады және оларды мінез-құлық аналитикасының көмегімен үнемі бейімдеп отырады. PA осылайша деректерге қол жеткізуге сұранысты ұсынуға, қабыл алмауға немесе кері шақырып

алуға мүмкіндік бере отырып, PE қабылдаған шешімдердің орындалуын қамтамасыз етеді. ZTA-да бір де бір пакет криптографиялық қолтаңбасыз сенімді деп саналмайды, ал саясат болса, IP-адрестерді пайдаланып емес, бағдарламалық жасақтаманы және пайдаланушыларды сәйкестендіргіштерді пайдаланып құрылады. PE мен PA арасындағы қарым-қатынасты білдірудің басқа бір тәсілі мынандай: пайдаланушы PE-ге уақыт пен күн, геолокация және құрылғының қалпы сияқты ақпаратты береді, PE тәуекелдерді бағалайды және PA-ға осыны орындау қажет болатын шешімді жібереді.

Компаниялар Zero Trust қауіпсіздік моделін қалайша пайдаланады?

Microsoft өз қызметтерімен келесі нөлдік сенім архитектурасын ұсынады (4-сурет) (Inside Track staff, 2023) .



4-сурет. Нөлдік сенім архитектурасы
Figure 4. Zero Trust Architecture

Пандемия жағдайында ұйым қызметкерлерінің қашықтан жұмыс істеу мүмкіндігі туралы мәселе туындайды. Бұл жағдайда Microsoft келесі жұмыс тәсілдерін ұсынады (Spataro J., 2020), олардың сипаттамалары 1-кестеде көрсетілген.

1 кесте. Microsoft-та қашықтан жұмыс істеуді қамтамасыз ету тәсілдері

№	Тәсілдің атауы	Сипаттамасы
1	Пайдаланушыны сәйкестендіру және кіру	Корпоративтік желіге кіруді қажет ететін пайдаланушы Azure Active Directory-мен (Azure AD) синхрондалған негізгі есептік жазбаны алады.
2	Шынайылықты көп факторлы тексеру (MFA)	Анықтап танып, сәйкестендірудің үш әдісі ұсынылады: сертификаты бар виртуалды және физикалық смарт-карталар, бизнеске арналған Windows Hello (PIN-коды немесе биометриялық кірісі бар) және Azure көп факторлы анықтап танып, сәйкестендіру.

3	Құрылғыларды басқару	Бұлттық басқару ортасына толығымен көшу. Бұл ретте Microsoft Endpoint Manager (MEM) - мен бірлесіп басқару тәсілі қолданылады. MEM Microsoft Intune мен Configuration Manager-ді мұнда пайдаланушы өзінің барлық соңғы нүктелері мен қосымшаларын басқара алатын және олардың қауіпсіздігі мен сенімділігін қамтамасыз ету үшін шаралар қолдана алатын бірыңғай консольге біріктіреді.
4	Өнімділікті арттыруға арналған қосымшалар	Outlook Mobile, Microsoft Teams және OneDrive барлық корпоративтік құрылғыларда өрістетілген, сондықтан пайдаланушылар Windows өткізгішінде, Mac-тағы Finder-де және мобильді құрылғылардағы Office қосымшаларында өздерінің электрондық поштасына, күнтізбелері мен файлдарына кіру мүмкіндігін ала алады.
5	Жиналыстар және бірлескен жұмыс	Microsoft-та күн сайын чат, жиналыстар, қоңыраулар және бірлескен жұмыс үшін Teams пайдаланылады.
6	Бизнес - қосымшаларға қол жеткізу	Windows виртуалды жұмыс үстелі қолданылады, ол жұмыс үстелдері мен қосымшаларды виртуалдандыруды жүргізуге мүмкіндік береді. Бұл ретте барлық жұмыс бұлтта жүзеге асырылады.
7	Сервистер мониторингі	Қосымшалар мен желінің өнімділігі мұқият қадағаланады. Бұл үшін әр шешімге өнім телеметриясының мониторингі енгізілген. Әрі бұл есептерді пайдаланушылардың қанағаттанушылық көрсеткіштері мен қызметтердің мінез-құлқындағы өзгерістер тұрғысынан тексеруге мүмкіндік береді.
8	Мәдениет және өзгерістерді басқару	Қызметкерлерді командаларда адамдарды біріктіретін қауымдастықтар құру үшін Yammer-ді қолдануға үйрету жүргізілуде.
9	Нақты рөлдер үшін жобалау	Microsoft корпорациясында қолдау қызметтері, сондай-ақ қашықтан жұмыс істеу кезінде туындаған мәселелер бойынша пайдаланушыға кеңес бере алатын онлайн-мамандар бар.

Google компаниясы BeyondCorp ұсынады — бұл нөлдік сенім моделін іске асыру. Ол Google-дің идеяларымен және қоғамдастықтың озық тәжірибелерімен үйлескен он жылдық жұмыс тәжірибесіне негізделген. Кіруді бақылауды желінің периметрінен жекелеген пайдаланушыларға жылжыту арқылы, BeyondCorp дәстүрлі VPN-ді пайдалануды қажет етпестен, кезкелген дерлік жерден қауіпсіз жұмыс істеуді қамтамасыз етеді (Vergadia, Saltonstall, 2020).

Microsoft сияқты, BeyondCorp та бірыңғай кіруді, кіруді, прокси кіруді бақылау саясаттарын, сондай-ақ пайдаланушылар мен құрылғылардың негізінде анықтап танып, сәйкестендіру мен авторландыруды қолдайды. Бұл ретте BeyondCorp принциптері Zero Trust моделінің принциптерімен сәйкес келеді, атап айтқанда:

- Қызметтерге қол жеткізу Сіз қосылған желіге байланысты болмауы керек.
- Қызметтерге қолжетімділік пайдаланушыдан және оның құрылғысынан контекстік факторлардың негізінде беріледі.
- Қызметтерге кіру анықтап танып, сәйкестендірілуге, авторландырылуға және шифрлануға тиіс.

Бұл тұжырымдаманың жеке қосымшасы да бар - бұл нөлдік сеніммен

желіге кіру немесе Zero Trust Networks деп аталады. Біз осы тұжырымдамамен және оның негізінде жатқан принциптермен айналысамыз (Peter Rising, 2023).

Жарайды, бірақ Zero Trust Network Access бағдарламасының бұған қандай қатысы бар деп ойларсыз?

Өйткені, тұжырымдаманың өзі тек теория болды, ол іске асырудың практикалық қадамдарын ұсынбады, сондықтан әртүрлі компаниялар әртүрлі әрекет етті. Бірақ Zero Trust Network Access (ZTNA) тәуекелдерді азайту қадамдарының практикалық орындалуы туралы ақпаратты бере алады.

Сонымен қатар, бір сәтте компания желілік инфрақұрылымның ескірген құрылғылар мен бағдарламалық қамтамасыз етуді қамтитынын білуі мүмкін, оларда заманауи қауіпсіздік стандарттарын енгізу мүмкін емес немесе қиын. Оларды ауыстыру көп ресурстарды және уақытты қажет етеді. Дегенмен, барлық қызметкерлер дайын болған жағдайда, барлық мәселелерді шешу өте шынайылыққа тән (Golubev, 2020). Қол жеткізуді басқарудан және көп факторлы аутентификациядан бастаған жөн, өйткені бұзулардың шамамен 70% дұрыс орналастырылған аутентификация жүйесінің болмауына байланысты болады. Көп жағдайда көшуді бірден жасау мүмкін емес. Керісінше, бұл бірте-бірте, көп сатылы процесс (Zero Trust Networks: что это, зачем и как работает, 2022).

Желілік технологияның әлемдегі көшбасшысы ретінде Cisco компаниясы екенін бәрі біледі. Қауіпсіздік саясаты негізінде қол жеткізуге, пайдаланушыларды, құрылғыларды, жүйелерді және корпоративтік ортадағы басқа ресурстарды бақылауға, сондай-ақ оқиғаларды егжей-тегжейлі журналдауға, қауіптерді тиімді анықтау және оларға жауап беру процедурасын уақтылы бастау үшін олардың негізінде есептер мен ескертулер алуға мүмкіндік беретін Cisco Zero Trust моделін қарастырыңыз. Cisco Zero Trust-бұлттық инфрақұрылымда да, жергілікті жерде де орналастыруға болатын үш өнім жиынтығы: Cisco Duo қызметкерлер мен олардың құрылғыларын тіркелгі деректерін ұрлаудан, фишингтен және сәйкестендіру мәліметтерін пайдаланатын басқа да ұқсас шабуылдардан қорғауды қамтамасыз етеді. Корпоративтік қосымшаларға қол жеткізуді қамтамасыз етудің міндетті шарты сәйкестендіру рәсімінен өту болып табылады, нәтижесінде жүйе құрылғыларға сенім деңгейлерін тағайындайды. Cisco Secure Workload (Tetration) ақ тізімге негізделген нөлдік сенім үлгісін енгізу үшін микросегментацияға жауап береді; жұмыс жүктемесінің негізгі мінез-құлық көрсеткіштерін анықтайды және ауытқуларды алдын ала анықтайды; серверлерде орнатылған бағдарламалық жасақтама пакеттерінде жиі кездесетін және онымен байланысты осалдықтарды анықтайды; осалдықтарды анықтаған кезде бақыланатын түйіндерді карантинге қою және алмасуды блоктау арқылы проактивті қорғауды пайдаланады саясаттың бұзылуын анықтаған кезде деректермен қамтамасыз етеді; деректер орталығының жалпы қауіпсіздік жағдайы туралы тұтас түсінік береді. Cisco Software-Defined (SD) Access жұмыс ортасын қорғау үшін бағдарламалық жасақтамамен анықталған қол жетімділік моделін жүзеге асырады және кіруді басқарудың негізгі орны болып

табылады. Модельдің негізгі функциялары: автоматтандыру: құрылғыны жаңарту автоматты және жоспарланған болуы мүмкін. Аппараттық жабдықты түгендеуді қадағалау және жағдайды бақылау. Бүкіл сайтта роуминг. Әрбір виртуалды жергілікті желі әр платформа қосқышында белсенді болып, бұл аумақтық ағашының тұрақсыздығын болдырмайды. Пайдаланушылар мен құрылғыларды виртуалды жергілікті желілермен және ISE негізіндегі қауіпсіздік топтарымен сәйкестендіру. ISE тағайындаған топтарға негізделген әр сайттың ішіндегі пайдаланушылар мен құрылғыларды автоматты түрде сегменттеу, көптеген сайттар үшін біркелкі болып келеді. Пайдаланушылар мен құрылғылар топтарының ішінде және арасында трафикке арналған саясатты көрсетуге болады. Сегменттер (топтар) арасындағы және тіпті олардың ішіндегі трафикті басқару үшін SDA қосқыштары SGACL қолданады. Виртуалды желілер (VRF) мен SDA-дағы топтар мен деректер орталығының немесе желінің қалған бөлігі арасындағы топтық трафикті басқару саясатын мәжбүрлеп қолдану үшін біріктірілген брандмауэрлерді пайдалануға болады. SDA Transit технологиясының көмегімен VXLAN сегменттерін біріктірілген брандмауэрлердің бір немесе бірнеше жұбына оңай туннельдеуге болады. Қашықтықтан қол жеткізу пайдаланушыларына топтарды тағайындауды қолдау үшін AnyConnect пайдалануға болады. Коммутатор мен брандмауэрдің кіру тізімдері (ACL) IP мекенжайларының орнына пайдаланушы топтарын пайдалану арқылы ACL немесе sgacl қауіпсіздік/масштабталатын топ тізімдері болуы мүмкін.

Қазіргі уақытта Duo парольсіз аутентификациясы асимметриялық шифрлауға негізделген және биометрияны жергілікті жерде, құрылғыда, орталықтандырылған дерекқорсыз қауіпсіз сақтауға және тексеруге мүмкіндік беретін WebAuthn веб-аутентификация стандартын қолданады. Forcepoint компаниясының Private Access шешімі ZTNA моделін жүзеге асыратын dynamic Edge Protection SASE сервисінің құрамдас бөлігі болып табылады. Дегенмен, оны қашықтан жұмыс істеуді ұйымдастыру аясында қызметкерлерді қауіпсіз қосуды жүзеге асыру үшін дербес бұлттық қызмет ретінде пайдалануға болады. Private Access пайдаланушылардың корпоративтік ресурстарға қол жеткізуін басқарудың икемді моделін жүзеге асыруға мүмкіндік береді (мысалы, рұқсат етілмеген пайдаланушыларға кейбір ақпаратты көруге мүмкіндік беретін ережелерді конфигурациялауға болады) (Нөлдік сенімді желіге қол жеткізуді (Knowings, 2023).

Сонымен қатар қазіргі таңда бизнес Zero Trust моделін жүзеге асырса, ол бұрын қарастырмаған қауіптерді анықтай алады. Бұл оған деректер ағынынан, рұқсатсыз кіруден немесе ескірген бағдарламалық жасақтамадан туындайтынына қарамастан, тиісті қауіптерге жауап беруге көмектеседі. Zero Trust сонымен қатар деректердің бұзылуын болдырмауға және деректер ағындарын жақсы басқаруға көмектеседі. The GDPR ғасыры бұл әсіресе маңызды. Zero Trust ортасындағы қауіпсіздікті үздіксіз бақылау ағып кету немесе бұзылу белгілеріне дереу жауап беруге көмектеседі.

Қорытынды

Zero Trust – бұл осыны орнатып алып, босаңсуға болатын бағдарламалық өнім емес, жүйе емес екендігін баса көрсету керек. Бұл бар болғаны корпоративті желіні қорғау процестерін ұйымдастыруға қойылатын талаптардың жиынтығы ғана, бұл оны әртүрлі түсіндіру үшін еркіндік береді. Тұжырымдаманың мәнісі кез-келген құрылғының, оның ішінде өзінің орналасқан жерін өзгертетін құрылғының тексеру процедурасынан қайта өтуі керектігінде болып отыр. Ол желіні сегменттеуді жүргізуді, АТ-ресурстарды бақылау үшін мирокпериметрлерді құруды, аймақтар арасында мониторинг, басқару және өзара әрекеттестік жүйесін өрістетуді көздейді.

Біз қазіргі заманғы шындыққа дәстүрлі көзқарасты бейімдеу ретінде пайда болған нөлдік сенімді желіге қол жеткізу тұжырымдамасы өте перспективалы екенін көреміз. Zero Trust Network Access (ZTNA) қағидаттарын корпоративтік инфрақұрылымға енгізу бұлтты технологияларды дамыту және қашықтықтан жұмыс істеу жағдайында желілік периметрдің барған сайын "сырғанайтын" шекараларына қарамастан қауіпсіздіктің жоғары деңгейін сақтауға мүмкіндік береді. Ақпараттық қауіпсіздік саласындағы шешімдер мен сервистердің вендорлары нөлдік сенімділікпен желіге қол жеткізу моделіне деген қызығушылықтың артуына жауап беріп, оны іске асыратын өнімдерді шығарғаны қисынды. Осылайша, қазір әлемдік нарықта осындай шешімдердің көп саны ұсынылған. Бұл негізінен пайдаланушылар мен құрылғылардың корпоративтік ресурстарға қауіпсіз қол жеткізуін ұйымдастыратын бұлттық қызметтер.

Табысқа жету үшін қазіргі таңда қажетті басқа факторларға тоқталатын болсақ:

Сондай-ақ, қолданыстағы архитектураның ескірген компоненттеріне және айтарлықтай әсер ететін компоненттерге басымдық беру қажет. Тағы бір негізгі фактор-жан-жақты көрінуді қамтамасыз ету. Бұл аспект Zero Trust тұжырымдамасын жүзеге асырудың алғашқы жобаларында жиі ескерілмеді. Zero Trust моделінің барлық дерлік пайдаланушылары атап өткендей, сіз тек көргеніңізге сене аласыз.

Микросегментация бұл өте пайдалы әдіс, бірақ актерлердің жеке басын анықтайтын Zero trust компонентіне күшті қолдау болмаса, одан әрі микросегментация нөлдік сенімді тәсілдің қайтарымын төмендетеді, азайтады. Қазіргі таңда тәуекелді азайтудың маңызды стратегиясы ретінде көптеген ұйымдар үшін zero trust басымдылық болып табылады, бірақ аз ғана ұйымдар нөлдік сенімді іске асыруды аяқтап жатыр. Gartner, Inc. 2026 жылға қарай ірі кәсіпорындардың 10 %-ы жетілген және өлшенетін нөлдік сенім бағдарламасына ие болады, бұл бүгінгі күні 1 %-дан аз болып келеді.

ӘДЕБИЕТТЕР

Microsoft-тың IT-бөлімінің өзінің қызметкерлеріне қашықтан жұмыс істеуге мүмкіндік беретін 9 негізгі тәсілі. — *https://www.microsoft.com/en-us/microsoft-365/blog/2020/03/12/top-9-ways-microsoft-it-enabling-remote-work-employees/?elevate-wr*

Peter Rising, (2023). Microsoft 365 Security, Compliance, and Identity Administration: Plan and implement security and compliance strategies for Microsoft 365 and hybrid environments. — August 18,

Jason Garbis, Jerry W. Chapman (2021). «Zero Trust Security, An Enterprise Guide».

The CISO Guide to Zero Trust Security by Raj Badhwar. — February 7, 2022.

L.D. Knowings (2023). ZERO TRUST SECURITY DEMYSTIFIED: Expert Insights, Proven Strategies, and Real World Implementations for Digital Defense: Your Roadmap to a Resilient Network and Unparalleled Data Protection Paperback — December 9, — 2023.

Evan Gilman, Doug Barth, Zero Trust (2017). — Networks: Building Secure Systems in Untrusted Networks 1st Edition, — July 25, 2017, — 238 p.

Роуз С., Борхерт О., Митчелл С. и Коннелли С. (August 2020.). Архитектура нулевого доверия, Специальная публикация (NIST SP), Национальный институт стандартов и технологий, — Гейтерсбург, Мэриленд, [онлайн], — https://doi.org/10.6028/NIST.SP.800-207, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420

Нөлдік сеніммен сәйкестендіру қауіпсіздігі дегеніміз не? — *https://cloud.google.com/blog/topics/developers-practitioners/what-zero-trust-identity-security*

Нөлдік сенім желілері: бұл не, неге және қалай жұмыс істейді? — *https://habr.com/ru/company/zyxel/blog/651667/*

Нөлдік сенім үлгісі: принциптер мен артықшылықтар: — *https://techexpert.ua/ru/model-zero-trust/*

Нөлдік сенімді желіге қол жеткізуді (ZTNA)ұйымдастыруға арналған Әлемдік және ресейлік шешімдер нарығына шолу: — *https://www.anti-malware.ru/analytics/Market_Analysis/Russian-and-Global-ZTNA-market-overview#part62*

Өзекті киберқауіптер: 2020 жылдың III тоқсаны. — https://www.ptsecurity.com/ru-ru/research/analytics/

Zero Trust тұжырымдамасы: сенім білдіре берме — әрқашан тексеріп отыр. — https://blog.kaspersky.kz/zero-trust-security/22636/

Zero Trust деген не? Қауіпсіздік моделі. — https://habr.com/ru/company/varonis/blog/472934/

Zero Trust моделі: желілік периметрді әдеттегі қорғау енді жеткіліксіз. — https://www.anti-malware.ru/analytics/Technology_Analysis/Reviving-zero-trust-model

Zero Trust қауіпсіздік моделін Microsoft-қа енгізу. — https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft

Zero Trust тұжырымдамасы: сенбе, әрқашан тексер: — *https://blog.kaspersky.kz/zero-trust-security/22636/*

REFERENCES

Peter Rising, (2023). Microsoft 365 Security, Compliance, and Identity Administration: Plan and implement security and compliance strategies for Microsoft 365 and hybrid environments. — August 18,

Jason Garbis, Jerry W. Chapman (2021). «Zero Trust Security, An Enterprise Guide».

The CISO Guide to Zero Trust Security by Raj Badhwar. — February 7, — 2022.

L.D. Knowings (2023). ZERO TRUST SECURITY DEMYSTIFIED: Expert Insights, Proven Strategies, and Real World Implementations for Digital Defense: Your Roadmap to a Resilient Network and Unparalleled Data Protection Paperback — December 9, — 2023

Evan Gilman, Doug Barth (2017). — Zero Trust Networks: Building Secure Systems in Untrusted Networks 1st Edition, — July 25, — 2017, — 238 p.

Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, — 59 p. — August 2020. Zero Trust Architecture, — NIST Special Publication 800–207, National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology.

Concept of Zero Trust: never trust, always verify: — *https://blog.kaspersky.kz/zero-trust-security/22636/*

Introducing the Zero Trust security model to Microsoft. — https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft

Overview of the Global and Russian Solutions Market for Zero Trusted Network Access (ZTNA):

— https://www.anti-malware.ru/analytics/Market_Analysis/Russian-and-Global-ZTNA-market-overview#part62

Topical cyber threats: Q3 2020. — https://www.ptsecurity.com/ru-ru/research/analytics/

What is Zero Trust? Security model. — https://habr.com/ru/company/varonis/blog/472934/

What is zero-trust identity security? — https://cloud.google.com/blog/topics/developers-practitioners/what-zero-trust-identity-security

Zero Trust concept: don't trust — always verify. https://blog.kaspersky.kz/zero-trust-security/22636/

Zero Trust Model: Conventional network perimeter protection is no longer sufficient. — https://www.anti-malware.ru/analytics/Technology_Analysis/Reviving-zero-trust-model

Zero trust model: principles and advantages: — https://techexpert.ua/ru/model-zero-trust/

Zero Trust Networks: What, Why, and How Do They Work? — https://habr.com/ru/company/zyxel/blog/651667/

9 key ways Microsoft's IT department is enabling its employees to work remotely. — https://www.microsoft.com/en-us/microsoft-365/blog/2020/03/12/top-9-ways-microsoft-it-enabling-remote-work-employees/?elevate-wr

МАЗМҰНЫ

К.С. Алдажаров, С.К. Батырхан
АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ҚАЗІРГІ ЗАМАНҒЫ МОДЕЛІН ТАЛДАУ.....7
Ж.С. Алимова, Н.Н. Дюсенгазина, А.Т. Абенова, Г.С. Балгабаева, Л.З. Исабекова
ДЕРЕКТЕРДЕГІ АЙҚЫН ЕМЕС БАЙЛАНЫСТАРДЫ АНЫҚТАУДА В. ЛЕОНТЬЕВТІҢ ЕНГІЗУ-ШЫҒАРУ МОДЕЛІН ҚОЛДАНУ.....21
А.Х. Абишева, Б.Б. Ибраева, Н.Т. Телибаева, Д. Муса, К.Г. Балгинбаева
ГЕОИНФОРМАТИКА: ГЕОГРАФИЯ ЖӘНЕ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР СИНТЕЗІ.....32
А.С. Баегизова, А.Х. Касымова , А.М. Бисенгалиева, Б.О. Мухаметжанова, М.Ж. Базарова
МӘТІНДІК СИПАТТАМАЛАРҒА НЕГІЗДЕЛГЕН ГЕНЕРАТИВТІ ҚАРСЫЛАС ЖЕЛІЛЕРДІ ПАЙДАЛАНЫП КЕСКІНДЕРДІ ЖАСАУ.....43
А.Г. Батырханов, С.Р. Шармуханбет
ЛАТЫН ЖӘНЕ ҚАЗАҚ ЛАТЫН ӘЛІПБИІ.....59
Д.Г. Габдуллаев, И. Жансері, А.Б. Айдарбекова,Ш.Ж. Мусиралиева
ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІНІҢ НЕГІЗІНДЕ СУРЕТТЕРГЕ СТЕГОТАЛДАУ ЖАСАУ.....75
А.Х. Давлетова, Е.Т. Асан, А.Х. Касымова, А.Б. Медешова
БІЛІМ БЕРУДЕГІ ЖАСАНДЫ ИНТЕЛЛЕКТІ ҚОЛДАНУДЫҢ АРТЫҚШЫЛЫҚТАРЫ МЕН КЕМШІЛІКТЕРІ.....99
Б.А. Ерназарова, В.В. Стекольщиков, К.А. Айтбозова, С.Х. Сарамбетова, С.Д. Абжанов
ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ ОНЫ БІЛІМ БЕРУДЕ ҚОЛДАНУ.....110
Т. Жукабаева, Л. Жолшиева, А. Адамова, Е. Марденов, Н. Карабаев
СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕРГЕ ШАБУЫЛДАРДЫ АНЫҚТАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ: XGBOOST ЖӘНЕ SGD ТИІМДІЛІГІН ТАЛДАУ.....121
А.М. Джумагалиева, А.Ә. Шекербек, М.Г. Байбулова, А.И. Онгарбаева, А.К. Токкулиева
ЭЛЕКТРОНДЫҚ ДАУЫС БЕРУ ЖҮЙЕСІНЕ БЛОКЧЕЙН ТЕХНОЛОГИЯСЫН ЕНГІЗУДІ ТАЛДАУ.....136
А.А. Исмаилова, А.А. Нурпейсова, Ж.Т. Бельдеубаева, Г.О. Исакова, Н.Т. Исаева
ОФТАЛЬМОЛОГИЯДА ТОР ҚАБЫҚ ҚҰРЫЛЫМДАРЫН ТАЛДАУ ҮШІН ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ.....152
А.Е. Ибраимкулов, А.С. Еримбетова, Б. Сакенов
МӘТІНДІ ҚАЗАҚ ТІЛІНЕН ЫМДАУ ТІЛІНЕ КОМПЬЮТЕРЛІК АУДАРУ ЖҮЙЕСІН ӘЗІРЛЕУ МӘСЕЛЕЛЕРІ.....166
Г.Н. Кажатова, Ж.Т. Бельдеубаева, А.А. Исмаилова, А.А. Нурпейсова, Г.О. Исакова
КОРПОРАТИВТІК БІЛІМДІ БАСҚАРУДАҒЫ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР.....177
М.Ж. Қалдарова, А.С. Аканова, А.Е. Назырова, А.С. Муканова, Г.К. Муратова
MACHINE LEARNING КӨМЕГІМЕН ОРМАН ШАРУАШЫЛЫҒЫНЫҢ ШЕКАРАЛАРЫН АНЫҚТАУ.....192

А.Е. Кулакаева, Б.Ж. Медетов, А.З. Айтмагамбетов, А.Т. Жетписбаева, Н. Албанбай
ЖЕРСЕРІКТІК РАДИОБАҚЫЛАУ БАРЫСЫНДА КАЛМАН СҮЗГІШІ АРҚЫЛЫ СИГНАЛДЫ АНЫҚТАУ ӘДІСІНІҢ ТҰРАҚТЫЛЫҒЫН АНЫҚТАУ.....212
Ө.Ж. Мамырбаев, Д.О. Оралбекова, Ә.А. Айтқазина, С.М. Даулбаев, Н.Ө. Жұмажан
АУЫЛ ШАРУАШЫЛЫҒЫ СЕКТОРЫНДАҒЫ ЖЫЛУ ЭНЕРГИЯСЫН ЕСЕПТЕУ АРҚЫЛЫ ТЕМПЕРАТУРА БАЛАНСЫНЫҢ ДИНАМИКАСЫН ЗЕРТТЕУДІҢ ТЕРМОДИНАМИКАЛЫҚ МОДЕЛІ.....225
Т.М. Мұратов, М.А. Кантуреева, А.С. Омарбекова, А.Ж. Карипжанова, Ж.Ж. Кайсанова
ҚАЗАҚСТАНДАҒЫ АВИАЦИЯ САЛАСЫНДА ҚОЛДАНЫЛАТЫН IT ШЕШІМДЕРДІҢ ЕРЕКШЕЛІКТЕРІН ТАЛДАУ.....248
Ш.Ж. Мусиралиева, Қ. Багитова, К. Байсылбаева, М. Болатбек, Қ.Азанбай
ОНЛАЙН ӘЛЕУМЕТТІК ЖЕЛІЛЕРІ БЕЙНЕЛЕРІН ӨҢДЕУ АРҚЫЛЫ САЯСИ ЭКСТРЕМИЗМДІ АНЫҚТАУ МОДЕЛІ.....260
Г.С. Омарова, А.Н. Жәкіш, Ю.К. Жүсіпбек, А.А. Мырзамуратова, А.Б. Бексейтова
ДЕРЕКТЕР КӨЛЕМІН ҰЛҒАЙТУ ҮШІН ГЕНЕРАТИВТІ ҚАРСЫЛАС ЖЕЛІЛЕРДІ (GANS) ПАЙДАЛАНУ АРҚЫЛЫ ДЕРЕКТЕРДІ ГЕНЕРАЦИЯЛАУ.....283
С.К. Серикбаева, Г.А. Шангытбаева, А.Г. Батырханов, З.Д. Айдаралиева, К.А. Ибрагимова
ҒЫЛЫМИ-БІЛІМ БЕРУ ҚЫЗМЕТІ САЛАСЫНДАҒЫ ҚҰЖАТТАРҒА ҚОЛ ЖЕТКІЗУДІҢ ТҰЖЫРЫМДАМАСЫ МЕН ӘДІСТЕРІН ҚАЛЫПТАСТЫРУ.....297
М.А. Сексембаева
СТАТИКАЛЫҚ ТЫНУЫ БАР КӨП ЖОЛАҚТЫ АРНАЛАР АРҚЫЛЫ ШУҒА ТӨЗІМДІ КОДТАУЫ БАР ЦИФРЛЫҚ БАЙЛАНЫС ЖҮЙЕСІН МОДЕЛЬДЕУ.....317
А.Ж. Танирбергенов, Н.Ә. Жұматай, В.Е. Махатова, А.Т. Абдыхалық, Г.А. Шангытбаева
ЖОБАЛАРДЫ БАСҚАРУДАҒЫ КОММУНИКАЦИЯНЫҢ РӨЛІ: «ҰАТ» АҚ ТИІМДІЛІГІН АРТТЫРУ СТРАТЕГИЯЛАРЫ.....327
Б. Тасуов, Б.О. Шинибеков
ОРТА МЕКТЕПТЕ КОМПЬЮТЕРЛІК ГРАФИКАНЫ ОҚЫТУДА ШЫҒАРМАШЫЛЫҚ ЖӘНЕ ТЕХНИКАЛЫҚ ҚҰЗЫРЕТТІЛІКТЕРДІ ДАМЫТУ.....341
А.С. Тыныққұлова, А.А. Мұханова, М.К. Тыныққұлов, Р.С. Қуанышева, М.М. Иманғалиев
СОЛТҮСТІК ҚАЗАҚСТАН ОБЛЫСЫ АЙЫРТАУ АУДАНЫНЫҢ МЫСАЛЫНДА ЖЕР РЕСУРСТАРЫН ОҢТАЙЛЫ ПАЙДАЛАНУ ҮШІН АҚПАРАТТЫҚ ЖҮЙЕНІ ҚҰРУ АЛГОРИТМІ.....356
Ж.С. Такенова, А.А. Ташев
БІЛІМ БЕРУ ҰЙЫМДАРЫНДАҒЫ БАСҚАРУ МІНДЕТТЕРІН ШЕШУДІҢ ЖАҢА ТӘСІЛДЕРІ.....368

СОДЕРЖАНИЕ

К.С. Алдажаров, С.К. Батырхан
АНАЛИЗ СОВРЕМЕННОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....7
Ж.С. Алимова*, Н.Н. Дюсенгазина, А.Т. Абенова, Г.С. Балгабаева, Л.З. Исабекова
ПРИМЕНЕНИЕ МОДЕЛИ ВВОДА-ВЫВОДА В. ЛЕОНТЬЕВА ПРИ ОПРЕДЕЛЕНИИ НЕЯВНЫХ СВЯЗЕЙ В ДАННЫХ.....21
А.Х. Абишева, Б.Б. Ибраева, Н.Т. Телибаева, Д. Муса, К.Г. Балгинбаева
ГЕОИНФОРМАТИКА: СИНТЕЗ ГЕОГРАФИИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....32
А.С. Баегизова, А.Х. Касымова, А.М. Бисенгалиева, Б.О. Мухаметжанова, М.Ж. Базарова
ГЕНЕРАЦИЯ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ НА ОСНОВЕ ТЕКСТОВЫХ ОПИСАНИЙ.....43
А.Г. Батырханов, С.Р. Шармуханбет
О ЛАТЫНИ И КАЗАХСКОЙ ЛАТИНИЦЕ.....59
Д.Г. Габдуллаев, И. Жансери, А.Б. Айдарбекова, Ш.Ж. Мусиралиева
СТЕГОАНАЛИЗ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ.....75
А.Х. Давлетова, Е.Т. Асан, А.Х. Касымова, А.Б. Медешова
ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ.....99
Б.А. Ерназарова, В.В. Стекольщиков, К.А. Айтбозова , С.Х. Сарамбетова, С.Д. Абжанов
ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ.....110
Т. Жукабаева, Л. Жолшиева, А. Адамова, Е. Марденов, Н. Карабаев
ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АТАК В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ: АНАЛИЗ ЭФФЕКТИВНОСТИ XGBOOST И SGD.....121
А.М. Джумагалиева, А.А. Шекербек, М.Г. Байбулова, А.И. Онгарбаева, А.К. Токкулиева
АНАЛИЗ ВНЕДРЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В СИСТЕМУ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ.....136
А.А. Исмаилова, А.А. Нурпейсова, Ж.Т. Бельдеубаева, Г.О. Исакова, Н.Т. Исаева
ПРИМЕНЕНИЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА СТРУКТУР СЕТЧАТКИ В ОФТАЛЬМОЛОГИИ.....152
А.Е. Ибраимкулов, А.С. Еримбетова, Б. Сакенов
ПРОБЛЕМЫ РАЗРАБОТКИ СИСТЕМЫ КОМПЬЮТЕРНОГО ПЕРЕВОДА ТЕКСТА С КАЗАХСКОГО ЯЗЫКА НА ЖЕСТОВЫЙ ЯЗЫК.....166
Г.Н. Кажатова, Ж.Т. Бельдеубаева, А.А. Исмаилова, А.А. Нурпейсова, Г.О. Исакова
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ КОРПОРАТИВНЫМИ ЗНАНИЯМИ.....177
М.Ж. Калдарова, А.С. Аканова, А.Е. Назырова, А.С. Муканова, Г.К. Муратова
ОПРЕДЕЛЕНИЕ ГРАНИЦ ЛЕСНОГО ХОЗЯЙСТВА С ПОМОЩЬЮ MACHINE LEARNING.....192

А.Е. Кулакаева, Б.Ж. Медетов, А.З. Айтмагамбетов, А.Т. Жетписбаева, Н. Албанбай
ОПРЕДЕЛЕНИЕ УСТОЙЧИВОСТИ МЕТОДА ОБНАРУЖЕНИЯ СИГНАЛОВ С ПОМОЩЬЮ ФИЛЬТРА КАЛМАНА ПРИ СПУТНИКОВОМ РАДИОМНИТОРИНГЕ.....212
О.Ж. Мамырбаев, Д.О. Оралбекова, А.А. Айтказина, С.М. Даулбаев, Н.О. Жумажан
ТЕРМОДИНАМИЧЕСКАЯ МОДЕЛЬ ИЗУЧЕНИЯ ДИНАМИКИ ТЕМПЕРАТУРНОГО БАЛАНСА ПУТЕМ РАСЧЕТА ТЕПЛОВОЙ ЭНЕРГИИ В СЕЛЬСКОХОЗЯЙСТВЕННОМ СЕКТОРЕ.....225
Т.М. Муратов, М.А. Кантуреева, А.С. Омарбекова, А.Ж. Карипжанова, Ж.Ж. Кайсанова
АНАЛИЗ ОСОБЕННОСТЕЙ ИТ РЕШЕНИЙ В АВИАЦИОННОЙ СФЕРЕ КАЗАХСТАНА.....248
Ш.Ж. Мусиралиева, К. Багитова, К. Байсылбаева, М. Болатбек, К. Азанбай
МОДЕЛЬ ОБРАБОТКИ ИЗОБРАЖЕНИЙ ОНЛАЙН СОЦИАЛЬНЫХ СЕТЕЙ, ИСПОЛЬЗУЕМЫХ ДЛЯ РАСПОЗНАВАНИЯ ПОЛИТИЧЕСКОГО ЭКСТРЕМИЗМА.....260
Г.С. Омарова, А.Н. Жакиш, Б.К. Жусипбек, А.А. Мырзамуратова, А.Б. Бексейтова
ГЕНЕРАЦИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ (ГАНС) ДЛЯ УВЕЛИЧЕНИЯ ДАННЫХ.....283
С.К. Серикбаева, Г.А. Шангытбаева, А.Г. Батырханов, З.Д. Айдаралиева, К.А. Ибрагимова
ФОРМИРОВАНИЕ КОНЦЕПЦИИ И МЕТОДОВ ДОСТУПА К ДОКУМЕНТАМ В СФЕРЕ НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ.....297
М.А. Сексембаева
МОДЕЛИРОВАНИЕ СИСТЕМЫ ЦИФРОВОЙ СВЯЗИ С ПОМЕХОУСТОЙЧИВЫМ КОДИРОВАНИЕМ ПО МНОГОЛУЧЕВЫМ КАНАЛАМ СО СТАТИЧЕСКИМ ЗАМИРАНИЕМ.....317
А.Ж. Танирбергенов, Н.А. Жуматай, В.Е. Махатова, А.Т. Абдыхалык, Г.А. Шангытбаева
РОЛЬ КОММУНИКАЦИИ В УПРАВЛЕНИИ ПРОЕКТАМИ: СТРАТЕГИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ В АО «НИТ».....327
Б. Тасуов, Б.О. Шинибеков
РАЗВИТИЕ ТВОРЧЕСКИХ И ТЕХНИЧЕСКИХ КОМПЕТЕНЦИЙ В ОБУЧЕНИИ КОМПЬЮТЕРНОЙ ГРАФИКЕ В СРЕДНЕЙ ШКОЛЕ.....341
А.С. Тыныкулова, А.А. Муханова, М.К. Тыныкулов, Р.С. Куанышева, М.М. Имангалиев
АЛГОРИТМ СОЗДАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ОПТИМАЛЬНОГО ИСПОЛЬЗОВАНИЯ ЗЕМЕЛЬНЫХ РЕСУРСОВ НА ПРИМЕРЕ АЙЫРТАУСКОГО РАЙОНА СЕВЕРО-КАЗАХСТАНСКОЙ ОБЛАСТИ.....356
Ж.С. Такенова, А.А. Ташев
НОВЫЕ ПОДХОДЫ В РЕШЕНИИ УПРАВЛЕНЧЕСКИХ ЗАДАЧ В ОРГАНИЗАЦИЯХ ОБРАЗОВАНИЯ.....368

CONTENTS

K.S. Aldazharov, S.K. Batyrkhan
ANALYSIS OF THE MODERN MODEL OF INFORMATION SECURITY.....7
Z. Alimova, N. Dyussengazina, A. Abenova, G. Balgabayeva, L. Issabekova
APPLICATION OF THE I / O MODEL OF V. LEONTIEV IN IDENTIFYING IMPLICIT CONNECTIONS IN DATA.....21
A.H. Abisheva, B.B. Ibraeva, N.T. Telibaeva, D. Musa, K.G. Balginbayeva
GEOINFORMATICS: SYNTHESIS OF GEOGRAPHY AND INFORMATION TECHNOLOGIES.....32
A.S. Baegizova, A.K. Kassymova, A.M. Bissengaliyeva, B.O. Mukhametzhanova, M.Zh. Bazarova
GENERATING IMAGES USING GENERATIVE ADVERSARIAL NETWORKS BASED ON TEXT DESCRIPTIONS.....43
A. Batyrkhanov, S. Sharmukhanbet
ABOUT LATIN AND KAZAKH LATIN.....59
D. Gabdullaev, I. Zhanseri, A. Aidarbekova, Sh. Mussiraliyeva
IMAGE STEGO ANALYSIS BASED ON DEEP LEARNING METHODS.....75
A.Kh. Davletova, Y.T. Assan, A.K. Kassymova, A.B. Medeshova
ADVANTAGES AND DISADVANTAGES OF USING ARTIFICIAL INTELLIGENCE IN EDUCATION.....99
B.A. Yernazarova, V.V. Stekolchshikov, K.A. Aitbozova, S.KH. Sarambetova, S.D. Abzhanov
ARTIFICIAL INTELLIGENCE AND ITS APPLICATION IN EDUCATION.....110
T. Zhukabayeva, L. Zholshiyeva, A. Adamova, Y. Mardenov, N. Karabayev
APPLICATION OF MACHINE LEARNING METHODS FOR ATTACK DETECTION IN WIRELESS SENSOR NETWORKS: PERFORMANCE ANALYSIS OF XGBOOST AND SGD.....121
A.M. Jumagaliyeva, A.A. Shekerbek, M.G. Baibulova, A.I. Ongarbayeva, A. Tokkuliyeva
ANALYSIS OF IMPLEMENTATION BLOCKCHAIN TECHNOLOGY TO ELECTRONIC VOTING SYSTEM.....136
A.A. Ismailova, A.A. Nurpeisova, Zh.T. Beldeubayeva, G.O. Issakova, I. Issayeva
APPLICATION OF DEEP LEARNING METHODS FOR ANALYSIS OF RETINAL STRUCTURES IN OPHTHALMOLOGY.....152
A.Ye. Ibraimkulov, A.S. Yerimbetova, B. Sakenov
PROBLEMS OF DEVELOPING A SYSTEM FOR COMPUTER TRANSLATION OF TEXT FROM KAZAKH INTO SIGN LANGUAGE.....166
G. Kazhatova, Zh. Beldeubayeva, A. Ismailova , A. Nurpeisova, G. Issakova
INFORMATION TECHNOLOGY IN CORPORATE KNOWLEDGE MANAGEMENT.....177
M.Zh. Kaldarova, A.S. Akanova, A.E. Nazyrova, A.S. Mukanova, G.K. Muratova
DETERMINING FORESTRY BOUNDARIES USING MACHINE LEARNING.....192
A.E. Kulakayeva, B.Zh. Medetov, A.Z. Aitmagambetov, A.T. Zhetpisbayeva, N. Albanbay
DETERMINATION OF THE STABILITY OF THE SIGNAL DETECTION METHOD USING THE KALMAN FILTER IN SATELLITE RADIO MONITORING.....212

O.Zh. Mamyrbayev, D.O. Oralbekova, A.A. Aitkazina, S.M. Daulbayev, N.O. Zhumazhan
THERMODYNAMIC MODEL FOR STUDYING THE DYNAMICS OF TEMPERATURE BALANCE BY CALCULATING THERMAL ENERGY IN THE AGRICULTURAL SECTOR.....225
T. Muratov, M. Kantureeva, A. Omarbekova, A. Karipzhanova, Zh. Kaisanova
ANALYSIS OF FEATURES IT SOLUTIONS IN THE AVIATION SECTOR OF KAZAKHSTAN.....248
Sh. Mussiraliyeva, K. Bagitova, K. Baisylbaeva, M. Bolatbek, K. Azanbai
MODEL FOR PROCESSING IMAGES OF ONLINE SOCIAL NETWORKS USED TO RECOGNIZE POLITICAL EXTREMISM.....260
G.S. Omarova, A.N. Zhakish, B.K. Zhussipbek, A.A. Myrzamuratova, A.B. Bekseitova
DATA GENERATION USING GENERATIVE-ADVERSARIAL NETWORKS . (GANS) TO INCREASE THE DATA.....283
S. Serikbayeva, G. Shangytbayeva, A. Batyrkhanov, Z. Aidaraliyeva, K. Ibragimova
FORMATION OF THE CONCEPT AND METHODS FOR ACCESSING DOCUMENTS IN THE FIELD OF SCIENTIFIC AND EDUCATIONAL ACTIVITIES.....297
M.A. Seksembayeva
MODELING OF A DIGITAL COMMUNICATION SYSTEM WITH NOISE-RESISTANT CODING OVER MULTIPATH CHANNELS WITH STATIC FADING.....317
A. Tanirbergenov, N. Zhumatayn, V. Makhatova, A. Abdykhalyk, G. Shangytbayeva
THE ROLE OF COMMUNICATION IN PROJECT MANAGEMENT: STRATEGIES FOR IMPROVING EFFICIENCY IN JSC «NIT».....327
B. Tassuov, B. Shinibekov
DEVELOPMENT OF CREATIVE AND TECHNICAL COMPETENCIES IN TEACHING COMPUTER GRAPHICS IN SECONDARY SCHOOL.....341
A.S. Tynykulova, A.A. Mukhanova, M.K. Tynykulov, R.S. Kuanysheva, M.M. Imangaliyev
ALGORITHM FOR CREATION OF AN INFORMATION SYSTEM FOR OPTIMAL USE OF LAND RESOURCES ON THE EXAMPLE OF AYYRTAU DISTRICT OF NORTH KAZAKHSTAN REGION.....356
Zh. Takenova, A. Tashev
NEW APPROACHES IN SOLVING PROBLEMS OF MANAGEMENT IN EDUCATIONAL ORGANIZATIONS.....368

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Подписано в печать 28.03.2024.
Формат 60x881/8. Бумага офсетная. Печать–ризограф.
21,0 п.л. Тираж 300. Заказ 1.

РОО «Национальная академия наук РК» 050010,
Алматы, ул. Шевченко, 28, т. 272-13-19