ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

горизонты для исследований и разработки в области математики, криптографии и вычислительной техники. Мы ожидаем, что наше исследование внесет значительный вклад в научное сообщество и стимулирует дальнейшие работы в этом направлении. Анализ данных и их визуализация являются ключевыми аспектами данного исследования, позволяя не только подтвердить теоретические предположения, но и наглядно продемонстрировать возможности предложенного метода.

Список использованных источников

1. Lenstra, A. K., Lenstra, H. W., Manasse, M. S., & Pollard, J. M. (1990). The number field sieve. Proceedings of the twenty-second annual ACM symposium on Theory of computing, 564-572.
2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th annual symposium on foundations of computer science, 124-134.
3. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

УДК 004.056.5

ФИШИНГТІК ВЕБ-САЙТТЫ АНЫҚТАУ ӘДІСТЕРІНЕ ЖҮЙЕЛІ ӘДЕБИЕТТІК ШОЛУ

Елеуов Батырхан Назымбекович
batyrkhan0808@gmail.com
Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 1-курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – т. ғ. к., «Ақпараттық қауіпсіздік» кафедрасының доценті, К.М.Сагиндыков

Аннотация

Фишинг - бұл шабуылдаушы пайдаланушыдан құпия ақпарат алу үшін сенімді тұлға немесе ұйым ретінде өзін-өзі көрсететін алаяқтық әрекет. Бұл жүйелі әдебиеттерді зерттеу фишингті анықтаудың әртүрлі әдістерін, соның ішінде Тізімдерге Негізделген (Lists Based), Визуалды Ұқсастық (Visual Similarity), Эвристикалық, Машиналық Оқыту (Machine Learning) және Терең Оқыту (Deep Learning) әдістерін, олардың тиімділігін талдауды және салыстыруды зерттейді. Мақалада фишингтік веб-сайттар үшін көптеген алгоритмдері, деректер жиындары және анықтау әдістері мұқият зерттелді, сәйкесінше зерттеу сұрақтары жасалынды. Соңғы бес жыл ішінде ғылыми журналдарда, конференцияларда, семинарларда, зерттеушілердің тезистерінде, кітап тарауларында және беделді веб-сайттарда жарияланған 40 ғылыми мақалаларға жан-жақты шолу жасалды. Бұл зерттеу фишингті анықтау әдістемелерінің заманауи тенденцияларына баса назар аудара отырып, әдебиеттерге алдыңғы жүйелі шолуларға негізделген, оқырмандардың әртүрлі анықтау әдістері, деректер жиынын пайдалану және алгоритмдік өнімділікті салыстыру туралы түсінігін байытады. Айта кететін жайт, Машиналық Оқыту әдістері басым: зерттеу нәтижелеріне сәйкес, олар 28 зерттеуде қолданылған. Соның ішінде 15 зерттеуде Random Forest Classifier қолданылды. Айта кететін жайт, Convolutional Neural Network (CNN) фишингтік веб-сайттарды анықтауға арналған әртүрлі зерттеулерде ең жоғары дәлдікке қол жеткізді - 99,98%.

Кілт сөздер

Фишинг, Фишингті Анықтау, Киберқауіпсіздік, Машиналық Оқыту

1. Кіріспе

Фишинг, әлеуметтік инженерлік шабуыл, киберқылмыскерлер интернет пайдаланушысының жеке деректерін, соның ішінде банктік картасының деректерін, пайдаланушы аттары мен құпия сөздерді заңсыз алу үшін қолданатын негізгі әдіс ретінде кеңінен танылды. Кейде фишингтік шабуылдар зиянды бағдарламаларды желі ішінде тарату құралы ретінде қызмет етеді. Бұл шабуылдар әртүрлі формаларда көрінеді, соның ішінде

спуфинг, зиянды бағдарламаларға негізделген фишинг, DNS негізіндегі фишинг, деректерді ұрлау, электрондық пошта/спам, веб-жеткізу және телефон фишингі. Қылмыскерлер электрондық пошта, жедел хабар алмасу, QR кодтары және әлеуметтік медиа платформалары сияқты әртүрлі байланыс арналарын пайдаланады. Олар көбінесе пайдаланушыларды алаяқтық веб-сайттардағы құпия ақпаратты ашуға алдау үшін банктер немесе электрондық коммерция веб-сайттары сияқты беделді ұйымдардың кейпіне енеді. Мысалы, пайдаланушы өзінің банктік шотына қатысты шұғыл хабарлама ала алады, бұл оны жалған веб-сайтқа апарады, онда ол өзінің тіркелгі деректерін байқаусызда енгізеді, бұл шабуылдаушыларға олардың заңды шоттарын ұрлауға мүмкіндік береді. Осы қауіпке жауап ретінде зерттеулерде әртүрлі әдістер, соның ішінде Тізімдерге Негізделген, Визуалды Ұқсастық, Эвристикалық, Машиналық Оқыту және Терең Оқыту әдістері ұсынылды.

Тізімге Негізделген: Microsoft Edge, Firefox және Google Chrome сияқты Браузерлер фишингтік веб-сайттарды анықтау үшін Тізімге Негізделген әдістерді пайдаланады. Бұл әдістер ақ тізімге және қара тізімге енгізуді қамтиды. Ақ тізімдер браузерлер кіре алатын бекітілген URL мекенжайларынан тұрады, егер URL мекенжайы сәйкес келсе, веб-беттерді жүктеуге рұқсат береді. Керісінше, қара тізімдерде фишингке немесе алаяқтық әрекеттерге қатысты URL мекенжайлары бар, бұл браузерлердің осы веб-беттерге кіруіне жол бермейді. Дегенмен, Тізімге Негізделген тәсілдер URL мекенжайын шамалы өзгертуге осал болып табылады, бұл фишингтің жаңа әрекеттерімен күресу үшін жиі жаңартуларды қажет етеді.

Визуалды Ұқсастық: Бұл әдіс веб-сайттарды күдікті және күдіксіз деп ажырату үшін визуалды белгілер негізінде орындалады. Мәтін орналасуы, бастапқы код, логотиптер және скриншоттар сияқты визуалды атрибуттарды салыстыра отырып, бұл құралдар фишинг пен шынайы веб-беттер арасындағы ұқсастықтарды анықтайды. Алайда, ол бұрын кездескен сайттармен салыстыруға негізделгендіктен, Визуалды Ұқсастық әдістері нөлдік-сағаттық фишингтік шабуылдарға қарсы тиімсіз.

Эвристикалық: Эвристикалық тәсіл фишингтік веб-сайттарды осындай сайттарға тән ерекшеліктерді талдау арқылы ажыратады. Ол URL мекенжайлары, мәтіндік мазмұн, DNS ақпараты, сандық сертификаттар және веб-сайт трафигінің үлгілері сияқты атрибуттарды пайдаланады. Эвристикалық әдістер нөлдік сағаттық фишингтік шабуылдарды анықтауға қабілетті, бұл басқа әдістерге қарағанда артықшылық береді.

Машиналық Оқыту: Машиналық Оқыту фишингті анықтаудың көрнекті әдісі ретінде пайда болды. Ол фишингтік URL мекенжайларын және қатысты сайттарды сипаттау үшін URL деректері, веб-сайт құрылымдары және JavaScript мүмкіндіктері сияқты атрибуттарды жинауды қамтиды. Содан кейін фишингтік веб-сайттарды анықтау үшін машиналық оқыту классификаторлары осы мүмкіндіктер бойынша, әсіресе үлкен деректер жиынтығымен тиімді оқытылады. 99% - дан астам дәлдікке қол жеткізе отырып, Машиналық Оқыту классификаторлары осы салада жоғары тиімділікпен ерекшеленеді.

Терең Оқыту: Терең Оқытудағы соңғы жетістіктер Deep Neural Networks фишингті анықтау үшін Машиналық Оқытудың дәстүрлі әдістерінен асып түсетінін көрсетеді. Терең Оқытудың көрнекті алгоритмдеріне Deep Neural Networks, Recurrent Neural Networks, Feed-Forward Deep Neural Networks, Шектеулі Больцман машиналары, Convolutional Neural Networks, терең сенімді желілері және терең автоматты кодерлер жатады.

Бұл зерттеу жұмысының екі негізгі мақсаты бар:

1. Фишингтік веб-сайттарды анықтаудың ең тиімді әдістерін анықтау және фишингтік шабуылдардан қорғау жүйелерін нығайтудың оңтайлы тәсілдерін көрсету.

2. Осы саладағы ғалымдар қолданатын әдістерге, мәліметтер жиынтығына және алгоритмдерге бағытталған жан-жақты шолу мақаласын ұсыну.

2. Ілеспе жұмыстың негізі

Көптеген авторлар фишингтік сайттарды анықтауды зерттеді. Алайда, төменде сипатталғандай, тақырып бойынша әдебиеттерге жүйелі шолу жасағандар аз.

Бенавидес (2020) Терең Оқыту алгоритмдерін қолдану арқылы фишингтік шабуылдарды анықтау үшін зерттеушілер қолданатын әртүрлі тәсілдерді талдауға

бағытталған жүйелі шолу жүргізді. Олардың нәтижелері фишингтік шабуылдарды анықтау үшін Терең Оқыту алгоритмдері саласындағы айтарлықтай алшақтықты көрсетеді. Шолу 2014-2019 жылдар аралығында жарияланған 19 зерттеуді ғана қамтитын шектеулі әдебиеттерді қамтиды. Мақалада фишинг пен Терең Оқытудың негізгі тақырыптарына арналған зерттеу мақалалары ғана қарастырылған [1].

Аршад (2021) өз зерттеулерінде фишингтің әртүрлі түрлеріне және фишингке қарсы әдістерге сараптама жүргізді. Олардың Әдебиеттерге Жүйелі Шолуы телефон фишингін, email spoofing, spear phishing және электрондық поштаны манипуляциялауды жиі қолданылатын фишинг тактикасы ретінде анықтады. Зерттеу Машиналық Оқыту тәсілдері фишингті анықтауда ең жоғары дәлдікті қамтамасыз ететінін хабарлады. Дегенмен, бұл зерттеу тек 20 мақалаға сүйенуімен шектелетінін ескеру маңызды [2].

Катал (2022) тоғыз зерттеу сұрағын шешуге бағытталған әдебиеттерге жүйелі шолу жүргізді. Олардың негізгі мақсаты фишингті анықтау үшін терең оқыту тәсілдеріне қатысты нәтижелерді анықтау, бағалау және бекіту болды. Олардың зерттеуіне сәйкес, бақыланатын машиналық оқыту алгоритмдері қарастырылған 43 зерттеудің 42-сінде қолданылған. Ең көп таралған алгоритм Deep Neural Network (DNN) болды, оның ең жақсы көрсеткіштері DNN және Hybrid Deep Learning алгоритмдерінде байқалды. Бұл жұмыс тек фишингті анықтау үшін терең оқыту әдістеріне қатысты зерттеулерге бағытталған [3].

3. Әдістеме

Мақалада сипатталған әдебиеттерге жүйелі шолу Китченхэм (2010) сипаттаған нақты анықталған зерттеу процесіне сәйкес келеді. Әдістеме бірнеше негізгі кезеңдерді қамтиды, соның ішінде зерттеу сұрақтарын тұжырымдау, барлау үшін электрондық дерекқорларды анықтау, деректерді жинау, жиналған деректерді талдау, қорытындыларды талқылау және алып тастау критерийлерін қолданғаннан кейін соңғы таңдалған зерттеу мақалаларын салыстырмалы түрде зерттеу. Бұл жүйелі әдебиеттерді шолудың негізгі мақсаты зерттеушілер фишингтік веб-сайттарды анықтау үшін пайдаланатын ең тиімді тәсілді, деректер жинағын және алгоритмді анықтау болып табылады [4].

3.1. Зерттеу сұрақтары

Тиісті ізденістерден кейін тұжырымдалған зерттеу сұрақтары анықталған және төменде көрсетілген. Бұл талқылаулардың негізгі мақсаты фишингтің әртүрлі әдістемелерін түсіндіру, тиісті зерттеулерде қолданылатын деректер жиынын анықтау, осы салада кең таралған алгоритмдерді анықтау және осы алгоритмдер қол жеткізген дәлдіктің ең жоғары деңгейін анықтау болып табылады.

1. Фишингтік веб-сайтты анықтау әдістері қандай және көптеген зерттеулерде қандай әдіс қолданылған?

2. Авторлар қандай алгоритмдерді қолданды және негізінен зерттеуші қандай алгоритмді қолданды?

3. Фишингтік шабуылдарды анықтауға келгенде қай алгоритм ең жақсы дәлдікке ие?

3.2. Тиісті дерекқорлар

Кешенді жүйелі шолуды қамтамасыз ету үшін арнайы кілт сөздер негізінде тиісті нәтижелерді тиімді қамтамасыз ете алатын сәйкес дерекқорларды таңдау өте маңызды. Бұл зерттеуде келесі үш дерекқор анықталды:

1. IEEE Explore.

2. Elsevier.

3. Springer.

3.3. Инклюзивті критерийлер

Инклюзивтілікті қарастыру критерийлері маңызды емес құжаттарды біртіндеп сүзу үшін үш түрлі деңгейде қолданылды. Бастапқыда ізденіс ақпараттық жүйелер және ақпараттық қауіпсіздік бағытында атқарылды. Кейіннен, "Машиналық Оқытудың" пәнаралық екенін мойындай отырып, сол бағыттағы мақалалар да бастапқы тізімге енгізілді.

Жүйелі шолу үш түрлі деңгейден өтті, оның соңы зерттеу жұмыстарының соңғы жиынтығын анықтаумен аяқталды. Бастапқыда барлығы 62 мақала жиналды. Инклюзивті

критерийлерін қолданғаннан кейін 49 ізденіс жұмыстары қаралды. Кейіннен кілт сөздердің өзектілігі мен ізденіс жұмысының мазмұнының талдануы негізінде 40 мақала алынды.

4. Фишингтік веб-сайтты анықтау тәсілдері

Фишингтік шабуылдарды анықтау және алдын алу үшін фишингке қарсы әртүрлі әдістер бар.

Келесі бөлімде фишингтік веб-сайттарды анықтау әдістеріне негізделген әдебиеттер талқыланады.

4.1. Эвристикалық әдіс

Эвристикалық әдіс фишингтік веб-сайттардан алынған ерекшеліктер негізінде күдікті және күдікті емес сайттарды ажырату үшін пайдаланады. Бұл ерекшеліктер URL мекенжайында "@" белгісінің болуы, қалқымалы терезелер арқылы құпия сөз сұраулары және домен бөлігіндегі IP мекенжайлары сияқты күдікті көрсеткіштерді анықтауға көмектеседі.

Гупта (2021) жүргізген зерттеу ерекше көзге түседі, онда олар Random Forest классификаторын қолданып, 99,57% әсерлі дәлдікке қол жеткізді. Бұл эвристикалық тәсілдерді қолданатын барлық мақалалар арасындағы дәлдіктің ең жоғары деңгейін білдіреді [5].

4.2. Визуалды Ұқсастыққа негізделген әдіс

Бұл әдісте веб-беттерді салыстыру беттердегі мазмұн мен визуалды элементтердің ұқсастығына сүйенеді. Бұл тәсілде мәтіндік мазмұн, форматтау, бастапқы код, скриншоттар, логотиптер, кескіндер және басқа визуалды элементтер сияқты әртүрлі факторлар қарастырылады.

Хидаят (2021) жүргізген зерттеу Fuzzy set әдісін қолдана отырып, 99,77% әсерлі дәлдікке қол жеткізе отырып, ерекшеленеді. Бұл Визуалды Ұқсастық тәсілдерін қолданатын барлық мақалалар арасындағы ең жоғары дәлдікті білдіреді [6].

4.3. Тізімге Негізделген әдіс

Microsoft Edge, Firefox және Google Chrome сияқты браузерлер фишингтік веб-сайттарды анықтау үшін тізімге негізделген әдістерді пайдаланады. Қара тізімге спам деп жарияланған веб-сайттардың тізімі кіреді, ал ақ тізімге браузерлер кіре алатын веб-беттер кіреді.

Тізімге негізделген әдістердің ішінде, Барраклоу (2021) бөлшектер алгоритмін қолдану арқылы 99,33% дәлдікке қол жеткізді. Бұл тізімге негізделген тәсілдерді қолданатын басқа мақалалар арасындағы ең жоғары дәлдік [7].

4.4. Машиналық Оқыту әдістері

Бұл әдіс ерекшеліктерді шығаруды және жіктеу мақсатында машиналық оқыту алгоритмдерін қолдануды қамтиды. URL ақпараты, веб-сайт құрылымы және JavaScript мүмкіндіктері сияқты атрибуттар әдетте фишингтік URL мекенжайларын және қатысты веб-сайттарды көрсету үшін жиналады. Кейіннен осы мүмкіндіктер негізінде фишингтік деректер жиынтығы алынады және машиналық оқыту классификаторлары алынған мүмкіндіктерді пайдалана отырып, фишингтік веб-сайттарды анықтауға үйретіледі.

Стоббс (2020) Random Forest алгоритмін қолдану арқылы 99,33% әсерлі дәлдікке қол жеткізілді, Бұл машиналық оқыту тәсілдерін қолданатын барлық мақалалар арасында ең жоғары дәлдікті көрсетті [8].

4.5. Терең Оқыту әдісі

Терең Оқыту әдістемелеріндегі соңғы жетістіктерге сәйкес, Deep Neural Networks (DNN) фишингтік веб-сайттарды анықтауда дәстүрлі машиналық оқыту әдістемелерінен асып түседі деп күтілуде.

Вэй (2020) жүргізген зерттеу Convolutional Neural Network (CNN) 99,98% ерекше дәлдігі туралы хабарлады, келтірілген барлық зерттеулердің ең жоғары дәлдігі болып табылады [9].

5. Нәтижелер

Әдебиеттерге жүйелі шолу нәтижелері зерттеу сұрақтарына сәйкес орындалған. Бастапқыдағы, 62 фишингтік шабуылдарға қатысты зерттеулерден тек 40 мақала ары қарай

зерттелу үшін анықталды. Осы 40 жарияланымның ішінде қазіргі әдебиеттердің 43% - құрайтын 17 мақала IEEE журналдарынан алынды, ал 13 (31%) Springer, 10 (26%) Elsevier журналдарынан алынды. Бұл сандар IEEE-дің фишингтік шабуылдар тақырыбындағы зерттеулерді жариялаудағы маңыздылығын көрсетеді.

5.1. Зерттеу сұрақтарын талқылау

Фишингтік веб-сайтты анықтау әдістері қандай және көптеген зерттеулерде қандай әдіс қолданылған?

Әдебиеттерді жүйелі шолу шеңберінде фишингке қарсы негізгі тәсілдерді бес негізгі бағытқа бөлуге болатындығы анықталды: Тізімге негізделген, Визуалды ұқсастыққа негізделген, Эвристикалық, Машиналық оқыту және Терең оқыту. Ғылыми қауымдастық осы әдістердің әрқайсысы бойынша әртүрлі зерттеулер жүргізді.

Авторлар қандай алгоритмдерді қолданды және негізінен зерттеуші қандай алгоритмді қолданды?

Зерттеу көрсеткендей, зерттеушілер фишингтік сайттарды анықтау үшін бірнеше алгоритмді пайдаланады. Random Forest Classifier 40 зерттеудің 15-інде қолданылды, бұл осы зерттеуге енгізілген жұмыстардың 38,75% құрайды. Support Vector Machines екінші орында, ал Decision Tree үшінші орында, сәйкесінше 36,25% және 27,5% құрайды. CNN ең жоғары дәлдікті сақтайды - 99,98%.

Фишингтік шабуылдарды анықтауға келгенде қай алгоритм ең жақсы дәлдікке ие?

Convolutional Neural Network (CNN) әдістерінің эволюциясы фишингтік шабуылдарды анықтауды қоса алғанда, әртүрлі болжау талдауларында дәстүрлі машиналық оқыту алгоритмдерімен салыстырғанда жоғары дәлдікке әкелді. Бұл артықшылық Вэй (2020) зерттеуінде айқын көрінеді. онда CNN 99,98% әсерлі дәлдікке қол жеткізді, бұл зерттелген барлық басқа әдістер арасындағы ең жоғары көрсеткіш.

Қорытынды

Зерттеу соңғы бес жылдағы фишингтік веб-сайттарды анықтау әдістерінің тиімділігін талдай отырып, әдебиеттерге жүйелі зерттеу жүргізді. Бастапқыда үш электронды кітапханада барлығы 62 зерттеу нысаны зерттелді. Инклюзионды критерийлерін қолданғаннан кейін мақалалар саны 49-ға дейін қысқарды, одан әрі сараптау арқылы 40 зерттеуге дейін қысқарды.

Бұл 40 мақала зерттеу бағытын сәйкестендіру үшін алдын ала анықталған зерттеу сұрақтарына негізделген мұқият тексеруден өтті. Нәтижелер бірнеше негізгі сұрақтарды қарастырады:

Зерттеу фишингті анықтаудың бес негізгі әдісін анықтады, ең көп қолданылатын машиналық оқыту тәсілдері таңдалған зерттеулердің 71,25% құрайды.

Random Forest классификаторы мақалалардың 38,75% - ында көрсетілген ең жиі қолданылатын алгоритм ретінде пайда болды. Танымалдылығына қарамастан, зерттеу Convolutional Neural Network (CNN) дамуымен оның дәлдігі дәстүрлі машиналық оқыту алгоритмдерінен асып түсетінін атап өтті. Атап айтқанда, CNN деректер жиынтығына немесе болжамды талдау үшін алынған мүмкіндіктерге қарамастан зерттеуге енгізілген барлық зерттеулердің ең жоғары дәлдігіне 99,98% қол жеткізді.

Қолданылған әдебиеттер тізімі

1. Benavides E. et al. Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review //Developments and Advances in Defense and Security: Proceedings of MICRADS 2019. – 2020. – С. 51-64.
2. Arshad A. et al. A systematic literature review on phishing and anti-phishing techniques //arXiv preprint arXiv:2104.01255. – 2021.
3. Catal C. et al. Applications of deep learning for phishing detection: a systematic literature review //Knowledge and Information Systems. – 2022. – Т. 64. – №. 6. – С. 1457-1500.
4. Kitchenham B. et al. Systematic literature reviews in software engineering–a tertiary study //Information and software technology. – 2010. – Т. 52. – №. 8. – С. 792-805.

5. Gupta B. B. et al. A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment //Computer Communications. – 2021. – Т. 175. – С. 47-57.

6. Hidayat R. et al. Similarity measure fuzzy soft set for phishing detection //International Journal of Advances in Intelligent Informatics. – 2021. – Т. 7. – №. 1. – С. 101-111.

7. Barraclough P. A., Fehringer G., Woodward J. Intelligent cyber-phishing detection for online //computers & security. – 2021. – Т. 104. – С. 102123.

8. Stobbs J., Issac B., Jacob S. M. Phishing web page detection using optimised machine learning //2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). – IEEE, 2020. – С. 483-490.

Wei W. et al. Accurate and fast URL phishing detector: a convolutional neural network approach //Computer Networks. – 2020. – Т. 178. – С. 107275.

ИНТЕРНЕТ ЗАТТАРЫ (IOT) ЖЕЛІСІНДЕГІ ҚАУІПСІЗДІК АУДИТІ

Жайлаухан Әсел Сардарбекқызы
asel.zhaylaukhan@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасының 4 курс студенті, Астана, Қазақстан
Ғылыми жетекші – Сисенов Н.М., Жарасхан Н.Ж.

Интернет заттары (IoT) – бұл физикалық объектілердің, құрылғылардың, көлік құралдарының, ғимараттардың және басқа да нәрселердің интернет арқылы өзара байланыста болатын желісі. Бұл объектілер ұсынылатын деректерді жинақтап, талдап, және басқару функцияларын атқара алады. IoT технологиясының өсуімен, қауіпсіздік мәселелері де күн тәртібіне қойылуда. Осыған байланысты, IoT жүйелерінде қауіпсіздік аудиті өте маңызды рөл атқарады.

IoT құрылғыларының көптігі және олардың әртүрлілігі, сондай-ақ кең ауқымды қолданыстары қауіпсіздікке қойылатын талаптарды күрделендіреді. Қауіпсіздік аудиті арқылы ұйымдар бұл құрылғылар арқылы туындайтын мүмкін қауіптерді анықтап, оларды басқару стратегияларын жасай алады.

Қазақстан технология саласында жаһандық даму үрдістеріне белсенді түрде қосылып келеді. Интернет заттары желісі (IoT) сондай-ақ, өнеркәсіп, ауыл шаруашылығы, қалалық инфрақұрылым және тұтынушылық қызметтер сияқты көптеген салаларда қолданыс табуда.

Қазақстанның мұнай-газ секторы және тау-кен өндірісі IoT технологияларын белсенді қолдануда. Бұл арқылы олар өндірістік процестерді оптимизациялай алады, қауіпсіздік стандарттарын күшейтеді және тиімділікті арттырады.

Ауыл шаруашылық технологияларында IoT құрылғылары ауа райын бақылау, өсімдіктердің өсуін бақылау және жер қорын тиімді пайдалану сияқты маңызды ақпараттарды жеткізеді.

Алматы және Астана сияқты ірі қалалар қауіпсіздік және жол көлік инфрақұрылымын жақсарту үшін IoT шешімдерін қолдануда. Мысалы, бақылау камералары, жол белгілерінің автоматтандырылған жүйелері және ақылды жарықтандыру жүйелері.

Қазақстандағы көптеген үйлер мен кеңселерде ақылды үй жүйелері қолданылады, олар жылу, жарық және энергияны басқаруда тиімділікті арттырады.

Қазақстан IoT технологияларын дамытуға инвестиция салып, ұлттық инновациялық жоспарларда оған ерекше көңіл бөлінеді. Дегенмен, қауіпсіздік мәселелері – әлі де басым тақырып болып табылады. Қауіпсіздікті арттыру жолдарына қатысты заңнамалық базаны жетілдіру және технологиялық нормативтерді бекіту қажет.

Қазақстанда IoT технологияларының қолданысы кеңейіп келеді және бұл бағыттағы даму үрдістері жалғаса береді. Алайда, инфрақұрылымдық жаңартулар мен қауіпсіздік шараларын қолға алу арқылы бұл технологиялардың тиімділігін арттыруға және