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

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№3
2025

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

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

3 (355)

JULY – SEPTEMBER 2025

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: «Central Asian Academic Research Center» LLP (Almaty).
Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*
Периодичность: *4 раза в год.*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

МАЗМҰНЫ

СОДЕРЖАНИЕ

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 3. Namber 355 (2025). 41–51

https://doi.org/10.32014/2025.2518-1726.362

ҒТМР 81.93.29
ӘОЖ 004.056.5

A. Amirova*, B. Aldosh, A. Ibraikhan, T. Smagulov, A. Aitmagambet, 2025.
Astana IT University, Astana, Kazakhstan.
E-mail: Akzhibek.amirova@astanait.edu.kz

A MACHINE LEARNING-BASED APPROACH TO DETECT MALICIOUS LINKS ON INSTAGRAM

Amirova Akzhibek — PhD, Assistant Professor, Astana IT University, Astana, Kazakhstan, E-mail: akzhibek.amirova@astanait.edu.kz, ORCID ID: https://orcid.org/0000-0002-5715-4954;
Aldosh Balziya — MSc, Senior Lecturer, Astana IT University, Astana, Kazakhstan, E-mail: b.aldosh@astanait.edu.kz, ORCID ID: https://orcid.org/0000-0002-2531-9718;
Alinur Ibraikhan — Student, Astana IT University, Astana, Kazakhstan, E-mail: 221596@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0009-3929-7378;
Temirlan Smagulov — Student, Astana IT University, Astana, Kazakhstan, E-mail: 221278@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0001-9039-3594;
Aysultan Aitmagambet — Student, Astana IT University, Astana, Kazakhstan, E-mail: 220920@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0008-2158-4234.

Abstract. With the rapid development of social networks and their integration into everyday life, platforms such as Instagram are becoming increasingly vulnerable to cyberattacks. One of the most common and dangerous vectors is the spread of malicious links. This study focuses on identifying and mitigating threats associated with the placement of harmful URLs in Instagram users' biographies, direct messages, and comments. The authors emphasize that traditional filtering methods, such as blocking or URL matching, are insufficient, since attackers actively use social engineering to disguise the true purpose of their links. To address this issue, a hybrid detection system is proposed that combines machine learning methods (Random Forest, LightGBM, XGBoost) with heuristic analysis. This approach enables a more comprehensive evaluation of suspicious content and significantly improves detection performance. Experimental results showed that the system reached 98% accuracy in classifying suspicious links. It was implemented as a browser extension, allowing users to promptly identify and flag potential threats, which demonstrates its practical value. Although the current version requires local installation, future work will focus on integrating deep learning techniques and incorporating contextual information to further increase automation and precision.

The proposed approach thus makes an important contribution to the development of cybersecurity methods for social networks and can serve as a foundation for scalable threat monitoring systems.

Keywords: Malicious link detection, machine learning, cybersecurity, real-time analytics, Instagram security, URL classification

А. Амирова*, Б. Альдош, А. Ибраихан, Т. Смагулов, А. Айтмагамбет, 2025.
Astana IT University, Астана, Қазақстан.
E-mail: Akzhibek.amirova@astanait.edu.kz

INSTAGRAMДАҒЫ ЗИЯНДЫ СІЛТЕМЕЛЕРДІ АНЫҚТАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУҒА НЕГІЗДЕЛГЕН ТӘСІЛ

Амирова Акжибек — PhD, ассистент профессор, Astana IT University, Астана, Қазақстан,
E-mail: akzhibek.amirova@astanait.edu.kz, ORCID ID: https://orcid.org/0000-0002-5715-4954;
Альдош Балзия — магистр, аға оқытушы, Astana IT University, Астана, Қазақстан,
E-mail: b.aldosh@astanait.edu.kz, ORCID ID: https://orcid.org/0000-0002-2531-9718;
Алинур Ибраихан — студент, Astana IT University, Астана, Қазақстан,
E-mail: 221596@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0009-3929-7378;
Темирлан Смагулов — студент, Astana IT University, Астана, Қазақстан,
E-mail: 221278@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0001-9039-3594;
Айсултан Айтмагамбет — студент, Astana IT University, Астана, Қазақстан,
E-mail: 220920@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0008-2158-4234.

Аннотация. Әлеуметтік желілердің қарқынды дамуымен және олардың күнделікті өмірге енуімен Instagram сияқты платформалар кибершабуылдарға осал бола бастады. Ең көп таралған және қауіпті векторлардың бірі – зиянды сілтемелердің таралуы. Бұл зерттеу Instagram қолданушыларының өмірбаянында, тікелей хабарламаларында және түсініктемелерінде зиянды Url Мекенжайларын орналастырумен байланысты қауіптерді анықтауға және азайтуға бағытталған. Авторлар URL мекен-жайларын бұғаттау немесе сәйкестендіру сияқты дәстүрлі сүзгілеу әдістері жеткіліксіз екенін атап көрсетеді, өйткені шабуылдаушылар өздерінің сілтемелерінің шынайы мақсатын жасыру үшін әлеуметтік инженерияны белсенді қолданады. Бұл мәселені шешу үшін машиналық оқыту әдістерін (Random Forest, LightGBM, XGBoost) эвристикалық талдаумен біріктіретін гибридті анықтау жүйесі ұсынылады. Бұл тәсіл күдікті мазмұнды жан-жақты бағалауға мүмкіндік береді және анықтау өнімділігін айтарлықтай жақсартады. Эксперименттік нәтижелер жүйенің күдікті сілтемелерді жіктеуде 98% дәлдікке жеткенін көрсетті. Ол пайдаланушыларға ықтимал қауіптерді дереу анықтауға және белгілеуге мүмкіндік беретін шолғыш кеңейтімі ретінде енгізілді, бұл оның

практикалық құндылығын көрсетеді. Ағымдағы нұсқа жергілікті орнатуды қажет етсе де, болашақ жұмыс автоматтандыру мен дәлдікті одан әрі арттыру үшін терең оқыту әдістерін біріктіруге және контекстік ақпаратты енгізуге бағытталады. Осылайша, ұсынылған тәсіл әлеуметтік желілер үшін киберқауіпсіздік әдістерін дамытуға маңызды үлес қосады және қауіптерді бақылаудың ауқымды жүйелерінің негізі бола алады.

Түйін сөздер. Зиянды сілтемелерді анықтау, машиналық оқыту, киберқауіпсіздік, нақты уақыттағы талдау, Instagram қауіпсіздігі, URL классификациясы

А. Амирова*, Б. Альдош, А. Ибраихан, Т. Смагулов, А. Айтмагамбет, 2025.
Astana IT University, Астана, Казахстан.
E-mail: Akzhibek.amirova@astanait.edu.kz

ПОДХОД НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ССЫЛОК В INSTAGRAM

Амирова Акжибек — PhD, ассистент профессор, Astana IT University, Астана, Казахстан,
E-mail: akzhibek.amirova@astanait.edu.kz, ORCID ID: https://orcid.org/0000-0002-5715-4954.
Альдош Балзия — магистр, старший преподаватель, Astana IT University, Астана, Казахстан,
E-mail: b.aldosh@astanait.edu.kz, ORCID ID: https://orcid.org/0000-0002-2531-9718;
Алинур Ибраихан — студент, Astana IT University, Астана, Казахстан,
E-mail: 221596@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0009-3929-7378;
Темирлан Смагулов — студент, Astana IT University, Астана, Казахстан,
E-mail: 221278@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0001-9039-3594;
Айсултан Айтмагамбет — студент, Astana IT University, Астана, Казахстан,
E-mail: 220920@astanait.edu.kz, ORCID ID: https://orcid.org/0009-0008-2158-4234.

Аннотация. С развитием социальных сетей и их глубокой интеграцией в повседневную жизнь такие широко используемые платформы, как Instagram, становятся все более уязвимыми для кибератак. Особенно в последние годы использование вредоносных ссылок превратилось в один из наиболее распространённых и опасных векторов атак, создавая серьёзные угрозы личным данным пользователей, их финансовой безопасности и целостности информационных систем. Подобные атаки часто направлены на обман пользователей с целью получения доступа к их аккаунтам, хищения конфиденциальной информации или распространения вредоносного программного обеспечения. Данное исследование ориентировано на выявление и снижение рисков, связанных с размещением вредоносных URL-адресов в биографиях, личных сообщениях и комментариях пользователей Instagram. Авторы подчёркивают, что традиционные методы фильтрации, такие

как блокировка или сопоставление URL, оказываются недостаточными. Это связано с тем, что злоумышленники активно используют методы социальной инженерии, маскируя истинное назначение ссылок и вводя пользователей в заблуждение. Для решения этой проблемы предлагается гибридная система обнаружения, объединяющая методы машинного обучения (Random Forest, LightGBM, XGBoost) с эвристическим анализом. Система выполняет комплексный анализ различных параметров, классифицирует подозрительные ссылки и достигает высокой эффективности. Экспериментальные результаты показали, что точность классификации достигает 98%. Реализация в формате расширения для браузера позволяет пользователям быстро выявлять и отмечать потенциальные угрозы. В настоящее время система требует локальной установки, однако в дальнейшем планируется внедрение методов глубокого обучения, использование контекстной информации и полная автоматизация процессов. Таким образом, предложенный подход вносит значительный вклад в обеспечение кибербезопасности в социальных сетях и может стать прочной основой для построения масштабируемых систем мониторинга угроз.

Ключевые слова: обнаружение вредоносных ссылок, машинное обучение, кибербезопасность, аналитика в реальном времени, безопасность Instagram, классификация URL

Кіріспе. Заманауи коммуникациялық технологиялар адамдар арасындағы қарым-қатынастарды, сондай-ақ таратылатын ақпарат пен коммерциялық әрекеттерді түбегейлі өзгертті. Қазіргі қоғам әлеуметтік медиа платформаларына қатты тәуелді, онда Instagram өзін олардың арасында әлемдік көшбасшы ретінде көрсетеді. Платформа 2 миллиардтан астам белсенді пайдаланушыларды қабылдайтындықтан, ол пайдаланушыларға іскерлік және жеке қажеттіліктерді қанағаттандыра отырып, нақты уақытта алмасуға және мазмұнды және тікелей хабарламаны бөлісуге мүмкіндік беретін қуатты платформа ретінде жұмыс істейді (Statista, 2024). Әлеуметтік медианың кеңеюі киберқауіптердің пропорционалды өсуіне әкелді, өйткені қылмыскерлер алаяқтық схемаларды жүргізу үшін платформаларды пайдаланады (Alharbi et al., 2024; Sheikhi, 2020). Instagram желісінде таратылатын зиянды сілтемелер пайдаланушылар жиі кездесетін және қауіпті киберқауіптердің бірі болып табылады. Бұл гиперсілтемелер түсініктемелер, DM және био және ақылы жарнамалар арқылы фишингтік алаяқтық, зиянды бағдарламаларды жіберу және қаржылық алаяқтық үшін кіру нүктесі ретінде әрекет етеді (Meshram et al., 2021).

Сандық қауіптер стандартты қауіпсіздік жүйелерін күн сайын тиімділігін төмендететін деңгейге дейін дамыды. Қара тізімдер және ережеге негізделген сүзгілеу сияқты зиянды сілтемелерді анықтау және блоктаудың дәстүрлі әдістері дамып келе жатқан шабуыл стратегияларына ілесу үшін күреседі. Киберқылмыскерлер өздерінің сілтемелерін әртүрлі әдістер арқылы анықтауды қиындатады, соның ішінде URL қысқартқыштары доменді өзгерту және

динамикалық қайта бағыттау тізбегі (Pradeep et al., 2023; Mughaid et al., 2023). Зиянды бағдарламалық қамтамасыз етуді таратушылар жаңылыстыратын байланыс және жалған жүлде жарнамалары немесе жеке басын куәландыратын жалған алаяқтық сияқты алдау әдістері арқылы пайдаланушыларды алдау үшін әлеуметтік инженерия әдістерін пайдаланады (Aljabri et al., 2023; Caruccio et al., 2023). Жағдай анықтаудан жалтаруға тырысатын зиянды сілтемелерді анықтау арқылы қорғаныс қызметін атқаратын жетілдірілген интеллектуалды жүйені талап етеді.

Инстаграмдағы зиянды сілтемелерді тарату жеке пайдаланушыларға қарағанда көбірек әсер ететін әсерлер жасайды. Инстаграмды маркетинг мақсаттары үшін, сонымен қатар брендинг мақсаттары мен тұтынушылармен өзара әрекеттесу үшін қолданатын ықпал етушілермен және ұйымдармен бірге компаниялар әлеуетті киберқауіптерге тап болады (Raja et al., 2021; Kaushik et al., 2022). Жалған өнімді жылжыту және фишингтік шабуылдармен бірге брендке еліктеу схемасы шынайы бизнеске елеулі бедел мен қаржылық зиян келтіреді (Durga et al., 2023). Платформа деңгейіндегі осалдықтарды азайта отырып, қауіптерді анықтау үшін толық қауіпсіздік жүйесін қажет етеді. Зерттеулер қауіпті азайту шешімдерін әзірлеу кезінде анықталған зиянды сілтеме қауіптерін Instagram үшін сенімді анықтау жүйесін құру үшін осы жұмысты жүзеге асырады. Зерттеу миллиондаған әлеуметтік медиа қолданушыларын бүкіл әлем бойынша қорғауды қамтамасыз ету үшін жаңа кибершабуыл жүйелеріне белсенді түрде бейімделетін қауіпсіздік негізін жасау үшін жетілдірілген алгоритмдерді енгізеді (Durga et al., 2023).

Ұсынылған зерттеу Instagram-дағы URL мекенжайларын анықтау үшін статикалық қара тізімдердің немесе ережеге негізделген анықтау әдістерінің орнына оқытуға негізделген тәсілді қолданады (Salamh et al., 2021; Nobili et al., 2023). Бірнеше киберқауіпсіздік зерттеулері қара тізімге негізделген URL сүзгісінің негізгі әлсіз жақтарын сипаттайды, себебі шабуылдаушылар анықтау шараларын айналып өту үшін URL қысқартқыштары мен динамикалық домен жасау әдістерін пайдаланады.

Материалдар мен әдістер. Инстаграмдағы зиянды сілтемелерді анықтауға көмектесу үшін машиналық оқыту және эвристикалық әдістер біріктірілді. Бұл әдістеме белгілі шабуыл үлгілерін пайдалана отырып, жаңа қауіптерді анықтауға қабілетті сенімді және бейімделгіш жүйені қамтамасыз етеді. Әзірленген алгоритм Random Forest, XGBoost және LightGBM көмегімен URL мекенжайларын зиянсыз, бүліну, фишинг және зиянды бағдарламалар санаттарына жіктеді. Жалпы фишинг сипаттамаларына негізделген URL мекенжайларының күдікті сипатын бағалау үшін қолмен жасалған ережелер жиынтығы қолданылды (Alsharida et al., 2023; Prince et al., 2024). Эвристикалық ережелерді машиналық оқытуға қосымша қадамдар ретінде қолдану дәлдікті және жаңа деректердегі үлгілерді анықтау мүмкіндігін жақсартты.

Функция таңдау

Машинамен оқытудың тиімді болуы үшін URL мекенжайларынан пайдалы

мүмкіндіктерді табуға болады (сурет). Бұл ерекшеліктерді келесідей жіктеуге болады:

Лексикалық мүмкіндіктер (URL құрылымы)

− URL ұзындығы: Ұзын URL мекенжайлары күдіктірек болады.

− Арнайы таңбалар саны: @, %, -, _, = және? нормадан тыс мөлшерде.

− Ішкі домендер саны: ішкі домендер тым көп (example.phishing.attack.com).

− Сандық қатынас: домендегі цифрлардың жоғары саны (мысалы, paypal123.com).

− IP мекенжайының болуы: өңделмеген IP мекенжайлары бар URL мекенжайлары (http://192.168.1.1).

− TLD талдауы: Сирек емес TLD (мысалы, .xyz, .tk) зиянды болуы мүмкін. Хост негізіндегі мүмкіндіктер (домен талдауы)

− WHOIS деректері: доменді тіркеу мәліметтерін (жасы, тіркеуші, жасалған күні) тексереді.

− Домен жасы: Жақында тіркелген домендер жиі зиянды.

− Танымалдық: Alexa, Majestic немесе Google Safe Browsing көмегімен домен рейтингін тексереді.

− SSL сертификатының болуы: зиянды домендерде HTTPS шифрлауы жиі болмайды.

Мазмұнға негізделген мүмкіндіктер

− HTML және JavaScript мүмкіндіктері: түсініксіз JavaScript, iframes және күдікті қайта бағыттауларды іздейді. 36

− Қайта бағыттаулардың болуы: тым көп қайта бағыттау фишинг немесе зиянды бағдарлама сайттарын көрсетуі мүмкін.

− Енгізілген сілтемелер: веб-беттегі сілтемелерді тексереді. Желіге негізделген мүмкіндіктер

− DNS ақпараты: доменнің IP мекенжайларын жиі өзгертетінін тексереді (жылдам ағын).

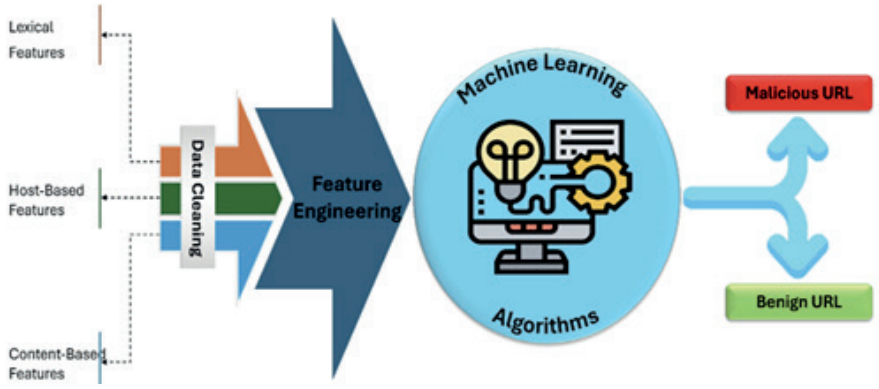
− PTR жазбалары: заңдылықты тексеру үшін кері DNS іздеулері.

− Хостинг туралы ақпарат: зиянды мазмұнмен белгілі хостинг провайдерлерін анықтайды.

Анықтау алгоритмінің жұмыс процесі

Машиналық оқыту алгоритмдерінің кірістері сандар болғандықтан, лексикалық сандық мүмкіндіктер файлдардағы URL мекенжайларынан жасалады (Сурет 1). Осылайша, машиналық оқыту алгоритмдеріне кіріс нақты өңделмеген URL мекенжайларынан гөрі сандық лексикалық мүмкіндіктер болады.

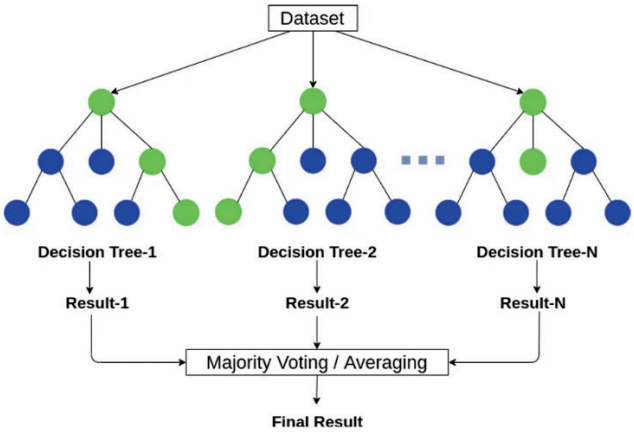
1-сурет. Машиналық оқыту моделі



Сәйкес келетін алгоритмді таңдау

Бұл жұмыс дәстүрлі машиналық оқыту үлгілерімен жақсы орындалады. Ең күшті алгоритмдерді табу үшін талдау дәлдік, дәлдік, еске түсіру және F1 балл негізінде жүргізіледі. Кездейсоқ орман, LightGBM және XGBoost сияқты машиналық оқытудың үш моделі олардың қалай жұмыс істейтінін білу үшін қарастырылады (сурет 2).

2-сурет. Кездейсоқ орман үлгісі



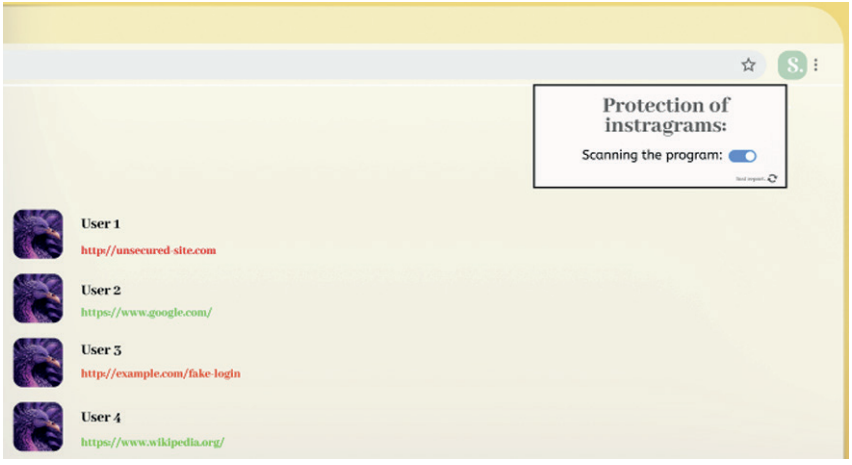
– Деректерді жинау және алдын ала өңдеу 660000-нан астам URL мекенжайлары бар деректер жиынын Firefox қамтамасыз етті. Деректер жинағы жүктелетін, талданатын және стратификацияланған іріктеу арқылы оқу және сынақ жиындарына бөлінген белгіленген URL мекенжайларын қамтиды.

– Функция инженериясы Әр түрлі URL негізіндегі мүмкіндіктер Python көмегімен бағдарламалық түрде шығарылды. Нүктелер саны, арнайы таңбалар

және домен құрылымы сияқты күдікті сипаттамалар талданады. Таңдауды оңтайландыру үшін оқытылған үлгілер арқылы мүмкіндіктің маңыздылығы анықталды.

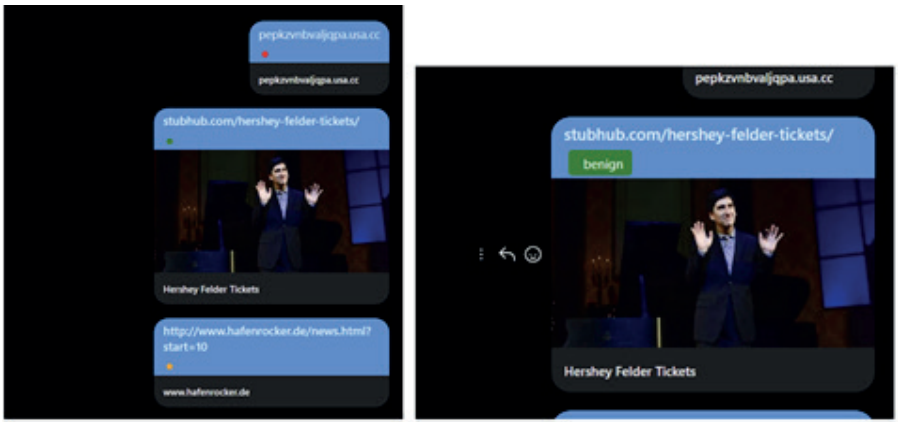
Нәтижелер мен талқылау. Интерфейс макети браузер кеңейтімі пайдаланушыларды Instagram сілтемелерінің қауіпсіздігі туралы ескертетінін көрсету үшін жасалған. 3-суретте интерфейстегі барлық пайдаланушылар және олардың әрқайсысы хабарламаға кіретін URL мекенжайлары көрсетілген. Барлық сілтемелер автоматты түрде сканерленеді және оларға сәйкес түс беріледі: қауіпті немесе жалған сілтемелер үшін қызыл және қауіпсіз сілтемелер үшін жасыл. «Instagram Protection: сканерлеу бағдарламасы» деп белгіленген Instagram қорғау кеңейтімі жоғарғы оң жақ бұрышта орналасқан. Әзірлеудің кейінгі кезеңдерінде мүмкіндіктер қолданбаны пайдалануды жеңілдету және кеңістікті толтырмау үшін жаңартылды. Сілтемелерде қауіп деңгейін көрсету үшін түстерді пайдаланбау үшін жаңа дизайн оны меңзерді апарған кезде көрсететін көпіршікті индикаторлармен ауыстырды. Әрбір сілтеменің жанында белгіше пайда болады және меңзерді оның үстіне апарған кезде, «фишинг», «зиянды бағдарлама» немесе «қатерсіз» сияқты қауіп түрін көресіз. Нәтижесінде дизайн пайдаланушыға ыңғайлы және негізгі қауіпсіздік фактілері әлі де қолжетімді.

3-сурет. Mock-up



Идея іске асырылды және MVP ретінде қарастырылды, бұл оның Instagram веб-сайтымен оңай жұмыс істеуін қамтамасыз етеді және нақты уақытта URL мониторингін ұсынады. Ағымдағы беттегі сілтемелер дереу сканерленеді және сервердегі ақпаратты пайдаланып кеңейтіммен бөлектеледі (Сурет 4).

4-сурет. Instagram Direct Messages ішіндегі бірнеше сілтемелерді тікелей таңбалау



Барлық сілтемелер олардың қандай сілтеме екенін көрсететін шағын белгілермен белгіленеді. «Фишинг» немесе «жақсы» сияқты сөздер кез келген хабар түріндегі немесе пайдаланушы биосындағы сілтемелердің жанында пайда болады, бұл қандай сілтемелер зиянды болуы мүмкін екенін тез көрсетеді. Жүйе тәуекел деңгейін көрсету үшін түсті индикаторлары бар (қызыл, жасыл, қызғылт сары сияқты) бірнеше тегтерді пайдаланады.

Тестілеу кезінде кеңейтім қысқартылған сілтемелер, қайта бағытталған домендер және тұрақты веб-сайттар сияқты әртүрлі URL мекенжайларын өңдеді. Нәтижесінде жүйе деректердің кең ауқымын жоғары дәлдікпен өңдей алады (Сурет 5).

5-сурет. Аралас жағдайдағы мысалдар

Осылайша, бұл тәсіл кәдімгі нақты уақыттағы қауіпсіздік қол жетімді болмаған кезде зиянды сілтемелерден қарапайым шолғышты қорғауды орнатуға болатынын көрсетеді.

Жүйе кейбір эвристикалық ережелермен қатар Random Forest, LightGBM және XGBoost машиналық оқыту үлгілерінің қоспасына негізделген. Сондықтан жасырын шабуылдар ертерек ашылады және проблемаларды танудағы қателер саны азаяды, бұл қажет, өйткені адамдар күнделікті әлеуметтік медианы көп пайдаланады. Модельді жасау кезінде төрт мүмкіндік

мұқият таңдалып, келесі санаттарға топтастырылды: лексикалық, желілік және хост. Нәтижесінде бұл командаға URL мекенжайларындағы өзгерістер, күдікті домендер және веб-сайттардың сілтемелерді қысқарту тәсілдері сияқты зиянды бағдарламаның әдеттен тыс шағын белгілерін табуға мүмкіндік берді. Осы механизмдердің арқасында зиянды сілтемелер тоқтатылады және адамның араласуынсыз басқаларға таралуына жол бермейді.

Зиянды URL мекенжайларын жылдам көруге ғана емес, зерттеу олардың әрекеттерін байқауға және оларды қауіпсіз сайттардан ажыратуға көмектесетін белгілерді таңдауға көмектесті. Нәтижесінде киберқауіпсіздік жүйелері күшейіп, жақсырақ қорғауға ие бола алады, сонымен қатар олар кездесетін қауіптер туралы көбірек түсінеді. Нәтижелерді ескере отырып, жүйені жетілдіретін және оны жағдайлардың кең ауқымында қолдануға жарамды ететін жаңа технологияларды қолдану арқылы одан әрі жұмыс істеуге болады. Конволюционды нейрондық желілер (CNN), қайталанатын нейрондық желілер (RNN) және трансформаторлар сияқты терең оқыту әдістері бүгінгі АИ дамуының негізгі бағыттары болып табылады. Бұл үлгілер жалған қорытындыларды азайту және қауіпті анықтауды жақсарту үшін URL мекенжайындағы таңбаларды, сондай-ақ олардың айналасындағы мәтінмәнді анықтайды.

Нәтижелерді ескере отырып, жүйені жетілдіретін және оны жағдайлардың кең ауқымында қолдануға жарамды ететін жаңа технологияларды қолдану арқылы одан әрі жұмыс істеуге болады. Конволюционды нейрондық желілер (CNN), қайталанатын нейрондық желілер (RNN) және трансформаторлар сияқты терең оқыту әдістері бүгінгі жасанжы интеллект дамуының негізгі бағыттары болып табылады. Бұл үлгілер жалған қорытындыларды азайту және қауіпті анықтауды жақсарту үшін URL мекенжайындағы таңбаларды, сондай-ақ олардың айналасындағы мәтінмәнді анықтайды. Жүйе киберәлемдегі жаңа және жылдам қозғалатын қауіптерге ілесе алуы маңызды. Модельдер нақты уақытта жаңартылуы және олардың нәтижелері өзгеріссіз қалуы үшін ағынды деректерді өңдеуді және бейімделген оқытуды қосу қажет. Пайдаланушы әрекетін талдау және контекстті зерделеу арқылы NLP зиянды сілтемелерді анықтауға көмектесе алады, сондай-ақ адаптивті аутентификация сияқты нәрселерді пайдалана отырып, жеке қорғанысты қолдайды.

Қорытынды. Зерттеулер гибридті машиналық оқыту қаупін бағалау шешімін әзірлеу арқылы Instagram сілтеме қатерін анықтауға айтарлықтай мән берді. Ұсынылған жүйе киберқауіпсіздік саласындағы елеулі прогресті көрсетеді, себебі ол жоғары дәлдік пен сенімділікті және нақты уақыттағы қауіптерді анықтау мүмкіндігін қамтамасыз етеді. Бұл жүйенің болашақ әзірлемелері терең оқыту интеграциясын, сондай-ақ бейімделгіш өңдеуді және контекстті ескеретін талдау мүмкіндіктерін, сонымен қатар қарсыластық сенімділігі мен құпиялылықты қорғау шараларын қажет етеді. Бұл жақсартулар цифрлық платформаларды әзірлеуде жеке пайдаланушыларды да, ұйымдарды да қорғайтын қауіпсіз цифрлық құрылымды жасайды.

References

Statista (2024) Most used social networks 2024, by number of users. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (in Eng.)

Alharbi N., Alkalifah B., Alqarawi G., & Rassam M.A. (2024) Countering social media cybercrime using deep learning: Instagram fake accounts detection. Future Internet, 16(10). — P.367–383. https://doi.org/10.3390/fi16100367 (in Eng.)

Sheikhi S. (2020). An efficient method for detection of fake accounts on the Instagram platform. Revue d'Intelligence Artificielle, 34(4). — P. 429–436. https://doi.org/10.18280/ria.340407 (in Eng.)

Meshram P., Bhambulkar R., Pokale P., Kharbikar K. & Awachat A. (2021, May) Automatic detection of fake profile using machine learning on Instagram. International Journal of Scientific Research in Science and Technology. — P. 117–127. https://doi.org/10.32628/ijsrst218330 (in Eng.)

Pradeep V. & Vaidehi V. (2023) Detection of malicious social bots using Instagram hashtags. International Journal of Advanced Engineering and Management, 8(2). — P.100–112. https://doi.org/10.35629/5252-06048794 (in Eng.)

Mughaid A., et al. (2023) A novel machine learning and face recognition technique for fake accounts detection system on cyber social networks. Multimedia Tools and Applications, 82(17). — P.26353–26378. https://doi.org/10.1007/s11042-023-14347-8 (in Eng.)

Aljabri M., Zagrouba R., Shaahid A., Alnasser F., Saleh A., & Alomari D. M. (2023) Machine learning-based social media bot detection: A comprehensive literature review. Social Network Analysis and Mining, 13(1). https://doi.org/10.1007/s13278-022-01020-5 (in Eng.)

Caruccio L., Cimino G., Cirillo S., Desiato D., Polese G. & Tortora G. (2023) Malicious account identification in social network platforms. ACM Transactions on Internet Technology, 23(4). — P.1–25. https://doi.org/10.1145/3625097 (in Eng.)

Raja M.S., & Raj L.A. (2021) Detection of malicious profiles and protecting users in online social networks. Wireless Personal Communications, 127(1). — P.107–124. https://doi.org/10.1007/s11277-021-08095-x (in Eng.)

Kaushik K., Bhardwaj A., Kumar M., Gupta S.K., & Gupta A. (2022) A novel machine learning-based framework for detecting fake Instagram profiles. Concurrency and Computation: Practice and Experience, 34(28). https://doi.org/10.1002/cpe.7349 (in Eng.)

Durga P., & Sudhakar D.T. (2023, January) The use of supervised machine learning classifiers for the detection of fake Instagram accounts. Journal of Pharmaceutical Negative Results. — P.267–279. https://doi.org/10.47750/pnr.2023.14.03.36 (in Eng.)

Salamh F.E., Mirza M.M., Hutchinson S., Yoon Y.H., & Karabiyik U. (2021) What's on the horizon? An in-depth forensic analysis of Android and iOS applications. IEEE Access, 9. — P.99421–99454. https://doi.org/10.1109/ACCESS.2021.3095562 (in Eng.)

Nobili M. (2023) Review OSINT tool for social engineering. Frontiers in Big Data, 6. https://doi.org/10.3389/fdata.2023.1169636 (in Eng.)

Alsharida R.A., Al-Rimy B.A., Al-Emran M., & Zainal A. (2023) A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society, 73. — P.102–118. https://doi.org/10.1016/j.techsoc.2023 (in Eng.)

Prince N.U., et al. (2024, August). AI-powered data-driven cybersecurity techniques: Boosting threat identification and reaction. Nano-NTP, 20(S10). — P.1804–1815. https://doi.org/10.62441/nano-ntp.v20iS10.1804 (in Eng.)

Publication Ethics and Publication Malpractice
in the journals of the Central Asian Academic Research Center LLP

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

Submission of an article to the journals of the Central Asian Academic Research Center LLP 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 other language, 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 Central Asian Academic Research Center LLP 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 Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP 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)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 25.09.2025.
Формат 60x881/8. Бумага офсетная.
Печать –ризограф. 20,0 п.л. Заказ 3.

Национальная академия наук РК
050000, Алматы, ул. Кунаева 132