NEWS
OF THENATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2, Number 336 (2021), 91 – 95 **https://doi.org/10.32014/2021.2518-1726.25**

УДК 004.32

М. Е. Раимов, А. К. Мукашева, Г. Б. Исаева, Қ. Нұралбай

«Ғұмарбек Даукеев атындағы Алматы энергетика
және байланыс университеті», Алматы, Қазақстан.
E-mail:guka_issaeva@mail.ru

САЙТТАҒЫ КИБЕРШАБУЫЛДАРДЫ ТАНУДА ЗЕРТТЕУ ЖҮРГІЗУ

Аннотация. Интернет желісінің жылдам дамуы оң және теріс сәттерді өзімен алып келді. Жыл сайын ақпаратты ұрлауды жүзеге асырғысы келетін және ресурстың жұмысын бұзғысы келетін, басқа да осындай іс-әрекеттерді жүзеге асырғысы келетін адамдар мен тәсілдер көбейіп келеді. Осыған байланысты әртүрлі шабуылдарға сайттардың тұрақтылығы туралы мәселе ерекше өзекті болып отыр, яғни веб-қосымшаларды әзірлеушілерге өз өнімдерінің сенімділігін арттыруға көмектесетін көптеген жобалардың пайда болуына әкеледі. Шын мәнінде, веб сайтты тестілеу және сауалнама жүргізу, веб-қосымшалар іздеу секілді іс әрекеттер жақсы ескерту шарасы ретінде анықтауға мүмкіндік беретін кемшіліктері қосымшаны әзірлеу және жабық тестілеу, осылайша, қосымшаның ақпараттық қауіпсіздікке мықтылығын анықтауға болатынын көрсетеді.

Түйін сөздер: деректердің қауіпсіздігі, веб-сайт, кибершабуыл, ғаламтор.

Кіріспе. Веб-қосымшалардың қауіпсіздігі-ақпараттық қауіпсіздік контекстіндегі ең өткір мәселелердің бірі. Әдетте, интернетте қол жетімді веб-сайттардың көпшілігі әртүрлі осалдықтарға ие және үнемі шабуылдарға ұшырайды. Бұл жұмыстың негізгі мақсаты веб-қосымшалардың қауіпсіздік құралдарын зерделеу, сондай-ақ ең көп таралған осалдықтарды анықтау және веб-қосымшалардың немесе веб-сайттардың қауіпсіздік күшін арттыру бойынша ұсыныстарды әзірлеу және веб қосымша әзірлеу болып табылады.

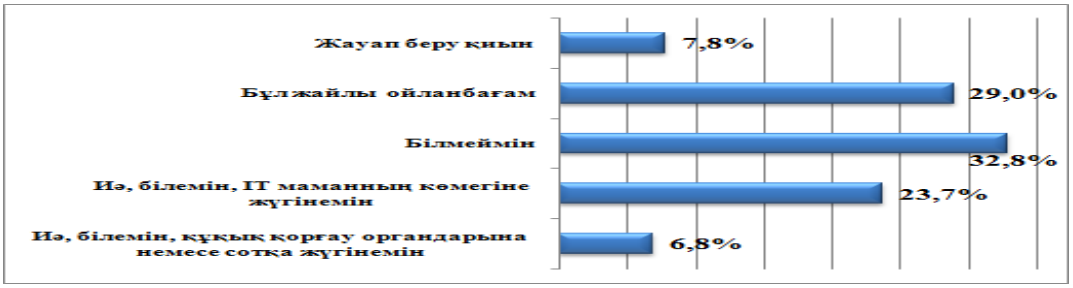
Веб сайттың қауіпсіздік мәселелері көптеген елдерде жетекші орындарды иеленеді. «Перспективный мониторинг» компаниясының зерттеулеріне сәйкес, 2019 жылы шабуылшылардың ең көп бөлігі жеке тұлғаларға бағытталған [1]: олар барлық шабуылдардың төрттен бір бөлігін құрайды (26%). Ұйымдарға келетін болсақ, кибершабуылдардан көп зардап шеккендер – мемлекеттік құрылымдар (13%), банктер және онлайн-сервистер (8%).

Трояндар ең көп таралған санатқа айналды: 2019 жылдың бірінші тоқсанының аяғында қолданушылардың 10.26%-ында табылды. Екінші және үшінші орынды вирустар (1,59%) және троян жүктегіштер (0,64%) алды.

Kaspersky Security Network мәліметтері бойынша 2019 жылдың үшінші тоқсанындағы веб сайттың қауіптер статистикасы [3]:

- «Kaspersky Lab» шешімдері әлемнің 203 елінде орналасқан интернет ресурстардан 947027577 шабуылдарға тойтарыс берді.
- Веб-антивирустар зиянды 246695333 URL мекен-жайларды тіркеді.
- Банктік шоттарға онлайн қол жеткізу арқылы ақша ұрлайтын зиянды
- бағдарламаларды іске қосу әрекеттері 305315 пайдаланушылардың компьютерлерінде тіркелді.
- Шифрлаушы бағдарламалардың шабуылдары 259867 пайдаланушылардың компьютерлерінде тіркелді.
- Антивирус 239177356 зиянды және жағымсыз нысандарды анықтады.

Жалпы жоғарыда келтірілген мағұлматтарды ескере отырып, Қазақстан тұрғындары кибершабуыл жағдайында қайда хабарласу керектігін білетіндігін сұрады. Осыған халықтың 32,8%-ы желіде шабуыл жасаған жағдайда қайда жүгіну қажет екенін білмеген. Сұралғандардың 23,7% IT-маманға көмек алу керектігін біледі. Халықтың 6,8% құқық қорғау органдарына жүгінеді (1-суретті қараңыз).



1-сурет – Кибершабуыл жағдайында қайда хабарласу керектігін білесіз бе? графигі

Кибершабуыл болған жағдайда Қостанай (49,3%), Жамбыл (45,6%) және Алматы (42,2%) облыстарының тұрғындары қайда хабарласу керектігін білмейді (2 суретті қараңыз).

РЕГИОНЫ	Иә, білемін, құқық қорғау органдарына немесе сотқа жүгінемін	Иә, білемін, IT маманның көмегіне жүгінемін	Білмеймін	Бұл жайлы ойланбағам	Жауап беру қиын
Атырау облысы	4,6%	12,7%	38,0%	35,9%	8,9%
Мангыстау облысы	3,5%	23,9%	33,6%	17,6%	21,5%
Солтүстік Қазақстан облысы	3,1%	26,0%	42,2%	25,1%	3,5%
Шымкент қ.	12,5%	49,3%	21,7%	12,5%	3,9%
Шығыс Қазақстан облысы	1,1%	7,9%	45,6%	39,2%	6,2%
Қызылорда облысы	0,6%	36,0%	30,9%	21,3%	11,2%
Туркестан облысы	9,3%	14,3%	41,0%	30,8%	4,5%
Актюбе облысы	11,1%	19,9%	49,3%	16,6%	3,0%
Батыс Қазақстан облысы	5,2%	10,9%	27,9%	36,2%	19,7%
Астана қ.	14,3%	36,1%	21,3%	23,9%	4,3%
Караганды облысы	2,0%	13,4%	23,4%	50,5%	10,6%
Павлодар облысы	9,1%	23,5%	24,3%	31,3%	14,3%
Жамбыл облысы	16,8%	28,7%	34,1%	15,6%	4,8%
Костанай облысы	13,8%	26,3%	32,6%	22,5%	4,8%
Алматы қ.	2,4%	33,1%	17,2%	35,9%	11,4%
Ақмола облысы	2,8%	26,0%	36,7%	27,7%	6,8%
Алматы облысы	12,1%	35,8%	25,5%	22,2%	4,4%

2-сурет – Кибершабуыл жағдайында қайда хабарласу керектігін білесіз бе? (өңірлер бойынша бөлінісінде) графигі

Бұдан әрі, жоғарыда көрсетілген сұраққа оң жауап берген халық санаты авторизация жасайтын сайттар туралы ақпаратты тексеретінін нақтылауды сұрады. Осы сұраққа қатысты зерттеу нәтижелері мынадай: респонденттердің тек төрттен бір бөлігі (25,8%) ресурс қандай да бір күмән туғызған кезде сайт туралы ақпаратты кейде тексереді. Қазақстандық пайдаланушылардың тағы 20,5%-ы ақпаратты өте сирек тексереді, ал 14,1%-ы ешқашан қауіпсіздік ресурсын тексермейді және 8,5%-ы сайтты қалай қауіпсіз тексеруге болатынын білмейді. Тек Қазақстанның әрбір бесінші тұрғыны авторланатын сайт туралы ақпаратты үнемі тексереді (19,6%) (3-диаграмманы қараңыз).

3-сурет – Сіз өзіңіз авторланатын сайттар туралы ақпаратты тексересіз бе? графигі

Еліміздің әрбір екінші тұрғыны онлайн қызметтерді пайдалану үшін мобильді қосымшаларды пайдаланады. Қарағанды облысының тұрғындары (62,8%) 25-тен 30 жасқа дейінгі (21,8%) жоғары білімі бар (99,9%). Түркістан облысының тұрғындары (88,8%), 65 және одан жоғары жастағы, орта білім деңгейі бар тұрғындары мобильді қосымшаларды өте сирек және ешқашан пайдаланбайды.

Халық арасында қызметтерді төлеуге арналған мобильдік қосымшалар арасында Каспий банкінің мобильдік қосымшасы көшбасшы болып табылады – Kaspi.kz (20,5%). Екінші орында Халық банкінің мобильді қосымшасы – MyHalyk (4%), үшінші орында DamuMed (1,8%) мобильді қосымшасы. Сауалнамаға қатысқандардың 63,2% - ы осы сұраққа жауап беруге қиналды (4-кестені қараңыз).

Жауап нұсқалары	%
Онлайн-банкинг	28,70%
Kaspi.kz	20,50%
Myhalyk	4%
Homebank.kz	0,70%
Старбанкинг	0,20%
Түрлі банктер	0,90%
Ақша аударымдары	0,10%
Қызметтерді онлайн сервистер арқылы төлеу	7,40%
Damumed	1,80%
Киви әмиян	1,60%
Қызметтерге, коммуналдық төлемдерге ақы төлеу, несиелерді төлеу, балабақша	0,80%
Билеттерді сатып алу	0,70%
Chocolife	0,70%
Egov.kz	0,60%
Билайн	0,20%
InDriver	0,10%
Олар көп (көрсетілмеген).ред.)	0,10%
Жауап беруге қиналамын	63.2%

4-сурет – Онлайн қызметтерді төлеу және алу үшін пайдаланылатын қосымшаның атауы

Жауаптардың сомасы 100% тең емес, өйткені бір респондент жауаптың бірнеше нұсқасын таңдай алды. Онлайн-қызметтерді алу үшін мобильді қосымшаларды пайдаланатын респонденттер ғана жауап берді.

Онлайн банктік операцияларды жасауда өзінің жеке деректерін пайдаланатын тұлғалардың көрсеткіштеріне қатысты біршама басқа көрініс. Мұнда елдің әрбір үшінші тұрғыны банк операцияларын онлайн жасайды.

Бұл, егер онлайн ақша операциялары туралы болса, халық өзінің қаржылық іс-қимылдарына сақтықпен қарайды деген сөз.

Сонымен қатар, сауалнамаға қатысушылар соңғы уақытта веб сайттың қауіпсіздіктің өзекті қатерлерінің үштігін атап өтеді. Осылайша, сауалнама қорытындысы бойынша 57,6% компьютерлік вирустар мен хакерлердің қызметі ең өзекті қауіп деп санайды. Екінші орында веб сайттың қауіпсіздік үшін өзекті қауіп – қатерлер тізімінде түрлі мазмұндағы спам тарату (25,8%). Үшінші орында-кибералаяқтар, оларда халықтың 19% көрсетті (5-кестені қараңыз).

Жауап нұсқасы	%
Хакерлердің қызметі	28,8%
Жүйелік әкімшілердің ісіне салғырт қарау	13,3%
Компьютерлік вирустар	28,8%
Кибермошенниктер, интернетте алаяқтар, көптеген адамдар алдауға тырысады,олардың шотына ақша аударуды сұрайды	19%
Түрлі мазмұндағы спам тарату	25,8%
Басқа	*0,3%*
Жауап беруге қиналамын	*19,8%*

5-сурет – Сіз қалай ойлайсыз, соңғы уақытта веб сайттың қауіпсіздікке қандай қауіп-қатерлер өзекті болды? Кестесі.

Сома 100% тең емес, өйткені бір респондент жауаптың бірнеше нұсқасын таңдайалады.

"Сіз соңғы жылы кибершабуылдарға ұшырадыңыз ба?"Қазақстан тұрғындарының жартысы теріс жауап берді (51%). Сонымен қатар, соңғы жылы кибершабуылдарға ұшырағандардың үлесі де бар. Жалпы алғанда, халықтың 34,1%-ы соңғы жылы кибершабуылға ұшыраған. Мұндай шабуылдарға келесі құбылыстарды жатқызуға болады: зиянды СПАМ (10,8%), зиянды бағдарламалық қамтамасыз ету (8,7%), әлеуметтік желілердегі аккаунттарды бұзу (7,4%), банктік карталармен кибералаяқтық, алаяқтықтың басқа түрлері (6,9%) (7-диаграмманы қараңыз).

Сурет 7 – Сіз соңғы жылы кибершабуылдарға ұшырадыңыз ба? графигі

Қорытынды: Веб сайттарды кибершабуылдан қорғау моделдері зерттеу барысынды сауалнама жүргізілген болатын. Сауалнама қорытындысы төменде келтірілген.

Жүргізілген әлеуметтік зерттеу нәтижесінде жаппай сауалнамаға әр түрлі жастағы, 18 жастан 65 жасқа дейін және одан үлкен 6000 респондент қатысты,олардың ішінде жастар көп жас тобы болып табылады, сауалнама Қазақстанның 17 өңірінде, оның ішінде Астана, Алматы және Шымкент қалаларындаөткізілді.

Жеке мәліметтерді қорғау бойынша шараларды жүзеге асыру кезінде Қазақстан Республикасында кездесетін мәселелерді анықтау халықтың соңғы жылы кибершабуылға ұшырағанын көрсетті. Алынған деректер дербес деректерді қорғау, киберқауіпсіздік мәселелерінде және веб сайттың қауіпсіздікті қамтамасыз ету бойынша қабылданып жатқан шараларда халықтың хабардарлығын арттырудың маңыздылығын күшейтеді.

ӘДЕБИЕТ

[1] Корченко А.Г., Архипов А.Е., Казмирчук С.В. Анализ и оценивание рисков информационной безопасности: монография /– К. : Лазурит–Полиграф, 2013. – С.253–275.

[2] Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації. К. : ПоліграфКонсалтинг. 2018. – 209с.

[3] Норткат С., Новак Жд. Обнаружение вторжения в сеть. / пер. с англ. – М.: Издательство «Лори», 2019. – 384с.

[4] Atighetchi M., Pal P., Webber F., Schantz R., Jones C., Loyall J. Adaptive Cyberdefense for Survival and Intrusion Tolerance // Internet Computing. - 2020. - Vol.8, No.6. – P.25–33.

[5] Уязвимости веб-приложений [электронный ресурс] : научно- популярный, открытый доступ. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Веб-Vulnerability-2016-rus.pdf (дата обращения: 17.05.2018

[6] Информационная безопасность: проблемы [электронный ресурс]: научно-популярный, открытый доступ. URL: http://ieu.cfuv.ru/viewfile/2372/Сборник трудов III международной конференции. Проблемы-инф. безоп. -2016.pdf (дата обращения: 15.03.2018)

[7] Vulnerabilities in data processing levels [электронный ресурс] : научно-популярный, открытый доступ. URL: http://www.slideshare.net/beched/slides-34960189 (дата обращения: 02.06.2018

REFERENCES

[1] Korchenko A. G., Arkhipov A. E., Kazmirchuk S. V. analysis and assessment of Risk Information Security: monograph / K. : Lapis Lazuli–polygraph, 2013. pp. 253-275.

[2] Tereikovskiy I. neuron of Honor in the zasobakh zachistu comp'uternoї informatsiї. K.: Polygrafconsalting. 2018. 209 P.

[3] Northkat S., Novak Zhd. "I don't know," he said. / per. from the English. Moscow: Publishing House "Lori", 2019. 384 p.

[4] Atighetchi M., Pal P., Webber F., Schantz R., Jones C., Loyall J. Adaptive Cyberdefense for Survival and Intrusion Tolerance // Internet Computing. 2020. Vol.8, No.6. P.25–33.

[5] web application [electronic resource]: scientific and popular, open access. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Веб-Vulnerability-2016-rus.pdf (date: 17.05.2018

[6] 6.information security: problem [electronic resource]: scientific and popular, open access. URL: http://ieu.cfuv.ru/viewfile/2372/Сборник labor III International Conference. The problem is Infa. "no," I said. -2016. pdf (date: 15.03.2018)

[7] Vulnerabilities in data processing levels [electronic resource]: scientific and popular, open access. URL: http://www.slideshare.net/beched/slides-34960189 (date: 02.06.2018)

Information about authors:

Master Raimov M. E., "Almaty University of energy and Communications named after Gumarbek Daukeev", Almaty, Kazakhstan. E-mail: r_m_18@mail.ru;

PhD, Mukasheva A. K., "Almaty University of energy and Communications named after Gumarbek Daukeev", Almaty, Kazakhsta. E-mail: a.mukasheva@aues.kz, https://orcid.org/0000-0001-98904910;

K. P. N, Issayeva G. B., "Almaty University of energy and Communications named after Gumarbek Daukeev", Almaty, Kazakhstan. E-mail: guka_issaeva@mail.ru;

Master's degree Nuralbay, "Gumarbek Daukeev Almaty University of energy and Communications", Almaty, Kazakhstan. E-mail: nuralbai.kundyz@gmail.com, https://orcid.org/0000-0002-9210-0740

М. Е. Раимов, А. К. Мукашева, Г. Б. Исаева, К. Нуралбай

Алматинский университет энергетики и коммуникаций им. Гумарбека Даукеева, Алматы, Казахстан

ИССЛЕДОВАНИЯ ПО РАСПОЗНАВАНИЮ КИБЕРАТАК НА САЙТ

Аннотация. Быстрое развитие сети Интернет принесло с собой как положительные, так и отрицательные моменты. С каждым годом все больше людей и способов, желающих осуществить кражу информации, нарушить работу ресурса и осуществить другие подобные действия. В связи с этим вопрос устойчивости сайтов к различным атакам становится особенно актуальным и приводит к появлению большого количества проектов, которые помогают разработчикам веб-приложений повысить надежность своих продуктов. На самом деле, такие действия, как тестирование и опрос веб-сайта, поиск веб-приложений позволяют определить как хорошую меру предупреждения недостатков. Разработки приложений и закрытое тестирование показывают, что таким образом можно определить, является ли приложение устойчивым к информационной безопасности.

Ключевые слова: безопасность данных, веб-сайт, кибератака, Интернет.

M. E. Raimov, A. K. Mukasheva, G. B. Isayeva, K. Nuralbay

Gumarbek Daukeev Almaty University of Energy and Communications, Almaty, Kazakhstan

RESEARCH ON THE RECOGNITION OF CYBER ATTACKS ON THE SITE

Abstract. The rapid development of the Internet has brought with it both positive and negative aspects. Every year, there are more and more people and methods that want to steal information and disrupt the work of the resource, to carry out other similar actions. In this regard, the issue of site resistance to various attacks becomes particularly relevant, that is, it leads to the emergence of a large number of projects that help web application developers to improve the reliability of their products. In fact, actions such as testing and polling a website, searching for web applications, allow you to determine as a good warning measure the shortcomings of application development and closed testing show that, in this way, it is possible to determine whether an application is resistant to information security.

Keywords: data security, website, cyber attack, internet.