

**А.И.Ходжиметов,
ЎзР БМА профессори**

**Ш.Б.Расулов,
ЎзР БМА магистри**

ТИЖОРАТ БАНКИНИНГ КИБЕРХАВФСИЗЛИГИГА ТАЪСИР ЭТУВЧИ ТАШҚИ ОМИЛЛАР

Аннотация: Молия тизимининг рақамли технологиялар тараф ҳаракати уни кибержиноятчилар учун заиф ва ўзига жалб этувчи соҳага айланишига олиб келмоқда. Мақолада тижорат банкларининг киберхавфсизлигига таъсир этувчи ташқи омиллар таҳлил қилиниб, уларнинг орасида энг кўп тарқалгани – malware инфекциясининг ўсиб бориши сурати моделлаштирилган.

Калит сўзлар: киберхавфсизлик, киберхужум, ташқи омил, malware, модель, тренд чизиғи, боғланиш, функция.

Аннотация: Высокие темпы внедрения цифровых технологий в финансовую систему делают ее слабым и привлекательным сектором для киберпреступников. В статье анализируются внешние факторы, влияющие на кибербезопасность коммерческих банков и моделирован рост наиболее распространенного из них, инфекции malware.

Ключевые слова: кибербезопасность, кибератака, внешний фактор, malware, модель, линия тренда, ссылка, функция.

Annotation: The rapid pace of digitalization in the financial system makes it a weak and attractive sector for cybercriminals. The article analyzes the external factors affecting the cybersecurity of commercial banks and simulates the growth of the most common of them, malware infection.

Keywords: Cybersecurity, cyber-attack, external factor, malware, model, trend line, link, function.

Кириш

Молия тизими шиддат билан рақамли технологиялар тараф ҳаракатланар экан, бу соҳа борган сари кибержиноятчилар учун заиф ва ўзига жалб этувчи соҳага айланиб бораверади. Виртуал маълумотлар ва активларни химоялаш эса кенг қамровли ва мустахкам хавфсизлик чораларини кўришни талаб этади. Киберхужумлар одатда махфий маълумотларга кириш, уларни ўзгартириш ёки йўқ қилиш, фойдаланувчилардан пул ундириш ёки бизнес жараёнларини бузишга қаратилган. Айниқса банк соҳаси киберхужумлардан асосий жабр кўрувчи ҳисобланади. Активларининг кўплиги ва мижозлар маълумотларининг катта тўплами банкларни кибержиноятларнинг асосий нишонига айлантиради.

Ташқи фирибгарлик хавфига қўшимча равишда, ходимлар, фойдаланилган заиф дастурий таъминот ёки эскирган ускуналардан фойдаланиш банклар учун ички таҳдидларнинг янги потенциал хавфини юзага келтиради. Иш берувчилар

ходимларни ўқитиш ва киберхавфсизлик бўйича ўқув дастурларини амалга ошириш бўйича чоралар кўришлари шарт, чунки ходимларни ушбу соҳада билимга эга бўлиши инсон омиллари туфайли юзага келадиган барча кибертаҳдидлар ва ҳодисалардан ҳимояланишни асосий шартидир. Шунинг учун ёдда тутиш керакки, барча ҳимоя чораларининг 90 фоизи ходимларнинг ҳаракатларига, уларнинг эҳтиёт чораларига тўғри риоя қилишларига боғлиқ.

Ташқи омиллар. Банклар киберхавфсизлигига таҳдид соладиган ташқи омиллар қуйидагилардир: 1) **Credential Stuffing** – кенг қўлланми кириш сўровлари ёрдамида фойдаланувчи ҳисобларига рухсатсиз кириш учун электрон почта идентификаторлари, фойдаланувчи номлари ва пароллар рўйхати ўғирланади; 2) **Social engineering** - компания серверларига кириш учун инсон хатти-ҳаракатларидан фойдаланади. Social engineering ходимларни логин маълумотлари ёки бошқа махфий маълумотларни алмашиш учун манипуляция қилади, улар кейинчалик тармоқни бузиш учун ишлатилади; 3) **фишинг хужумлари** - киберхужумларнинг энг кўп такрорланадиган тури эканлиги эътироф этилган ва сўнгги 30 йилликда ривожланган. Улар логин маълумотларини, кредит карта рақамларини ва бошқа муҳим фойдаланувчи маълумотларини ўғирлаш учун ишлатилади; 4) **malware, malicious software, (зарарли дастур)** - маълумотларга, қурилмаларга ёки одамларга зарар етказиш мақсадида ёзилган ҳар қандай дастурий таъминот. Зарарли дастурлар турларига компьютер вируслари, троянлар, жосуслик дастурлари, тўлов дастурлари, реклама дастурлари, файлсиз зарарли дастурлар ёки гибрид хужумлар киради; 5) **trojans** – компьютер қурилмасига ўрнатилгунга қадар қонуний дастурий таъминот бўлаги сифатида кўриниши мумкин, аммо у онлайн банк тизимлари орқали сақланган ёки қайта ишланадиган махфий маълумотларга кириш учун мўлжалланган зарарли компьютер дастуридир; 6) **ransomware** - кибер-таҳдид бўлиб, унда зарарли дастур муҳим маълумотларни шифрлайди ва эгаларига катта тўлов ёки тўловни тўламагунча киришни имконсиз қилади. Бу банк муассасалари учун жиддий таҳдиддир, чунки 2020 йили барча молия институтларининг 90 фоизи ransomware таҳдидини бошдан кечирган¹; **spoofing** - хакерлар клонлаштирилган сайтлардан фойдаланадилар. Улар имло ёки домен кенгайтмаси бироз ўзгарган домен яратиш ва худди асл нусхасига ўхшаб ишлайдиган веб-сайт ишлаб чиқиш орқали банк веб-сайтига тақлид қилади; **мобил иловалардан келиб чиқадиган хавфлар** - рақамлаштиришнинг кучайиши билан мобил иловалар трендга айланди. Мижозларга хизмат кўрсатишни осонлаштириш учун банклар ўзларининг мобил иловаларини ҳам ишлаб чиқдилар. Қанчалик осон ва вақтни тежайдиган бўлмасин, мижоз иловани ҳар сафар очганида банк технологияси киберхавфсизлик таҳдидига дуч келади ва бошқалар.

Келтирилган ташқи омиллар ичида энг кўп учрайдигани **malware** хужумлари бўлиб, машинали ўрганиш ва мақсадли фишинг электрон почта хабарларининг пайдо бўлиши билан янада мураккаблашди. 2019 йилда банк

¹ The Growing Threat of Ransomware. <https://purplesec.us/resources/cyber-security-statistics/ransomware/>
www.sharqjurnali.uz

секторидаги барча маълумотлар бузилишининг 75 фоизи malware хужумларига тўғри келади.²

Қуйидаги расмда 2009-2018 йилларда malware инфекцияларининг ўсиб бориш графиги келтирилган бўлиб, кўриниб турибдики, 10 йил ичида ўсиш тахминан 65 баробар бўлган.

1-диаграмма

Сўнгги ўн йил ичида malware инфекцияларининг ўсиб бориш графиги (миллион)³



Бугунги кунда, тижорат банкларининг киберҳавсизлигига таъсир этувчи ташқи омиллар турлари ва уларнинг динамикасини баҳолаш, бу омилларга қарши курашда жуда муҳим. Мисол тариқасида, **malware** инфекцияларининг қийматини прогнозлаш масаласини кўриб чиқамиз. Бу масалани Excel дастурида келтирилган тренд чизиклари ва уларнинг аналитик ифодасини аниқлаш опциясидан фойдаланиб, осонгина ҳал қилиш мумкин. Бунинг учун, расмда келтирилган ахборотлардан фойдаланамиз ва моделнинг аниқлигини ошириш учун стандарт қийматларга ўтиб оламиз (жадвал).

² Bitglass 2019 Financial Breach Report: More than 60% of All Leaked Records in Past Year Exposed by Financial Services Firms. <https://www.businesswire.com/news/home/20191216005207/en/Bitglass-2019-Financial-Breach-Report-60-Leaked>

³ 2021 Cyber Security Statistics

The Ultimate List Of Stats, Data & Trends. <https://purplesec.us/resources/cyber-security-statistics/>

1-жадвал

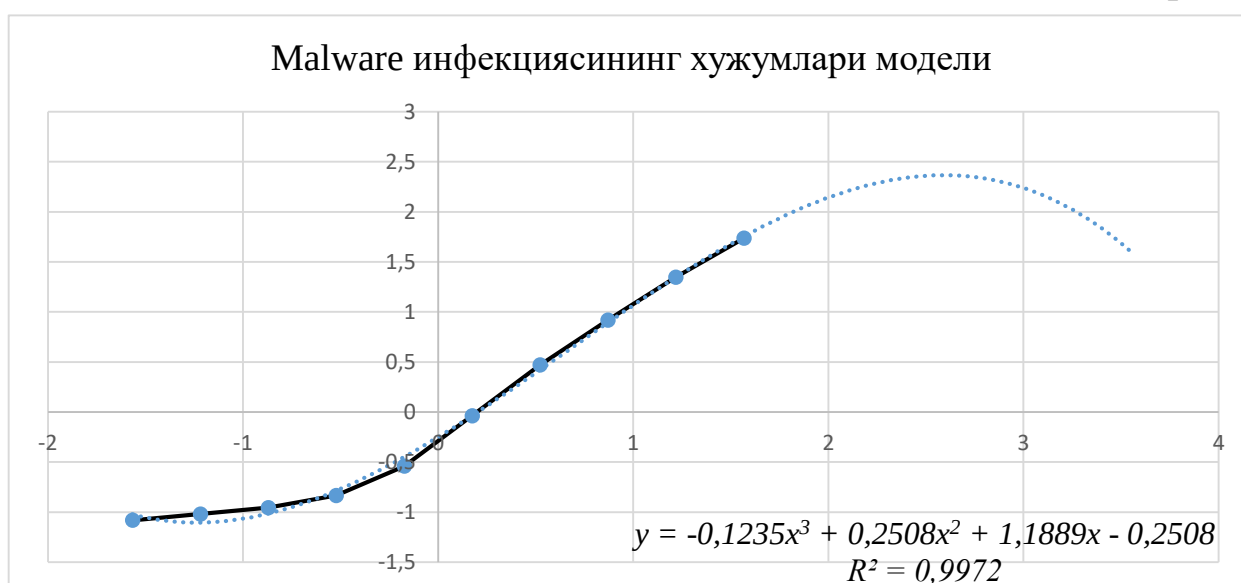
2009-2018 йилларда malware инфекцияси

№	Йил	Хужумлар сони, млн	Стандарт қийматлар		Хисоб натижалари	Фарқ, %
			йил, x	Хужумлар сони, y		
1	2009	12.4	-1.57	-1.08	-1.02	5.40
2	2010	29.97	-1.22	-1.02	-1.10	8.25
3	2011	48.17	-0.87	-0.96	-1.01	6.15
4	2012	82.62	-0.52	-0.83	-0.79	5.81
5	2013	165.81	-0.17	-0.54	-0.45	6.96
6	2014	308.96	0.17	-0.04	-0.04	1.49
7	2015	452.93	0.52	0.47	0.42	7.32
8	2016	580.4	0.87	0.92	0.89	2.77
9	2017	702.06	1.22	1.35	1.35	0.04
10	2018	812.67	1.57	1.74	1.75	0.97

Олинган натижалар

Ўтказилган ҳисоб-китоблар натижасида хужумлар сони (y) ва бу хужумлар амалга оширилган йил (x) ўртасида 2-расмда келтирилган функционал боғланиш ҳосил қилинди. Расмдаги пунктирли чизиқ (тренд чизиғи) моделдан олинган натижалар асосида қурилган бўлиб, фарқ энг кўпи билан 8,25 % ни ташкил қилди. Ҳосил қилинган боғланиш, malware инфекциясидан хужумлар ўтказиш 2020 йилда энг кўп бўлган бўлиб (989.8 млн), ундан кейинги йилларда хужумлар сонининг камайиш тенденцияси мавжудлигини кўрсатмоқда. Масалан, 2022 йилда – 955.5 млн., 2023 йилда эса бу кўрсаткич 799.1 млн ни ташкил қилиши мумкин.

2-диаграмма



Хулоса

Юқоридаги таҳлилдан шундай хулоса қилишимиз мумкинки, киберхавсизлик масаласи тобора катта аҳамият касб этаяпти ва керакли амалиётлар ҳам бажарилмоқда. Биз тузган математик моделга асосан 2023 йилга келиб malware хужумлари камайиши кутилмоқда бу шундан далолат берадики, бутун дунё бўйлаб киберхавсизликни таъминлашга қаратилган кенг кўламли ишлар амалга оширилмоқда ва булари самара бериши кутилмоқда. Юқорида банк киберхавсизлигига таъсир этувчи ички ва ташқи омиллар ҳақида маълумот бердик, ҳўш буларнинг қайси бири хавфлироқ? Уларнинг хаммаси ҳам бир хил даражада хавфли, аммо бу соҳа ва қандай маълумот олинганига боғлиқ. Келтирилган усулдан фойдаланиб, ҳар бир омил учун модель яратилса, у ҳолда бу омилларга қарши курашиш самарадорлиги, яъни тижорат банклари хавфсизлигини ошириш мумкин.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Bitglass 2019 Financial Breach Report: More than 60% of All Leaked Records in Past Year Exposed by Financial Services Firms. <https://www.businesswire.com/news/home/20191216005207/en/Bitglass-2019-Financial-Breach-Report-60-Leaked>
2. 2021 Cyber Security Statistics the Ultimate List of Stats, Data & Trends. <https://purplesec.us/resources/cyber-security-statistics/>
3. ISO/IEC 27032:2012 “Ахборот технологиялари - Хавфсизлик техникаси - Киберхавфсизлик бўйича кўрсатмалар”
4. Marcel, Sébastien. Handbook of Biometric Ахборот воситаларининг кибер хавфсизликдаги ўрни. nti-Spoofing. London. England.2017
5. Безкоровайный М.М., Лосев С.А., Татузов А.Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь.
6. Математическая статистика. Учебник | Ивченко Григорий Иванович, Медведев Юрий Иванович. 2020 г.