РАҚАМЛИ ИҚТИСОДИЁТ ШАРОИТИДА БАНКЛАР МОЛИЯВИЙ БАРҚАРОРЛИГИНИ КУЧАЙТИРИШДА КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ МАСАЛАЛАРИ

Олтаев Ш.С. – *СамИСИ доценти, и.ф.н.*

Аннотация. Мақолада рақамли молиявий хизматлар кенгайиши шароитида банк тизими молиявий барқарорлигига таҳдид солаётган киберхатарлар таҳлил қилинган. Киберхатарларнинг моҳияти, уларнинг асосий турлари ҳамда банк тизимига кўрсатаётган салбий таъсири ёритилган. Халқаро ташкилотлар томонидан ишлаб чиқилган киберхавфсизликни таъминлаш бўйича меъёрий ҳужжатлар ва ёндашувлар ўрганилган. Шунингдек, киберхавфсизликни мустаҳкамлаш орқали банк тизими барқарорлигини таъминлашга қаратилган стратегик йўналишлар асослаб берилган. Мақолада Ўзбекистон Республикаси банк тизимида киберхавфсизликни кучайтириш бўйича амалга оширилаётган чора-тадбирлар ва келгусидаги устувор вазифалар илмий жиҳатдан таҳлил қилинган.

Калит сўзлар: киберхатар, киберхавфсизлик, банк тизими, молиявий барқарорлик, рақамли молиявий хизматлар, киберҳужум, молиявий риск.

Сўнгги йилларда рақамли технологияларнинг жадал ривожланиши банк тизими фаолиятида янги имкониятлар билан бир қаторда янги хатарларни ҳам вужудга келтирмоқда. Айниқса, рақамли молиявий хизматларнинг кенгайиши киберҳужумлар сони ва кўламининг ортишига сабаб бўлиб, банк тизими молиявий барқарорлиги учун жиддий таҳдид сифатида намоён бўлмоқда.

Киберхатарлар банклар фаолиятида ахборот тизимларига ноқонуний кириш, молиявий маълумотларни ўғирлаш, пул маблағларини ноқонуний ўзлаштириш ҳамда мижозлар ишончининг пасайишига олиб келиши мумкин. Шу боис, банк тизимида киберхавфсизликни таъминлаш ва киберхатарларни

бошқариш масалалари молиявий барқарорликни сақлашнинг муҳим омилига айланмоқда.

Маълумки, киберхатар банклар молиявий барқарорлиги учун янги хатар турларидан бири бўлиб ҳисобланади. Сўнгги ўн йилликда рақамли молиявий хизматларнинг кенгайиши киберҳужумларнинг уч бараварга ошишига олиб келган.

Киберхатар бу киберҳудудда банк тизими манфаатларига салбий таъсир кўрсатиши мумкин бўлган эҳтимолий хатарлар ёки омиллардир.

Халқаро тажрибани таҳлил қилиш шуни кўрсатадики, банк тизими учун қуйидаги киберхатар турларини келтириш мумкин: биринчидан, техник аппаратларнинг кучсиз жиҳатлари орқали киберҳужум - турли ишлаб чиқарувчиларнинг микропроцессорлари кучсиз жиҳатларини мавжуд дастурий янгилаш ёрдамида олдини олиш имкони бўлмаган ҳолатларда, бу кибержиноятчилар учун киберҳужум имкониятига айланмоқда; иккинчидан, компьютер шпионажи - молиявий ташкилотнинг фаолиятига айғоқчилик қилиш мақсадида, муҳим маълумот инфратизими объектларида узоқ вақт мавжуд бўлишга қаратилган фаолият; учинчидан, мақсадли киберҳужумлар - аниқ бир молиявий ташкилотга қаратилган ҳужум бўлиб, ташкилотнинг тармоғига кириб, пул маблағларини уғирлашга қаратилган ҳаракатлар; тўртинчидан, мижозга йўналтирилган киберҳужумлар - банкнинг мижозларига қаратилган бўлиб, уларнинг шахсий маблағларини ўғирлашга қаратилган.

Халқаро ташкилотлар ва турли давлатларнинг тартибга солувчи органлари банк тизимида киберхавфсизликни таъминлаш масаласига катта эътибор қаратмоқда. Ҳозирги пайтда жаҳон тажрибасида киберхавфсизликни таъминлаш бўйича тизимли ёндашувлар, киберхатарни бошқариш бўйича қуйидаги қонунчилик ҳужжатлари ишлаб чиқилган: биринчидан, тўловлар ва бозор инфратузилмаси бўйича қўмита ҳамда қимматли қоғозлар бўйича

Халқаро ташкилот томонидан 2016 йил июнда ишлаб чиқилган “Молия бозори инфратузилмалари учун кибермустаҳкамлик бўйича қўлланма” (CPMI-IOSCO: Guidance on cyber-resilience for financial market infrastructures, June 2016); иккинчидан, 2017 йил августдаги Молиявий барқарорлик Институти ҳужжати “Банкларда киберхавфсизликни таъминлаш тизимини кучайтириш бўйича тартибга солувчи ёндашувлар”, (Financial Stability Institute: FSI Insights on policy implementation № 2 ”Regulatory approaches to enhance banks’ cybersecurity frameworks, August 2017); учинчидан, жаҳон банкининг 2017 йил октябрдаги ҳужжати “Молия тизими киберхавфсизлиги: регуляторлар дайжести”, (World Bank Group: Financial Sector’s Cybersecurity: A Regulatory Digest, October 2017); тўртинчидан, жаҳон банки томонидан 2018 йилда ишлаб чиқилган ҳужжат “Молия тизими киберхавфсизлиги: қоидалар ва тартибга солиш”, (World Bank Group: Financial Sector’s Cybersecurity: Regulations and Supervision, 2018); бешинчидан, банк назорати бўйича Базель қўмитаси томонидан 2018 йил декабрда ишлаб чиқилган ҳужжат “Киберхавфсизлик: тажриба шарҳи”, , Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018).

Австралия, Канада, Буюк Британия, Евроиттифоқ мамлакатлари, Америка Қўшма Штатлари, Швейцария, Сингапур, Белорусия каби давлатларнинг банк тизимини тартибга солувчи органлари томонидан, банк тизимида киберхавфсизликни таъминлаш принципларига талаблар ва киберхатарни бошқаришга ёндашувлар ишлаб чиқилган.

Молиявий ва технологик алоқанинг кучли эканлиги сабабли бир йирик банк тизимига қилинган ҳужум бутун молия тизимига тез тарқалиши ва тизимнинг кенг қамровда ишдан чиқишига, мижозларнинг ишончи йуқолишига олиб келиши мумкин.

Қуйидаги расмдан, Халқаро валюта фонди томонидан тақдим этилган маълумотларга киберҳужумлар динамикасини кўриш мумкин. Бундай киберҳужумлар сони сўнгги йилларда кескин ошган.

Рақамли технологияларнинг ривожланиши, бир томондан хакинг воситаларининг арзонлашуви ҳамда такомиллашувига ҳам олиб келмоқда. Мобил қурилмаларда пул маблағларини бошқариш билан боғлиқ ягона платформаларнинг кенг ишлатилиши хакерлар учун кенгроқ имконият яратмоқда.

Киберҳужумларни бир мамлакат доирасидаги хатар деб ҳисоблаш нотўғри бўлади, чунки хакерлар турли мамлакатлар доирасида фаолият кўрсатиш имконига эга. Шундан келиб чиқиб, кибержиноятларга қарши кураш халқаро даражадаги ечимини топиши лозим бўлган масала бўлиб ҳисобланади.

Шунингдек, юқоридаги маълумотлар киберҳужумлар натижасида ҳимоясиз қолаётган маълумотлар сони ҳам сўнгги йилларда сезиларли равишда ошганини кўрсатади.

Халқаро валюта фонди олиб борган тадқиқотларда киберхавфсизликни кучайтириш ва молиявий барқарорликни мустаҳкамлаш учун қуйидаги олти асосий стратегия таклиф қилинган :

1. Киберхатар картаси ва рискни миқдорий баҳолаш

Жаҳон молия тизими ўзаро алоқасининг турли жиҳатларини асосий операцион ва технологик ҳамда инфратизимнинг муҳим объектлари ҳамкорлиги картасини яратиш орқали яхшироқ англаш мумкин. Банкларнинг молиявий барқарорлигини таҳлил қилишда киберхатарни баҳолаш сифатини ошириш умумий тизимли рискни тушунишга ва уни камайтиришга имкон беради. Эҳтимолий оқибатларни миқдорий баҳолаш аниқ бир мавжуд муаммога жавоб чора-тадбирларини ишлаб чиқишга ва уни ҳал қилишга ёрдам беради. Кибержиноятларнинг оқибатлари тўғрисида маълумотларнинг етарли

эмаслиги ва моделлаштиришнинг қийинчилиги ушбу соҳадаги ишларни секинлаштирмоқда дея оламиз.

2. Тартибга солиш ва назоратни кучайтириш

Марказий банклар томонидан назорат қилиш ва тартибга солиш ишларини халқаро даражада келишилганлиги даражасини ошириш қонунчилик талабларига риоя этилиши ва янада яқин трансчегаравий ҳамкорликни йўлга қўйиш бўйича харажатларни камайтиришга имкон беради. Молиявий барқарорлик Кенгаши, Тўлов ва бозор инфратузилмалари масалалари бўйича Қўмита, Банк назорати бўйича Базель Қўмитаси каби халқаро ташкилотлар тизимни тартибга солишда ҳамкорлик ва бошқарувни мустаҳкамлаш бўйича ишлар олиб бормоқда. Турли мамлакатларнинг расмий органлари ушбу халқаро ташкилотлар билан ҳамкорликда киберхавфсизлик масалаларида ҳамкорлик қилишлари мақсадга мувофиқ бўлиб ҳисобланади.

3. Жавоб чора-тадбирларини амалга ошириш имкони

Киберҳужумлар сони ортиб бораётгани сабабли банклар молиявий барқарорлигини сақлаб қолиш мақсадида тизим фаолиятини оператив равишда янгилаш ва қайта тиклаш имконига эга бўлиши лозим. Бунда киберҳужумларга жавоб бериш ва қайта тикланиш стратегиясини ишлаб чиқиш кўзда тутилади. Трансчегаравий молия ташкилотлари киберҳужумларга жавоб бериш ва қайта тикланиш стратегиясини ишлаб чиқиши учун халқаро механизмлар талаб қилинади.

4. Маълумотларни бўлишишга тайёрлик

Киберхавфлар, ҳужумлар, уларни бартараф этиш чора-тадбирлари тўғрисида маълумотлар алмашинуви ортиши киберҳужумларга жавоб бериш бўйича самарали чора-тадбирлар ишлаб чиқишга имкон беради. Аммо миллий хавфсизлик ва маълумотлар ҳимояси масалаларида бу йўналишда жиддий тўсиқлар сақланиб қолмоқда. Тартибга солувчи органлар ва марказий банклар маълумотлар алмашинуви усуллари бўйича тартибга солувчи ҳужжатларни

ишлаб чиқишлари талаб қилинади. Бундай чора-тадбирлар ишончли тармоқларнинг кенгайиши, глобал даражада маълумотлар алмашинувига имкон яратади.

5. Чеклаш чора-тадбирларини кучайтириш

Кибержиноят натижасида олинган даромадларни мусодара қилиш, жиноятчиларни жиноий жавобгарликка тортиш каби самарали чора-тадбирлар ёдамида киберҳужумларни камайтириш масалалари кўриб чиқилиши лозим. Бунинг учун тартибга солувчи органлар ва ҳуқуқ тартибот органлари ҳамкорлиги кучайтирилиши талаб қилинади.

6. Тартибга солувчи ташкилотларнинг киберхавфсизлик салоҳиятини ошириш

Киберхавфсизлик масаласида тартибга солувчи органлар салоҳиятини оширишда халқаро ташкилотлар билан ҳамкорлик қилиш молиявий барқарорликни мустаҳкамлаш ва молиявий интеграцияни қўллаб қувватлашга имкон беради.

Юқоридагилардан хулоса қилиб шуни айтиш мумкинки, Ўзбекистон Республикаси банк тизими молиявий барқарорлигини таъминлашда киберхатарларнинг олдини олиш долзарб вазифалардан бири бўлиб ҳисобланади. Шуни таъкидлаш лозимки, банклар фаолиятида рақамли технологияларни кенг жорий этиш ҳамда тижорат банкларини хусусийлаштириш борасида белгиланган устувор вазифаларда Марказий банк ҳузуридаги банк ва молия-кредит соҳасида ахборот ва киберхавфсизлик таҳдидларининг олдини олиш ҳамда молиявий фирибгарликларга қарши таъсир чораларини кўриш ва текшириш (FINCERT) маркази ташкил этилиши назарда тутилган.

Келгусида банк тизими молиявий барқарорлигини мустаҳкамлашда киберхавфсизликни кучайтириш борасидаги устувор йўналишлар сифатида қуйидагиларни келтириш ўринли: биринчидан, Марказий банкда банк ва

молия-кредит соҳасида ахборот ва киберхавфсизлик таҳдидларининг олдини олиш ҳамда молиявий фирибгарликларга қарши таъсир чораларини кўриш ва текшириш (FINCERT) марказини ташкил этиш баробарида ушбу марказнинг фаолиятида ҳамдўстлик мамлакатларининг тартибга солувчи органлари билан ҳамкорлик ўрнатишига ва киберхавфлар, ҳужумлар, уларни бартараф этиш чора-тадбирлари тўғрисида маълумотлар алмашинувини йўлга қўйиш; иккинчидан, банк тизимида киберхавфсизликни таъминлаш Концепциясини ишлаб чиқиш ва қонунчилик нормативларини мустаҳкамлаш; учинчидан, ҳуқуқ тартибот органлари билан ҳамкорликда кибержиноят натижасида олинган даромадларни мусодара қилиш, кибержиноят субъектларини жиноий жавобгарликка тортиш каби самарали чора-тадбирлар ёрдамида киберҳужумларни камайтириш масалалари кўриб чиқилиши лозим.

Фойдаланилган адабиётлар рўйхати:

1. Гарнаева М.А., Функ К. Kaspersky security bulletin 2013 // Вопросы кибербезопасности. 2014. №3. С.65-68

2. Сидоренко Е. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений [Электронный ресурс] // Официальный сайт газеты Известия - Режим доступа: https://iz.ru/962966/ elena-sidorenko/potcifrovym-sledam-v-rf.

3. Центр политического анализа и информационной безопасности [Электронный ресурс] // Режим доступа: http://centerpolit.ru/content.

4. https://cbu.uz

5. https://www.imf.prg/ru/Blpgs/Articles/2020/12/07/blpg-cyber-risk-is-the-new-thregt-tp- financial-stability.

6. Ўзбекистон Республикаси Президентининг 28.01.2022 йилдаги "2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида"ги №ПФ-60 сонли Фармони // https://lex.uz/.

7. Емелина А.А. “Организация кибербезопасности”// Фундаментальные основы инновационного развития науки и образования// сборник статей VI Международной научно-практической конференции : в 3 ч.. Том Часть 1. 2019.

8. O'zbekiston respublikasi oliy va o'rta maxsus ta'lim vazirligi Mirzo Ulug'bek nomidagi O'zbekiston milliy universiteti iqtisodiyot fakulteti. "Moliya va soliqlar" ma' ruzalar kursi. Toshkent - 2012 yil.