ISSN: 2181-3906 2023

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 2 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

МАМЛАКАТ БАНК ВА МОЛИЯ ТИЗИМИГА КИБЕРТАҲДИДЛАРНИНГ ТАЪСИРИ

Зуҳра Маратдаевна Отакузиева
Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети, и.ф.н., доцент, Ташкент, Узбекистан.
Email: zukhra.otakuzieva@mail.ru
ORCID ID: 0000-0002-4283-8181
Исроилов Жавохирбек Абдуғаффор ўғли
Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети, Киберхавфсизлик факултети, Ахборот хавфсизлиги йўналиши 3-курс талабаси,
Email: javokhirbekisroilov166@gmail.com
https://doi.org/

Аннотация. *Ушбу мақолада дунёдаги кўплаб мамлакатлар банк ва молия тизимларига кибертаҳдидлар таъсири оқибатида юз берадиган салбий жиҳатлар батафсил статистика маълумотлари асосида кўрсатиб берилган. Жумладан уларга кибертаҳдидлар сабабли молиявий йўқотишлар, банк ва молия тизими обрўйига етказиладиган зарарлар, иш жараёнида келиб чиқадиган носозликлар, меъёрий талабларга мувофиқ келмасликни ва бошқаларни киритишимиз мумкин. Бундан ташқари, дунё мамлакатлари бугунги кунда қандай самарали киберхавфсизлик сиёсати олиб боришлари мумкинлиги ва қандай қоидалар ишлаб чиқишлари кераклиги ҳақида мақолада фикр юритилади.*

Калит сўзлар: *кибертаҳдид, банк ва молия тизимлари, молиявий йўқотишлар, кибержиноятчилар, молиявий операциялар, ахборот хавфсизлиги.*

THE EFFECT OF CYBER THREATS ON THE COUNTRY'S BANKING AND FINANCIAL SYSTEM

Abstract. *This article shows how detailed statistics reveal the negative aspects of the banking and financial systems of many countries in the world due to the impact of cyber threats. These negative aspects include financial losses due to cyber threats, damage to the reputation of the banking and financial system, malfunctions in the work process, non-compliance with regulatory requirements, and others. Additionally, the article discusses how countries around the world can develop effective cybersecurity policies.*

Keywords: *cyber threat, banking and financial systems, financial losses, financial transactions, information security, national security, cybersecurity costs, cybersecurity policy.*

ВЛИЯНИЕ КИБЕРУГРОЗ НА БАНКОВСКО-ФИНАНСОВУЮ СИСТЕМУ СТРАНЫ

Аннотация. *В данной статье на основе подробных статистических данных показаны негативные стороны воздействия киберугроз на банковско-финансовые системы многих стран мира. К их числу можно отнести финансовые потери из-за киберугроз, ущерб репутации банковско-финансовой системы, сбои в рабочем процессе, несоблюдение нормативных требований и другие. Кроме того, в статье рассматривается, как страны всего мира могут и должны сегодня разработать эффективную политику кибербезопасности.*

Ключевые слова: *киберугроза, банковско-финансовые системы, финансовые потери, киберпреступники, финансовые операции, информационная безопасность.*

INTRODUCTION

Бугунги кунда кибертаҳдидлар бутун дунё бўйлаб банк ва молия тизимлари учун жиддий муаммога айланди. Кибертаҳдидларнинг мамлакат банк ва молия тизимига таъсири жиддий бўлиши мумкин, бу молиявий йўқотишлардан тортиб обрўга путур этказиши ва ҳатто муҳим инфратузилманинг бузилишигача олиб келиши мумкин. Интернетда қанчалик кўп молиявий операциялар амалга оширилса, киберҳужумлар хавфи шунчалик юқори бўлади.

MAIN PART

Мамлакатнинг банк ва молия тизимига таъсир қилиши мумкин бўлган кибертаҳдидлар йўқотишларидан бири бу молиявий йўқотишлар ҳисобланади. Кибержиноятчилар банк ҳисоб варақларидан пул ўғирлашлари, молиявий маълумотларни манипуляция қилишлари ва жисмоний шахслар ва молия институтлари учун катта молиявий йўқотишларга олиб келадиган фирибгарлик фаолияти билан шуғулланишлари мумкин. 2021 йилда кибертаҳдид альянси Cyber Threat Intelligence Estimate томонидан келтирилган маълумотларига кўра, 2020 йилда молия секторига қарши кибержиноятлар 17 фоизга ошган. IBMнинг маълумотлар тарқалиб кетиши ҳақидаги ҳисоботига кўра, 2020 йилда бутун дунё бўйлаб молиявий институтлар учун маълумотлар бузилишининг ўртача қиймати 5,85 миллион долларни ташкил этди. Банк ва молия тизимларида киберҳужумлар ортидан келадиган зарарлардан яна бирига уларнинг обрўсига путур етаётганликни киритиш мумкин. Киберҳужумлар банклар ва молия институтларининг обрўсига ҳам путур этказиши мумкин. Агар киберҳужум молиявий йўқотиш ёки маълумотлар чиқиб кетишига олиб келса, мижозлар банк еки молия муассасасига ишончини йўқотишлари ва натижада бизнес ва даромад йўқолишига олиб келиши мумкин.

Киберҳужум оқибатида банк ёки молия институти иш фаолияти техник жиҳатдан бузилиши мумкин, бу эса хизмат кўрсатишда узилишлар ва кечикишларга олиб келади. Бунда мижозлар ўз ҳисобларига киришлари ва молиявий операцияларни амалга оширишлари борасида муаммоларга дуч келишлари мумкин, бу эса охиргиларнинг умидсизликка тушишига ва содиқлигининг йўқотишига олиб келади.

Бундан ташқари, банклар ва молия институтлари қатъий тартибга солиш талабларига риоя қилишлари шарт ва бунда маълумотларнинг бузилиши ёки бошқа хавфсизлик ҳодисаларига олиб келадиган киберҳужум тартибга солувчи органлар томонидан жарима ёки санкцияларга олиб келиши мумкин.

Кибертаҳдидлар мамлакатнинг банк ва молия тизимига яна қандай таъсир қилиши мумкинлиги ҳақида қўшимча маълумотлар келтириб ўтишни мақсадга мувофиқ деб ҳисоблаймиз:

- тизимли хавф. Йирик молия институтига киберҳужум мамлакатнинг бутун банк ва молия тизими учун тизимли оқибатларга олиб келиши мумкин. Мисол учун, агар йирик банк киберҳужумга учраса, бу унинг транзакцияларни қайта ишлаш қобилиятига таъсир этса, бу клиринг ва ҳисоб-китоб хизматлари учун ушбу банкка таянадиган бошқа банклар

ва молия институтларига таъсир қилиши мумкин. Бу молиявий бузилишлар ва йўқотишларнинг домино эффектига олиб келиши мумкин.

- юридик жавобгарлик. Молиявий институтлар киберҳужумлар натижасида етказилган зарар учун қонуний жавобгарликка тортилишлари мумкин. Бунга мижозлар томонидан етказилган зарарлар, шунингдек, молиявий хизматлар учун зарар кўрган муассасага таянадиган бошқа молия институтлари ёки корхоналар томонидан етказилган зарарлар киради.

- миллий хавфсизликка таъсири. Банклар ва молия институтларига киберҳужумлар миллий хавфсизликка ҳам таъсир қилиши мумкин. Мисол учун, мамлакатнинг молиявий тизимини бузадиган киберҳужум мамлакатнинг халқаро савдо ва молиялаштириш қобилиятига таъсир қилиши, иқтисодий ва геосиёсий оқибатларга олиб келиши мумкин.

Бугунги кунда банклар ва молия институтлари ўз тизимлари ва маълумотларини кибер таҳдидлардан ҳимоя қилиш учун киберхавфсизликка катта маблағ сарфлашлари керак бўлади. Бу шифрлаш ва ҳужумларни аниқлаш тизимлари каби хавфсизлик чораларини амалга оширишни ўз ичига олади. Аммо айтиб ўтиш жоизки, ушбу чора-тадбирлар қимматга тушиши ва киберхавфсизлик харажатлари молиявий институтлар, айниқса кичикроқ ташкилотлар учун катта юк бўлиши мумкин.

CONCLUSION

Умуман олганда, кибертаҳдидларнинг мамлакат банк-молия тизимига таъсири сезиларли бўлиши мумкин. Молиявий институтлар ушбу салбий таъсирларнинг олдини олиш учун ўз тизимлари ва мижозлар маълумотларини кибертаҳдидлардан ҳимоя қилиш учун доимий ва фаол равищда чоралар кўришлари керак булади.

Шундай қилиб, кибер таҳдидларнинг мамлакатнинг банк ва молия тизимига таъсири кенг қамровли ва муҳим бўлиши мумкин. Молиявий институтлар киберхавфсизликка жиддий ёндашишлари ва ўз тизимлари ва маълумотларини кибер таҳдидлардан ҳимоя қилиш учун кучли хавфсизлик чораларини кўришлари керак. Бундан ташқари, ҳукуматлар ва тартибга солувчилар банк ва молия тизимларига киберҳужумлар хавфини юмшатиш учун самарали киберхавфсизлик сиёсати ва қоидаларини яратиш учун биргаликда ишлаши керак бўлади.

REFERENCES

1. Global Economic Forum. The Global Risks Report 2017. 12th Edition [Электронный ресурс]. URL: http://wef.ch/risks2017.
2. Kopp E., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability. Working Paper, 2017. International Monetary Fund. [Электронный ресурс]. URL: https://www.imf.org/~/media/F iles/Publications/WP/2017/wp17185.ashx.
3. Peters Gereth W., Shevchenko P. V., Cohen D. R., Maurice D. Understanding Cyber Risk and Cyber Insurance, FinTech: Growth and Deregulation. [Электронный ресурс]. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3065635.
4. Cebula J. J., Young L. R. A Taxonomy of Operational Cyber Security Risks, Carnegie Mellon University. [Электронный ресурс]. URL: https://www.sei.cmu.edu/reports/10tn028.pdf.

5. Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures. June 2016. [Электронный ресурс]. URL: https://www.bis.org/cpmi/publ/d146.htm.
6. Federal Bureau of Investigation, Internet Crime Report. 2016. [Электронный ресурс]. URL: https://pdf.ic3.gov/2016_IC3Report.pdf.
7. Eling M. What do we know about cyber risk and cyber risk insurance? // The Journal of Risk Finance. 2017. Iss. 5. P. 474-491.