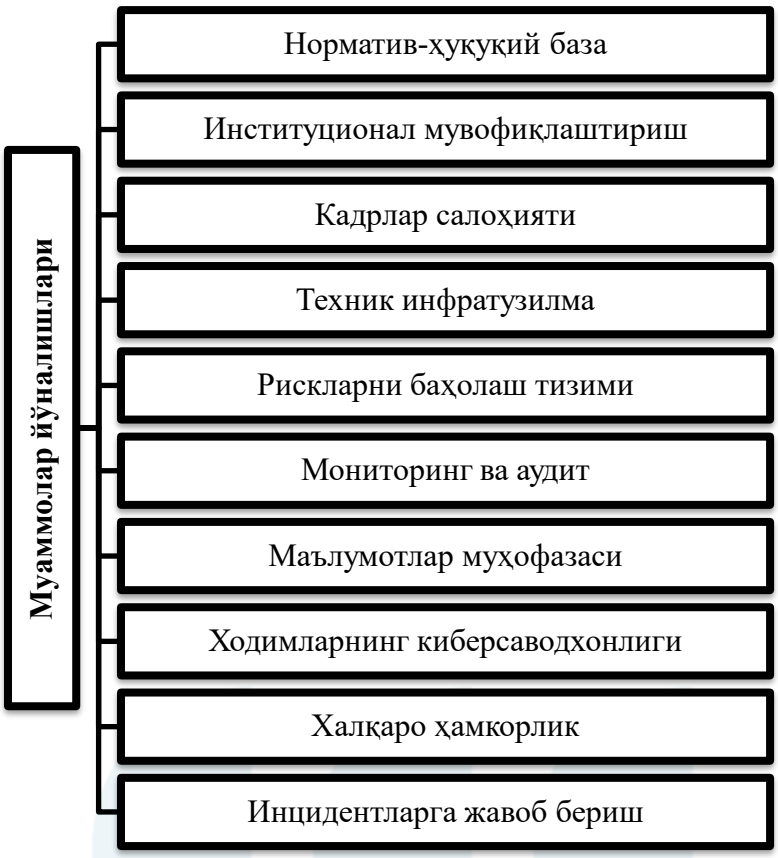
КИБЕРЖИНОЯТ РИСКЛАРИНИ СТРАТЕГИК БОШҚАРИШ МЕХАНИЗМИ АМАЛ ҚИЛИШИДАГИ МАВЖУД МУАММОЛАР

Хасанов Умиджон Юсупович
Бухоро давлат университети
мустақил тадқиқотчиси
https://doi.org/10.5281/zenodo.20953883

Ўзбекистон Республикасида давлат бошқарувини рақамлаштириш жараёнларининг жадал ривожланиши рақамлаштирилган давлат хизматларини кўрсатиш, маълумотлар алмашинуви ва бошқарув қарорларини қабул қилишда ахборот-коммуникация технологияларининг аҳамиятини кескин ошириши билан биргаликда, рақамли трансформация жараёнлари давлат ахборот тизимлари ва ресурсларига нисбатан кибержиноятлар, ахборот ўғирланиши, маълумотлар базаларига рухсатсиз кириш, зарарли дастурлар тарқалиши ҳамда давлат инфратузилмасига нисбатан кибертаҳдидлар кўламини ҳам кенгайтирмоқда. Бу турдаги кибертаҳдидлар кўлмининг кенгайиши ўз навбатида мамлакат давлат бошқаруви тизимида кибержиноят рискларини стратегик бошқариш механизми амал қилиши билан боғлиқ бўлган тизимли муаммоларни ҳам вужудга келтириши мумкин бўлади.

Бугунги Ўзбекистон шароитида мамлакат давлат бошқаруви тизимида кибержиноят рискларини стратегик бошқариш амалиёти самарадорлигига салбий таъсир кўрсатувчи омилларни аниқлашга эришдик. Таҳлилларга кўра, бу турдаги муаммолар норматив-ҳуқуқий база, институционал мувофиқлаштириш, кадрлар салоҳияти, техник инфратузилма, рискларни баҳолаш тизими, мониторинг ва аудит, маълумотлар муҳофазаси, ходимларнинг киберсаводхонлиги, халқаро ҳамкорлик ва инцидентларга жавоб бериш каби (1-расмга қаранг) йўналишларда намоён бўлмоқда. Юқорида келтириб ўтилган муаммоларнинг мамлакат двлат бошқаруви тизимида кибержиноят рискларини страатегик бошқариш таъсир доираларини таҳлил қилиш орқали улаарнинг тўлиқ моҳиятини англаб етиш мақсадида ҳар бир муаммо йўналишлари кесимида таҳлилларни (7-иловага қаранг) амалга оширишни лозим топдик. Бу орқали кейинги йилларда мамлакатда кибержиноят рискларини стратегик бошқариш механизми амал қилиши самарадорлигини оширишга эришилади.



1-расм. Ўзбекистонда кибержиноят рискларини стратегик бошқариш амалиётидаа намоён бўлаётгаан муаммоларнинг йўналишлари[1]

Ўзбекистон давлат бошқаруви тизимини рақамлаштирилиши ҳисобига электрон ҳукумат платформалари, давлат маълумотлар базалари, идоралараро рақамли интеграция ҳамда давлат хизматларининг электрон шаклга ўтиши киберхавфсизликни давлат бошқарувининг муҳим таркибий элементига айланиши шароитида рақамли инфратузилманинг жадал ривожланиши кибержиноят рискларини ҳам орттириб, мазкур соҳада самарали ҳуқуқий тартибга солиш заруратини юзага келтирмоқда. Бу эса мамлакатда амал қилаётган кибержиноят рискларини стратегик бошқаришнинг норматив-ҳуқуқий база билан боғлиқ бўлган муаммоларни вужудга келишига сабаб бўлмоқда.

Таҳлиллар шуни кўрсатадики, Ўзбекистон давлат бошқаруви тизимида ахборот технологияларининг кенг жорий этилишига қарамасдан, айрим давлат органларида техник инфратузилманинг ҳимоя даражаси бир хил эмас. Айниқса, эскирган сервер архитектуралари, лицензияланмаган ёки мунтазам янгиланмайдиган дастурий таъминот, марказлашган хавф мониторинги механизмларининг тўлиқ жорий этилмаганлиги кибертаҳдидлар таъсирчанлигини кучайтирувчи омил сифатида намоён бўлмоқда. Техник инфратузилманинг заифлиги давлат бошқарувига қуйидаги иқтисодий ва институционал салбий таъсирларни келтириб чиқариши мумкин:

давлат хизматлари кўрсатилишида узилишлар;

давлат маълумотларининг йўқолиши ёки тарқалиши;

[1] Муаллиф томонидан тузилган

ахборот тизимларини тиклаш учун бюджет харажатларининг ортиши;

фуқароларнинг рақамли давлат хизматларига ишончи пасайиши;

миллий рақамли иқтисодиёт барқарорлигига таҳдид юзага келиши.

Шу нуқтаи назардан, давлат бошқаруви тизимида кибержиноят рискларини бошқаришнинг стратегик самарадорлигини ошириш учун давлат ахборот тизимларини тўлиқ техник аудитдан ўтказиш, SOC ва SIEM тизимларини марказлаштирилган ҳолда жорий қилиш, муҳим давлат ахборот инфратузилмаси учун Zero Trust архитектурасини босқичма-босқич татбиқ этиш, ахборот тизимларини импортга қарам бўлмаган хавфсиз миллий платформалар асосида модернизация қилиш каби чораларни кўриш мақсадга мувофиқ, деб ҳисобланади.

Adabiyotlar, References, Литературы:

1. Ўзбекистон Республикасининг “Давлат сирлари тўғрисида”ги ЎРҚ-1016-сон Қонуни, 27.12.2024 й.

2. Ўзбекистон Республикасининг “Ахборотлаштириш тўғрисида”ги 560-II-сон Қонуни, 11.12.2003 й.

3. International Telecommunication Union (ITU). URL: https://www.itu.int/en/Pages/default.aspx

4. Global Cybersecurity Index 2024. 5th Edition. ITU Publications, International Telecommunication Union, Geneva, 2024. – 139 pages.

5. National Institute of Standards and Technology (NIST) URL: https://www.nist.gov/

6. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, Feb., 2024. – 27 pages. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf