Азимов Рустам Содиқович
“Ўзбекинвест экспорт-импорт суғурта компанияси” АЖ
Бош директори, и.ф.н.

ИҚТИСОДИЁТНИ РАҚАМЛАШТИРИШ ШАРОИТИДА КИБЕР-РИСКЛАРНИ СУҒУРТАЛАШ МАСАЛАЛАРИ

Аннотация. *Рақамлаштириш жараёни тезлашиши натижасида кибер хавфлар, кибер таҳдидлар, кибер жиноятлар инсониятнинг хавфли душманига айланди. Кибер рискларни аниқлаш, котегорияларга бўлиб таснифлаш орқали рискларни баҳолаш, кибер жиноятларга қарши курашиш, суғурта пакетлари орқали ҳимояланиш ва етиши мумкин бўлган зарарларни олдини олиш, корхонада хавфсизликни таъминлаш чораларини кўриш, ички тизимда маълумотлар хавфсизлигини таъминлаш, давлат миқиёсида ахборот хавфсизлигини таъминлаш чораларини кўриш фонида кибержиноятчиликка қарши ҳимоя деворини яратиш бугунги куннинг долзарб масаласи ҳисобланади. Ушбу мақола кибер рискларни аниқлаш, бутун дунё бўйлаб ҳукумат ва саноат тармоқлари кесимида киберхавфсизликни таъминлаш масалалари, кибер суғурта унсуридан фаол фойдаланиш натижасида эришиладиган натижалар таҳлили ёритилиб ўтилган. Бундан ташқари мақолада кибер суғурта қамров доираси, биринчи томоннинг йўқотишлари, ҳодисаларга жавоб бериш харажатлари, учинчи томон йўқотишлари тоифаларга ажратилиб тавсифи келтирилган.*

Калит сўзлар: *рақамлаштириш, киберхавф, кибертаҳдид, кибержиноят, кибер суғурта, суғурта полиси, киберхавфсизлик*

Azimov Rustam Sodikovich
Candidate of Economic Sciences, Director-General JSC EIIC «Uzbekinvest»
Tashkent, Uzbekistan

CYBER-RISK INSURANCE ISSUES IN THE CONTEXT OF DIGITALIZATION OF THE ECONOMY

Abstract. As a result of the acceleration of the digitization process, cyber risks, cyber threats, and cyber crimes have become a dangerous enemy of humanity. It is important to identify cyber risks, assess risks by classifying them into categories, fight against cyber crimes, and protect yourself through insurance packages. Moreover, creating a protective wall against cyber crime by taking measures to ensure security in the enterprise, ensuring data security in the internal system, and taking measures to ensure information security at the state level is an urgent issue today. This article describes the analysis of the results obtained as a result of the identification of cyber risks, ensuring cyber security in the government and industrial sectors, and the active use of cyber insurance. In addition, the article describes the scope of cyber insurance coverage divided into categories of first-party losses, incident response costs, and third-party losses.

Key words: digitization, cyber risk, cyber threat, cyber crime, cyber risk, cyber insurance, cyber security

Кириш

Молиявий бозорларда янги рақамли воситалар ва технологияларнинг кенг қўлланилиши молиявий-иқтисодий муҳитнинг чегаралари ва хусусиятларини шакллантиришга таъсир кўрсатиб, унинг иштирокчилари учун янги хавфлар

билан боғлиқ муаммоларни келтириб чиқаради. Рақамли молиявий технологиялар хизмат кўрсатиш соҳасидаги трансформацияни бошқарадиган рақамли платформаларнинг асосини ташкил қилади. Ривожланаётган мамлакатларда онлайн тўловлар, кредитлаш ва пул ўтказмаларининг кўпайиши молиявий технологиялар бозорида ўсиш омили ҳисобланади. Шу билан бир қаторда, киберҳужумлар миқёси, хавф даражаси ва ахборот хавфсизлигини таъминлаш харажатлари ортиб бориши аҳамиятлидир. Масалан, тижорат сирлари ёки шахсий маълумотларнинг ўғирланиши, маълумотлар тизимига зарар етказилиши, интеллектуал мулкни ўғирлаш, корпоратив брендларнинг қадрсизланишидан келиб чиқадиган зарарлар миқдори кундан кунга ортиб бормоқда. Бу иқтисодиётни рақамлаштириш вазифалари нуқтаи назаридан хўжалик юритувчи субектларнинг хавфларини баҳолаш ва кибертаҳдидларни олдини олиш, киберхавфлардан суғурта қилиш масаласи энг долзарб бўлиб қолаётганини англатади.

Рақамли иқтисодиёт жараёнларининг тезлашиши ривожланиш учун дастак бўлиш билан қаторда кибержиноятларнинг юзга келиши учун майдон вазифасини ўташига, қатор салбий оқибатларни келтириб чиқаришига ҳам гувоҳ бўляпмиз. Иқтисодиётдаги барча субектлар рақамли анологлардан фойдаланиши, иш жойларини автоматлашуви, маҳсулот етказиб беришдан токи резлизацияга қилишгача барча босқичларда рақамли, молиявий технологияларнинг иштирок этиши тадбиркорлар ва фуқоролар учун қатор хавфларни туғдиряпти. Ушбу хавфлар бизнес жараёнида энг қимматли бўлган „ишлаб чиқариш сири”, „ахборот хавфсизлиги”, „Киберхавф”, „Киберсуғурта” каби бир қатор янги тушунчаларнинг иқтисодиётдаги ролини оширмоқда.

Бугунги кунда рақамлаштириш орқали иқтисодиётда қатор ижобий натижаларга эришиш билан бир қаторда салбий статистик маълумотлардан ҳолат қанчалик жиддий эканлигини билиш мумкин. 2021 йил якуни бўйича кибержиноятларнинг глобал зарари 6 триллион долларни ташкил этиб, бу кўрсаткич АҚШ ва Хитойдан кейинги учинчи йирик давлатнинг ЯИМга тенгдир. Бутун дунёда кибержиноятнинг ўртача йиллик ўсиш суръати 15% ни ташкил қилади[1]. 2021-йилда ИТ хавфсизлиги учун глобал харажатлар 150 миллиард долларга баҳоланмоқда[2].

Allianz Global Corporate & Specialty (AGCS) томонидан ўтказиладиган йиллик сўровнома 89 мамлакат ва ҳудуддаги 2650 эксперт, жумладан, бош директорлар, риск менежерлари, брокерлар ва суғурта экспертларининг фикрларини ўз ичига олади. Ушбу сўровнома 2021 йил бўйича Allianz Risk Barometer ўтказган сўровномалар тарихида киберҳодисалар рейтингда иккинчи марта (овозларнинг 44%ни тўплаб) биринчи ўринни эгаллади, бизнесдаги киберҳужум туфайли таъминот занжиридаги узилишлар 2021 йилдаги олтинчи ўриндан иккинчи ўринга кўтарилди (42%) ва табиий офатлар учинчи (25%) ўринни эгаллаган. Иқлим ўзгариши тарихидаги энг юқори ўсиш

[1] https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf
[2] https://www.gartner.com/en/information-technology/insights/top-technology-trends

кўрсатиб, тўққизинчи ўриндан олтинчи ўринга кўтарилди (17%), овозлар натижасига кўра пандемия эпидемияси тўртинчи ўринга (22 %) тушиб кетди[3].

ИБМнинг берган маълумотларига кўра, 2021 йил якунида компанияда маълумотлар бузилишининг ўртача умумий қиймати 4,24 миллион долларни ташкил қилади. Шахсий маълумотларнинг йўқолган ёки ўғирланган ҳар бир ёзуви учун ўртача харажат 161 долларни ташкил қилди[4].

Шу сабабли, кўплаб мутахассислар кибер суғурта юзага келиши эҳтимоли юқори бўлган киберхавфларни бошқариш учун самарали восита бўлиши мумкинлигини таъкидлаганлар.

Adabiyotlar sharxi

Sebula, J. J. va Young, L. R., (2010) киберхавф атамасини юридик ёки жисмоний шахснинг технологик активларига, маълумотлар базасига ёки бошқа онлайн сақлаш жойларига таъсир кўрсатиши мумкин бўлган турли хил манбалар билан боғлиқ рисклар мажмуи деб таъриф берган. Умуман олганда, молия институтлари ва суғурта бозорини тартибга солувчилар кибер турдаги рисклар технология ва ахборот активлари билан боғлиқлиги сабабли операцион рискнинг бир қисми сифатида таснифлашади. Шу сабабли, киберхавф технологик активлар ва маълумотларнинг мавжудлиги, яхлитлиги ва махфийлиги билан боғлиқ бўлган операцион хавф сифатида таърифланиши мумкин.

Biener, Ch., ва бошқалар (2014) тадқиқотларига кўра, киберхавф - бу ташкилотнинг моддий ва номоддий активларига моддий зарар етказиш, бизнес занжиридаги узилишлар ёки обрўсига путур етказиши мумкин бўлган ахборот активлари, АКТ ресурслари ва технологик активларига таҳдид соладиган, кибермакондаги фаолиятни амалга ошириш билан боғлиқ операцион хавф деб таърифлаган.

Шундан келиб чиққан ҳолда, киберхавфларни хавф манбасига қараб иккита умумий гуруҳга бўлиш мумкин: инсайдер (молиявий зарар, фирибгарлик, маълумотлар базасини ва ходимларнинг шахсий маълумотларини ўғирлаш) ёки ауцайдер (компаниянинг махфий маълумотлари, пул билан боғлиқ операциялар). Ушбу киберхавфлар туфайли корхоналар нафақат махфий маълумотлар ва маблағларни йўқотиши, балки обрўси, бренд номи, контрагент ва истеъмолчи ишончини йўқотиб қўйиши мумкин.

Киберхавф атамаси ташкилот ичидаги АКТ ресурсларига жисмоний шахслар томонидан таҳдидларни ҳам ўз ичига олади. Бу борада Boehme ва бошқ., (2018) киберхавф кўрсаткичларини содир бўлиш сабаблари ва таъсир қилиш обектига қараб қуйидаги уч гуруҳга ажратиб кўрсатишган:

a. Рақамли сабаб → рақамли товарларга зарар.
b. Рақамли сабаб → жисмоний товарларга зарар.
c. Жисмоний сабаб → рақамли товарларга зарар.

[3] https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html
[4] https://www.ibm.com/downloads/cas/ADLMYLAZ

Ridd, J., (2002) тадқиқотларига кўра, кибер суғурта қопламасини тайёрлаш учун компаниянинг умумий ички маълумотларининг базасини 3 турга ажратиб яъни ИТ билан боғлиқ маълумотлар, кадрлар бўлими ва молия, ички аудит, ҳуқуқий масалаларни кўрсатиш мумкин.

Varian, H., (2000) киберхавф суғурта полисини ишлаб чиқишда бизнес маълумотлари суғурта компанияси билиши керак бўлган энг муҳим маълумотлар манбаси ҳисобланади ва шартнома шартлари икки томонлама манфаатли бўлиши учун суғурта компанияси мижозни чуқур таҳлил қилиши ишнинг муҳим қисмини ташкил қилади. Бу борада юзага келиши мумкин бўлган рискларни баҳолаш, компаниянинг кибертаҳдидларни ошкор қилиш даражасини ошириш ва суғурта қилиш бўйича ечимларни тайёрлаш учун бизнес профили яъни компаниянинг асосий фаолияти, мижозга ставкаси, географик маълумотлари, молиявий реквизитлари, ИТ хавфсизлиги бюджети маълумотларилари чуқур ўрганилиши лозим.

Bodin, L ва бошқалар (2018) таҳлилига кўра, маълумотлар корхонанинг энг муҳим активларидан биридир ва улар ўғирланган ёки йўқ қилинган тақдирда катта йўқотишларга ҳаттоки корхонани кризис ҳолатига олиб келади. Бундан ташқари, рақамлашли технологиялар шиддат билан ривожланиш босқичида ахборот-коммуникация технологиялари кундалик фаолиятда муҳим қисмига айланиб бормоқда. АКТ тизимига қилинган киберҳужумлар натижасида катта молиявий йўқотишларга содир бўлади.

Barreto ва бошқалар (2017) фикрига кўра, киберҳужумларнинг барчаси моддий йўқотишларга олиб келади, шунингдек, ташкилотнинг фаолият сектордаги обрўсини йўқотади. Учинчи шахсларнинг маълумотларини ҳимоя қилиш мажбурияти қонунларда белгилаб қўйилган ва улар йўқолган ёки ўғирланган тақдирда жиддий жиноий ва жазо чораларига жавобгар бўлади.

Тадқиқот методологияси. Ушбу мақолада иқтисодиётни рақамлаштириш шароитида кибер-рискларни тоифалари тавсифи, ҳукумат ва саноат тармоқлари кесимида киберхавфсизликни таъминлаш сататистикаси, суғурталаш масалалари, кибер рискларни содир бўлишига инсон омили, технология ва тизимдаги носозликлар, муваффақияциз ички бошқарув, ташқи омиллар таҳлили амалга оширилиб, таҳлил, синтез, абстракт-мантиқий ва танқидий фикрлаш, илимий опробация, қиёслаш, умумлаштириш каби усуллардан фойдаланилди.

Таҳлил ва натижалар.

Рақамли технологияларнинг жадал ривожланиши ва компанияларнинг ИТ инфратузилмасининг мураккаблашиши фонида кибержиноятлар сонининг сезиларли даражада ошгани ҳам эътироф этиш лозим. Маълумотларнинг йўқолиши, бизнес занжиридаги узилишлар, хаккерлик ҳужумлари ёки махфий маълумотларнинг чиқиб кетиши хавфидан ҳимоя қилиш масалалари долзарб бўлиб бораётгани ва кибер хавф суғуртаси зарарни камайтиришнинг оқилона усули сифатида майдонга келади.

Киберхавфни суғурталаш тартиби машаққатли ва мураккаб жараён ҳисобланади, чунки шартномада суғурта компаниясидан ташқари хавфларни баҳолайдиган ва суғурта компанияси учун хулосалар тайёрлайдиган маълум бир ахборот хавфсизлиги (Information Security) аудитор компанияси ҳам бўлиши керак. Аммо бугунги кунда суғурта бозорида комплекс кибер суғурта бўйича хавфларни баҳолаб берувчи таклифлар мавжуд эмаслиги масаланинг янада долзарб эканлигини ифодалайди.

2019 йил бошида дунё суғурта бозорида суғурталанувчилар суғурта компанияларига янада кенг қамровли хизматлар, қўшимча қамров имкониятлари ва потенциалини тақдим этишлари учун таклиф билан чиқишни бошлади. Натижада суғурта бозорида янгидан янги суғурта хизматлари таклифи сезиларли даражада ошди. 2022 йилга келиб эса киберхавфни ҳимоя қилишни сотиб олаётган суғурта компаниялар хавфларни бошқариш бўйича оптимал таклифлар ва сифатли хизматлар учун доимий суғурталовчига айланиш учун кураш олиб бормоқда. Умуман олганда, бундан кейин кибер суғурта бозори барқарор ривожланишда давом этади.

Киберхавф суғурта классларини ишлаб чиқиш, суғурта полисини яратиш суғуртачилар учун энг устувор масалалардан бири бўлиш сабаби шундаки, ҳали аниқланиши ва тавсифланиши керак бўлган жуда кўп шартлар ва тавсифлар мавжуд. Мисол учун, ушбу суғурта полиси соябони остида бўлмаган барча киберхавф ҳодисалари - жавобгарлик ва мулк сиёсати энг долзарб бўлади. Суғурталовчилар полис қамровини яъни мулк ёки жавобгарлик бўйича хавф суғурта қилиниши кераклигини аниқлаштириб олишлари керак.

Кибер суғурта аллақачон жаҳон суғурта бозорида катта улушга эга, шунга қарамай келажакда у янада катталашиши прогноз қилинмоқда. Глобал кибер суғурта саноатининг бозор ҳажми 2020 йил сўнгги маълумотларга кўра, 7,8 миллиард долларни ташкил этди. Прогнозлар шуни кўрсатадики, кибер суғурта 2025 йилга келиб 20 миллиард долларлик саноатга айланиши кутилмоқда. Бизнес вакиллари кибер суғура бозорида катта улуш билан ҳукумронлик қилади. Масалан, 2018 йилда Қўшма Штатлардаги кибер суғурта мукофотларининг 75 фоизи бизнес вакилларидан жалб қилинган бўлса, қолган 25 фоизи, яъни 500 миллион долларлик қисми жисмоний шахсларга тегишли[5].

Киберсуғурта бозори ўсишининг асосий омилларидан бири бу кибержиноятлар ҳажмининг ва таъсир етиш доирасининг кенгайишидир. Кибержиноятлар ҳақида тўплаган статистик маълумотларга кўра, 2020-йилда Ransomware киберҳужумлар қурбонига айланган ҳар 6 корхонадан 1 таси тўлов дастурига дуч келди ва уларнинг ярмига яқини тўловни тўлади. Ransomware - бу кибер жиноятчилар томонидан ишлатиладиган зарарли дастурларнинг бир тури. 2020-йилда кибержиноятлар тўғрисидаги хабарлар сони 2019-йилга нисбатан 69 фоизга ошганини қайд этилди. 2020-йилда кунига ўртача 2000 та кибержиноят хабари ОАВда эълон қилинди[6].

[5] Statista. (2021). Cyber insurance – Statistics & Facts. https://www.statista.com/topics/2445/cyber-insurance/

[6] FBI. (2020). Internet Crime Report. ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Киберҳужумлардан энг кўп зарар кўраётган давлатлар рейтингида Бангладеш мобил дастурлар ва зарарли вируслардан, Жазоир энг хавфли компютер дастурлари вируслари таҳдидларидан, Ўзбекистон крипто-майнинг хавфли ҳужумларидан, Германия эса энг хавфли молиявий дастур ҳужумлари зиёни бўйича дунёда энг кўп зарар кўраётган давлатлар сифатида эълон қилинди (1-расм).

1-расм. Бутун дунё бўйлаб ҳукумат ва саноат тармоқлари кесимида киберхавфсизлик таъминлаш рейтинги тавсифи, 2021 йил [7]

Шахсий маълумотларининг бузилиши хўжалик юритувчи субектлар ва шахслар фаолиятига кескин таъсир қилади. Биргина 2020-йилда маълумотларнинг бузилиши 37 миллиарддан ортиқ шахсий ёзувларни фош қилди, уларнинг 82 фоизи 5 та кибер жиноят натижасида келиб чиққан[8]. Маълумотларнинг бузилиши нафақат компания ва ташкилотларга, балки шахсий маълумотлари ошкор қилинган шахсларнинг шахсий дахлсизлигига, обрўсига ҳам таъсир қилади. 2020-йилда шахсга оид фирибгарлик йўқотишларининг 49 миллион қурбонига жами 56 миллиард доллар зарар етказди. Бу ҳар бир жабрланувчи учун 1100 долларга тушади[9]. Киберҳужумга дучор бўлганларнинг 69 фоиз инсонлар шахсий маълумоти ўғирланган, 64 фоиз кибербуллинг ва 69 фоиз кибертовламачилик киберҳужумлари энг кенг тарқалган.

Рақамлаштириш жараёни тезлашиши натижасида киберхавфлар, кибертаҳдидлар, кибержиноятлар инсониятга жиддий иқтисодий, ижтимоий,

[7] https://financesonline.com/cybersecurity-statistics/
[8] RiskBased Security. (2020). 2020 Year End Report.
[9] Javelin. (2021). 2021 Identity Fraud Study: Shifting Angles. javelinstrategy.com/content/Javelin-2021-Identity-Fraud-Study

молиявий зарар келтириб хавфли душманига айланди. Кибер рискларни аниқлаш, котегорияларга бўлиб таснифлаш орқали рискларни баҳолаш, кибер жиноятларга қарши курашишда ақлли, ҳимояланган, юқори сифатли шифрланган технологиялардан фойдаланиш, Финтечларни самарали қўллаш, суғурта пакетлари орқали ҳимояланиш, корхонада хавфсизликни таъминлаш чораларини кўриш, ички тизимда маълумотлар хавфсизлигини таъминлаш, давлат миқиёсида ахборот хавфсизлигини таъминлаш чораларини кўриш орқали кибержиноятчиликка қарши ҳимоя деворини яратиш қиммат хизмат турларидан ҳисобланади. Киберхавфсизлик харажатлари бутун дуно бўйлаб ўсиб бормоқда. Дунё бўйлаб хавфсизлик харажатлари энг тез ўсаётган етакчи тармоқлар ичида давлат ёки маҳаллий ҳукумат хавфсизлигини таъминлаш харажатлари 11.9%, телекоммуникация 11.8%, ресурс тармоқлари 11.0%, банк 10.4% кўрсаткич билан соҳалар ичида етакчилик кўрсатди.

2-расм. Дунё бўйлаб хавфсизлик харажатлари энг тез ўсаётган етакчи тармоқлар тавсифи, 2021 йил[10]

Ҳозирги кунда жаҳон амалиётида суғурта компаниялари қуйидаги хавф турлари бўйича суғурта қопламаларини таклиф этади: махфий маълумотларнинг ўғирланиши ва ундан кейинги ташкилот ходимлари томонидан фойдаланиш хавфи; жиноятчиларнинг банк мижозлари ҳақидаги маълумотларни, масалан, кредит карта ва ҳисоб рақамларини ўғирлаш хавфи; банк мижозларининг ҳисобварақларидан пул ўғирлаш хавфи; компания ходимларининг махфий маълумотларини ошкор қилиш хавфи; компютер тармоғидаги, ташкилот веб-сайтидаги носозликлар туфайли корхона фаолиятини тўхтатиш хавфи; нотўғри маълумотларни жойлаштириш билан боғлиқ ҳолда ташкилот томонидан зарар олиш ва ҳ.к.

Маълумотлар бузилишининг сабаблари, киберхавфсизликнинг бузилиши кўп ҳолларда киберҳужумлар натижасида содир бўлади, аммо Веризоннинг 2020 йилги маълумотлар бузилиши бўйича текширувлар ҳисоботида ҳар доим ҳам киберҳужумлар оқибатида юзага келмаслигини келтириб ўтилган, 2020 йилда маълумотлар бузилишининг асосий сабаблари эса қуйидагилар:

[10] https://financesonline.com/cybersecurity-statistics/

Хакерлик: рухсатиз бизнеснинг киберхавфсизлик чораларини йўқ қилиш орқали маълумотларга кириш ва ўғирлаш имконини берди.

Хатолар: хатоларнинг ўзига хос табиати турлича бўлган, жумладан ИТ кўникмаси заиф ходимлар сабабли учинчи шахсларга киришга имкон берувчи тизимдаги носозликлар.

Ижтимоий ҳужумлар: ижтимоий ҳужумлар орасида “фишинг” фирибгарликлари, шунингдек, алоҳида шахс, бизнес ёки ташкилотга қаратилган фирибгарликлар киради.

Зарарли дастурий таъминот: хакерлар компания маълумотларига ташқаридан кириш учун зарарли дастурлардан фойдаланганлар.

Ваколатли фойдаланувчилар: ваколатли кириш ҳуқуқига эга бўлган инсайдерларнинг ўз компаниялари тизимларини молиявий ёки шахсий манфаатлар учун атайлаб суиистеъмол қилишлари натижасида юзага келган.

Жисмоний шахслар: нозик маълумотларни сақлайдиган қурилмаларни ўғирлаган шахслар ҳам катта миқдордаги бузилишларга сабаб бўлди[11].

Solvency II ва Базел II ҳужжатларида келтирилган кўрсатмаларга кўра, киберхавфларни тўртта тоифага бўлиш мумкин: технология ва тизимдаги носозликлар, муваффақияциз ички муҳит, инсон омили ва ташқи омиллар.

1- жадвал

Кибер риск тоифалари тавсифи[12]

Туркум	**Таъриф**	**Омиллар**
Одамларнинг хатти-ҳаракати		
Беихтиёр	Зарарли мақсадлар кўзламасдан қилинган ҳаракатлар	Хатолар
Қасддан	Зарар етказиш учун қасддан қилинган ҳаракатлар	Фирибгарлик, ўғирлик, вандализм
Ҳаракацизлик	Зарарли вазиятда қарши ҳаракат қилмаслик	Кўникма ва билимнинг етишмаслиги
Технология ва тизимдаги носозликлар		
Ускуна	Қўлда ишлайдиган асбоб-ускуналардаги носозликлар билан боғлиқ хавфлар	Ишлаш, қувват, техник хизмат кўрсатиш туфайли муваффақияцизлик
Дастурий таъминот	Дастурлар, иловалар, операцион тизимлар томонидан юзага келадиган хавфлар	Хавфсизлик созламалари, кодлаш, тест, конфигурацияни бошқариш
Тизим	Интеграциялашган тизимлар каби носозликлар кутилганидек ишламайди	Интеграция, дизайн, спецификациялар
Муваффақияциз ички бошқарув		
Жараён дизайни	Жараённинг нотўғри дизайни ёки бажарилиши туфайли муваффақияцизлик	Ҳужжатлар, ахборот оқими, масъулият, огоҳлантиришлар, билдиришномалар.

[11] Verizon. (2020). 2020 Data Breach Investigations Report – Executive Summary. enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

[12] Тадқиқотчи ишланмаси.

Жараённи бошқариш	Жараён операцияларини ёмон назорат қилиш	Даврий кўриб чиқиш, жараёнга эгалик қилиш, мониторинг
Жараённи қўллаб-қувватлаш	Қўллаб-қувватлаш жараёнига тегишли ресурсларни етказиб бермаслик	Бухгалтерия ҳисоби, кадрлар билан таъминлаш, ўқитиш, ривожлантириш
Ташқи омиллар		
Фалокатлар	Ташкилот назорат қила олмайдиган инсоний ва табиий ҳодисалар	Об-ҳаво ҳодисаси, ёнғин, сув тошқини, табиий офатлар
Ҳуқуқий масалалар	Ҳуқуқий далиллардан келиб чиқадиган хавфлар	Қонунчилик, низомлар, суд жараёнлари
Бизнес масалалари	Ишбилармонлик муҳитининг ўзгариши билан боғлиқ хавфлар	Йетказиб берувчининг ишдан чиқиши, бозор ҳолати, иқтисодий сабаблар
Хизматга бўлган ишонч	Ташкилотнинг ташқи томонларга таянишидан келиб чиқадиган хавфлар	Коммунал хизматлар, ёқилғи, фавқулодда хизматлар, транспорт ва бошқа етказиб берувчилар

Ривожланган давлатларда компаниялар кибер суғуртадан суғурталаниши тартиби бир нечта талабларга жавоб бериши керак бўлади. Корхонада маълумотларни ҳимоя қилиш тизимига эга бўлган ахборот тизими, шахсий маълумотларни сақлаш тизими, ахборот хавфсизлиги талабларига мувофиқлик сертификатга эга бўлган давлат тизими ёки харажатларнинг оқилоналиги ва мутаносиблиги асосида танланган ҳимоя воситаларига эга бошқа ахборот тизими бўлиши мумкин. Бундай ҳолда, бизнес субйекти ўзини кибер суғурта орқали суғурта қилиши учун қуйидаги босқичлардан ўтиши керак:

– киберхавфни тўлиқ суғурталаш хизматини таклиф қилувчи суғурта компаниясини танлаш;

– ахборот хавфсизлиги аудитини ўтказиш учун эксперт ташкилотини танлаш (суғурта компанияси томонидан аккредитация қилинган ташкилотлар орасидан);

– ахборот хавфсизлиги рискларини текшириш ва баҳолаш (експерт ташкилоти томонидан ўтказилади);

– суғурта ҳодисаларининг таърифи;

– суғурта қопламаси ва суғурта мукофотлари миқдорини аниқлаш;

– комплекс кибер суғурта хизмати бўйича шартномани шакллантириш.

Киберхавфни суғурталаш полиси (кибер жавобгарликни суғурта қопламаси) кибер ҳужум оқибатида юз берган узилишлар, тармоқ шикастланишлари натижасида етказилган йўқотишларни камайтирадиган ҳимоя воситаси сифатида яратилган. Киберсуғурта киберҳужумлар ва маълумотлар бузилишининг зарарини камайтириш учун мўлжалланган. Бу биринчи навбатда мавжуд суғурта полисларида қопланадиган йўқотишларни ўз ичига олмаганлиги сабабли пайдо бўлди.

3-расм. Кибер суғурта қамров доираси тавсифи[13]

Корхоналар учун кибер суғуртанинг афзалликлари қуйидагилардан иборат:

-юридик тўловлар қопланиши: маълумотларнинг бузилиши каби киберҳужумлар натижасида келиб чиқадиган юридик тўловлар катта суммани ташкил қилиши мумкин. Чет элда киберсуғурта провайдерларининг максимал қамров миқдори ҳар бир даъво учун 1 миллион доллардан 100 миллион долларгача ўзгариб туради;

-бузилишдан тикланиш: киберсуғурта етказилган зарарларни қоплашдан тортиб бузилган маълумотларни тиклашгача бўлган бузилишларни бартараф этишда ёрдам беради;

-онлайн вандализм натижасида етказилган зарарни қоплаш: кибер вандализм содир бўлса, кибер суғурта бизнесни тиклашга ёрдам беради ва бу орқали суғурта провайдерлари йўқолган маблағларни қоплаб беради.

Хулоса

Киберхавфларни бошқаришда суғурта речагидан фойдаланишдан келиб чиққан ҳолда, хусусий корхоналар, давлат ташкилотлари киберхавфлардан ҳимояланиш учун фойдаланиладиган воситалар тўпламининг ишончлилигини баҳолаш учун бир нечта асосий йўналишларни қайта кўриб чиқишлари фойдалидир:

Биринчидан, киберхавфларни аниқ тушуниш ва баҳолаш лозим. Киберхавф ҳодисаларининг олдини олиш ва аниқлаш учун воситалар, жараёнлар ва бошқарув воситалари аниқланиши керак, масалан, контрагентлар, пудратчилар ва мижозлардан фойдаланган ҳолда корхонага киберҳужум уюштирилиши хавфининг мавжудлиги.

Иккинчидан, ташкилий-кадрлар масаласини қайта кўриб чиқиш. Киберхавфларни минималлаштириш учун компания раҳбарлари ҳар бўлимда ўз ваколатларини суистеъмол қилмайдиган, киберхавфсизлик соҳасида таҳдидлар, ҳужумлар ва ҳимоя технологияларидан фойдаланиш кўникмасига эга бўлган етакчи мутахассислари билан самарали ҳамкорлик қилишлари

[13] Tadqiqotchi ishlanmasi.

лозим. Кибер таҳдид доирасида рақамли ҳужум эҳтимоли бор бўлса, кибермудофаа технологияларидан самарали фойдаланиш ва мунтазам равишда янгилаб бориш мақсадга мувофиқ.

Учинчидан, шуни таъкидлаш мумкинки, инсон омили аралашганлигини ҳисобга олиб киберхавфсизликни таъминлашда суғурта орқали рисклани камайтириш ҳам муҳим ҳисобланади. Корхона раҳбарлари киберхавф етказиши мумкин бўлган зарар миқдорини баҳолаши, таҳлил қилиши ва уларни тўғри бошқаришлари керак. Корхона раҳбари ва менежерлари кибер суғурта имконият доирасини тушуниши ва хавф профилига мос келадиган суғурта маҳсулотларидан рискларни камайтириш ва етказилиши мумкин бўлган зарарни бартараф этиш учун жойлаштириш имкониятини қўлдан бой бермаслиги, киберхавфларни олдини олишда ўзининг бюджетини шакллантириб бориши мақсадга мувофиқ.

Фойдаланилган адабиётлар рўйхати

1. Cebula, J.J. and Young, L.R. (2010) A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/ SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.
2. Biener, Ch., & Eling, M & Wirfs, J. (2014). Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance - Issues and Practice. 40. 1-28. 10.1057/gpp.2014.19.
3. Böhme, Rainer & Kataria, Gaurav. (2018). Models and Measures for Correlation in Cyber-Insurance.
4. Ridd, J., 2002. Insuring Digital Risk: A Roadmap for Auction. Information Assurance Advisory Council. 28, 771-780
5. Hal Varian, Managing Online Security Risks, N.Y. Times, June 1, 2000.
6. Bodin, Lawrence & Gordon, Lawrence & Loeb, Martin & Wang, Aluna. (2018). Cybersecurity insurance and risk-sharing. Journal of Accounting and Public Policy. 37. 10.1016/j.jaccpubpol.2018.10.004.
7. Barreto, Carlos & Schwartz, Galina & Cardenas, Alvaro. (2021). Cyber-Insurance. 10.1007/978-3-030-65048-3_15.
8. https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf
9. https://www.gartner.com/en/information-technology/insights/top-technology-trends
10. https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html
11. https://www.ibm.com/downloads/cas/ADLMYLAZ
12. Statista. (2021). Cyber insurance – Statistics & Facts. https://www.statista.com/topics/2445/cyber-insurance/
13. FBI. (2020). Internet Crime Report. ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
14. https://financesonline.com/cybersecurity-statistics/

15. RiskBased Security. (2020). 2020 Year End Report. pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

16. Javelin. (2021). 2021 Identity Fraud Study: Shifting Angles. javelinstrategy.com/content/Javelin-2021-Identity-Fraud-Study

17. Verizon. (2020). 2020 Data Breach Investigations Report – Executive Summary. enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf