

**ТОШКЕНТ МОЛИЯ ИНСТИТУТИ ҲУЗУРИДАГИ  
ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ  
DSc.03/30.12.2019.I.17.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ**

---

**ТОШКЕНТ МОЛИЯ ИНСТИТУТИ**

**ХАСАНОВ ФАРРУХ РАВШАНОВИЧ**

**ЎЗБЕКИСТОНДА КИБЕР РИСКЛАРНИ СУҒУРТАЛАШ  
МАСАЛАЛАРИ**

**08.00.07 – Молия, пул муомаласи ва кредит**

**Иқтисодиёт фанлари бўйича фалсафа доктори (Doctor of Philosophy) диссертацияси  
АВТОРЕФЕРАТИ**

**Тошкент шаҳри - 2022 йил**

**Иқтисодиёт фанлари бўйича фалсафа доктори (PhD) диссертацияси  
автореферати мундарижаси**

**Оглавление автореферата диссертации доктора философии (PhD) по  
экономическим наукам**

**Contents of dissertation abstract of the doctor of philosophy (PhD) on  
economical sciences**

**Хасанов Фаррух Равшанович**

Ўзбекистонда кибер рискларни суғурталаш масалалари..... 3

**Хасанов Фаррух Равшанович**

Вопросы страхования кибер рисков в Узбекистане..... 29

**Khasanov Farrukh Ravshanovich**

Issues of cyber risks insurance in Uzbekistan..... 53

**Эълон қилинган ишлар рўйхати**

Список опубликованных работ

List of published works..... 57

**ТОШКЕНТ МОЛИЯ ИНСТИТУТИ ҲУЗУРИДАГИ  
ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ  
DSc.03/30.12.2019.I.17.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ**

---

**ТОШКЕНТ МОЛИЯ ИНСТИТУТИ**

**ХАСАНОВ ФАРРУХ РАВШАНОВИЧ**

**ЎЗБЕКИСТОНДА КИБЕР РИСКЛАРНИ СУҒУРТАЛАШ  
МАСАЛАЛАРИ**

**08.00.07 – Молия, пул муомаласи ва кредит**

**Иқтисодиёт фанлари бўйича фалсафа доктори (Doctor of Philosophy) диссертацияси  
АВТОРЕФЕРАТИ**

**Тошкент шаҳри - 2022 йил**

**Фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида №B2020.2.PhD/Iqt1372 рақам билан рўйхатга олинган**

Докторлик диссертацияси Тошкент молия институтида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида ([www.tfi.uz](http://www.tfi.uz)) ва «ZiyoNET» Ахборот таълим порталида ([www.ziynet.uz](http://www.ziynet.uz)) жойлаштирилган.

**Илмий раҳбар:** Шеннаев Хўжаёр Мусурманович  
иктисодиёт фанлари доктори (Dsc), доцент

**Расмий оппонентлар:** Кузиева Наргиза Рамазоновна  
иктисодиёт фанлари доктори, профессор  
Хамидулин Михаил Борисович  
иктисодиёт фанлари доктори, профессор

**Етакчи ташкилот:** Тошкент Давлат иқтисодиёт университети

Диссертация ҳимояси Тошкент молия институти ҳузуридаги DSc.03/30.12.2019.1.17.01 рақамли илмий кенгашнинг 2022 йил «28» 01 соат 16:00 даги мажлисида бўлиб ўтди. Манзил: 100000, Тошкент шаҳри Амир Темур кўчаси, 60а уй. Тел.: (99871) 234-53-34, факс: (99871) 234-67-71, e-mail: [ilmiykengash@tfi.uz](mailto:ilmiykengash@tfi.uz).

Диссертация билан Тошкент молия институтининг Ахборот-ресурс марказида танишиш мумкин (257 рақами билан рўйхатга олинган). Манзил: 100000, Тошкент шаҳри, Амир Темур кўчаси, 60а уй. Тел.: (99871) 234-53-34, факс: (99871) 234-67-71, e-mail: [admin@tfi.uz](mailto:admin@tfi.uz).

Диссертация автореферати 2022 йил «14» 01 куни тарқатилди.  
(2022 йил «14» 01 даги 70 рақамли реестр баённомаси).



*[Handwritten signature]*

**Т.З.Тешабаев**

Илмий даражалар берувчи илмий кенгаш раиси, иқтисодиёт фанлари доктори, профессор

*[Handwritten signature]*

**Ф.Т.Холмаматов**

Илмий даражалар берувчи илмий кенгаш илмий котиби, иқтисодиёт фанлари бўйича фалсафа доктори (PhD), доцент

*[Handwritten signature]*

**И.Н.Кўзиёв**

Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, иқтисодиёт фанлари доктори, профессор

## КИРИШ (фалсафа доктори (PhD) диссертацияси аннотацияси)

**Диссертация мавзусининг долзарблиги ва зарурати.** Жаҳон ҳамжамияти учун янги давр бошланди. Ушбу давр ахборот-коммуникация технологияларининг барча соҳа ва тармоқларга кириб бориши билан изоҳланади. Инсонларнинг кундалик фаолияти ахборот-коммуникация технологиялари билан чамбарчас боғлиқ бўлиб қолди. Жаҳондаги аксарият давлатлар рақамли иқтисодиёт тизимини жорий эта бошлади ва бу ўзгаришлар, пировард натижада, инсониятнинг фаровонлигига хизмат қилмоқда. Шу билан бирга, ахборот-коммуникация технологияларининг кундалик ҳаётимизга жадал кириб бориши кибер хавфсизликка таҳдид солувчи янги рискларни юзага келтирмоқда. Бу рисклар жаҳон амалиётида кибер рисклар деб номланиб, уларнинг салбий оқибатлари глобал миқёсда зарар етказишга қодир. БМТ Бош котиби Антониу Гутерриш бу ҳолатга қуйидагича фикр келтиргани бежиз эмас: «Рақамли иқтисодиёт янги хавф-хатарларни, жумладан, кибер хавфсизликка таҳдидлар, ноқонуний иқтисодий фаолиятнинг енгиллашуви, шахсий ҳаёт дахлсизлигини бузилиши билан боғлиқ салбий оқибатларни вужудга келтириши мумкин...»<sup>1</sup>. Шу сабабдан ҳам кибер хавфсизликни таъминлаш жаҳон ҳамжамиятининг долзарб муаммоларидан бирига айланиб бормоқда ҳамда мазкур муаммоларни ҳал этишда кибер рискларни суғурталаш тизимини кенг жорий қилиш ва ривожлантириш истиқболли йўналиш сифатида қаралмоқда.

Жаҳон амалиётида кибер хавфсизликни таъминлаш, хусусан кибер рискларни олдини олиш ва уларнинг салбий оқибатларини камайитиришга қаратилган риск-менежмент тизимининг қатор усуллари ва воситалари илмий тадқиқ этиб келинмоқда. Ушбу тадқиқотларда кибер хавфсизликни таъминлашнинг техник воситалари, яъни маълумотларни криптографик ҳимоялаш ва шифрлаш, маблағлар заҳиралаш, рискларни тақсимлаш (диверсификация), меъёрлаштириш (сертификатлаш, лицензиялаш) каби масалаларга эътибор қаратилган. Бироқ, мазкур тадқиқотларда кибер рискларни суғурталаш масалалари етарлича очиқ берилмаган, шу сабабдан ҳам ушбу йўналишда илмий изланишлар олиб бориш зарурати юзага келмоқда.

Ўзбекистонда ҳам ахборот-коммуникация тизимини янада ривожлантириш, рақамли иқтисодиётни жорий этиш борасида қўйилаётган илдам қадамлар, ўз навбатида, кибер хавфсизликни бошқариш механизмини ишлаб чиқишни тақозо этмоқда. 2017-2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналишлари бўйича Ҳаракатлар стратегиясида «янги турлардаги суғурта, лизинг ва бошқа молиявий хизматларнинг ҳисобига уларнинг хажмини кенгайтириш ва сифатини ошириш, капитални жалб қилиш ҳамда корхона, молиявий институтлар ва аҳолининг эркин ресурсларини жойлаштиришдаги муқобил

---

<sup>1</sup> Дорожная карта Генерального секретаря ООН по цифровому сотрудничеству. <https://www.un.org/ru/content/digital-cooperation-roadmap/>.

манба сифатида фонд бозорини ривожлантириш» белгиланган<sup>2</sup>. Шу сабабдан кибер хавфсизликни таъминлашда кибер рискларни суғурталаш тизимини ривожлантириш, хусусан бу борада тегишли илмий-услубий ёндашув ҳамда норматив-ҳуқуқий ҳужжатларни ишлаб чиқиш ва мавжудларини такомиллаштиришнинг зарурлиги танланган илмий тадқиқот мавзусининг долзарблигини белгилайди.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сонли «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида», 2020 йил 2 мартдаги ПФ-5953-сонли «2017 - 2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегиясини «Илм, маърифат ва рақамли иқтисодиётни ривожлантириш йили»да амалга оширишга оид Давлат дастури тўғрисида»ги Фармонлари, 2019 йил 2 августдаги ПҚ-4412-сонли «Ўзбекистон Республикасининг суғурта бозорини ислоҳ қилиш ва унинг жадал ривожланишини таъминлаш чора-тадбирлари тўғрисида»ги қарори, шунингдек мазкур соҳага тегишли бошқа норматив-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишда мазкур диссертация иши муайян даражада хизмат қилади.

**Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги.** Мазкур диссертация тадқиқоти республика фан ва технологиялар ривожланишининг I. «Демократик ва ҳуқуқий жамиятни маънавий-ахлоқий ва маданий ривожлантириш, инновацион иқтисодиётни шакллантириш» устувор йўналишига мувофиқ бажарилган.

**Муаммонинг ўрганилганлик даражаси.** Кибер рискларни суғурталаш масалалари ғарб олимлари Ж.П.Кесан ва Н.Шетти, Р.Беме, Р.Пал<sup>3</sup>нинг ишларида ўрганилган. МДҲ давлатларининг иқтисодчи олимлари А.Н.Ивашченко, С.А.Смирнов, Н.В.Косыгина, Е.В.Небольсина, Н.И.Артамонов<sup>4</sup>ларнинг ишлари кибер суғурта бозори ва кибер суғуртанинг услубиётига бағишланган. Мамлакатимиз олимлари ва мутахассислари С.С.Фуломов, Т.К.Иминов, Р.Ҳ.Хусанов, Н.Р.Кузиева, М.Б.Хамидулин, Қ.М.Қўлдошев, Х.М.Шеннаев, Б.Б.Ашрафханов, М.А.Мирсадиков, А.А.Ядгаров, А.Давлатов, И.Х.Абдурахмонов, Б.С.Гайбуллаев,

<sup>2</sup> Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги Фармони.

<sup>3</sup> Kesan J.P., Majuca R.P., Yurcik W.J. The Economic Case of Cyberinsurance; Shetty N., Schwartz G., Felegyhazi M., Walrand J. Competitive Cyber-Insurance and Internet Security. In: Workshop on Economics of Information Security (WEIS). University College London, 2009; Böhme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework; Pal R., Golubchik L., Psounis K. A Novel Cyber-Insurance Model.

<sup>4</sup> Ivashchenko A.N., Sharko I.A. [The world cyber risk insurance market: Opportunities and obstacles for development in the Republic of Belarus]. Материалы IX Международной научно-практической конференции студентов «Национальная экономика Республики Беларусь: проблемы и перспективы развития». Минск, 2016, С. 196–202; Смирнов С.А. Страхование киберрисков в России: анализ состояния и перспективы развития // Сборник научных работ / под ред. Г.Д. Дроздова. СПб., 2015. С. 303–306; Kosygina N.V., Anpilogova V.S. [Cyber risks and their insurance in the sphere of banking services]. Материалы II Международной научно-практической конференции «Актуальные вопросы экономики и финансов в условиях современных вызовов российского и мирового хозяйства». Самара, 2014, С. 203–204; Nebol'sina E.V. [Cyber risks as a global problem of the modern world]. Strakhovoe delo = Insurance Business, 2016, no. 1, pp. 22–28; Артамонов Н.И. Управление киберрисками в системе риск-менеджмента предприятий малого и среднего бизнеса // Страхование право. 2015. № 4. С. 53–57.

И.Мавлонова<sup>5</sup>лар томонидан суғурта фаолиятининг турли жиҳатлари ўрганилган. Бундан ташқари, Х.М.Шеннаев, М.Х.Ходжаева, М.Т.Асқарова, Т.М.Баймуратов, А.С.Нуруллаев, Қ.М.Қўлдошев, И.Х.Абдурахмонов, И.Г.Кенжаев, Г.Халиқулова<sup>6</sup>лар суғурта соҳасига бағишланган номзодлик ва докторлик диссертацияларини химоя қилган.

Иқтисодчи олимлар Т.К.Иминов, А.Н.Арипов ва Н.А.Иминова<sup>7</sup>ларнинг илмий ишларида ахборот-коммуникация соҳасида риск-менежмент, кибер хавфсизликни таъминлаш масалалари ўз аксини топган. Ушбу ишларда кибер рискларни суғурталаш кибер хавфсизликни таъминлашнинг усулларида бири сифатида қисман ўрганилган ва бу борада умумий мулоҳазалар берилган.

Таъкидлаш лозимки, мамлакатимизда шу кунгача кибер суғурта масаласига бағишланган алоҳида тадқиқот иши амалга оширилмаган. Шу сабабдан, кибер рискларни суғурталаш механизмини чуқур ўрганиш ва кенг жорий қилиш ҳамда ривожлантириш борасида таклиф ва тавсиялар ишлаб чиқиш мазкур диссертация мавзусини танлаш ва тадқиқот вазифаларини белгилашга асос бўлди. Ушбу илмий иш мамлакатимизда кибер рискларни суғурталаш масаласига бағишланган биринчи илмий тадқиқот иши саналади.

**Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасаси илмий-тадқиқот ишлари режалари билан боғлиқлиги.** Мазкур диссертация тадқиқоти Тошкент молия институти илмий-тадқиқот ишлари режасига мувофиқ «Рақамли иқтисодиёт шароитида молия, банк ва

---

<sup>5</sup> Фуломов С.С., Боев Ҳ.И. Валюта, кредит, молия ва суғурта муаммолари. – Т.: Мехнат, 1998; Иминов Т. Суғурта бозори ислохотлари ривожланиш босқичида. – Т.: Халқ сўзи, 2021, №5(7785); Хусанов Р.Х., Ядгаров А.А. Бозор иқтисодиёти шароитида суғурта тизими. – Т.: Янги аср авлоди, 2005. – 79 б.; Kuzieva N.R., Ashurova N.B., Ollokulova F.M. Business Processes In The Insurance System And Their Features. International Journal of Advanced Science and Technology Vol. 29, No. 7, (2020), pp. 7908-7913; Хамидулин М.Б., Мирсаидов М.А. Страхование. Учебно-методическое пособие. Ташкентский филиал ФГБОУ ВО «РЭУ им.Г.В.Плеханова», 2019; Қўлдошев Қ.М. Суғурта бозори, Т.: Иқтисод-молия, 2010. – 110 б.; Шеннаев Х. Суғурта иши. – Т.: Турон-иқбол, 2006. – 224 б.; Ашрафханов Б., Мирсаидов М. Развитие страхового законодательства Республики Узбекистан. – Т.: Рынок, деньги и кредит, 2002, №11-12. – 30 с.; Давлатов А. Автофуқаролик жавобгарлигининг химояси. – Т.: Бозор, пул ва кредит, 2008, №9. – 54-56 б., Абдурахмонов И. Мажбурий суғурта ижтимоий-иқтисодий ўсиш омили. – Т.: Бозор, пул ва кредит, 2009, №5. – 32-33 б.; Гайбуллаев Б. Регулирование инвестиционной деятельности страховщиков. – Т.: Бозор, пул ва кредит, 2009, №5, – 50-53 с., Мавлонова И. Суғурта-ижтимоий ва иқтисодий манфаатлар химояси. – Т.: Бозор, пул ва кредит, 2009, №10 – 53-55 б.

<sup>6</sup> Шеннаев Х.М. Ўзбекистон Республикасида суғурта фаолиятини ривожлантириш йўналишлари. И.ф.д. (Dsc) илмий даражасини олиш учун ёзилган диссертация автореферати, Т.: ТМИ, 2021; Ходжаева М.Х. Суғурта фаолияти бухгалтерия ҳисоби ва аудитининг ҳозирги аҳоли ва уни такомиллаштириш йўллари. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати, – Т.: БМА, 2001. – 130 б.; Асқарова М.Т. Развитие системы страхования в обеспечении экономического роста в условиях рыночных преобразований в Республики Узбекистан. Автореферат диссертации на соискание ученой степени к.э.н., – Т.: Институт экономики АН РУз, 2003. – 132 с.; Баймуратов Т.М. Ўзбекистонда суғурта фаолияти ва уни солиққа тортиш механизмини такомиллаштириш. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: Давлат ва жамият қурилиши академияси, 2004. – 125 б.; Нуруллаев А.С. Ўзбекистонда фермер ва деҳқон хўжалиқларини суғурталаш масалалари. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: БМА, 2007; Қўлдошев Қ.М. Суғурта бозорини ривожлантириш ва бошқариш муаммолари. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: БМА, 2009. – 130 б.; Абдурахмонов И.Х. Ўзбекистон Республикасида жавобгарликни суғурталашнинг амалиётини такомиллаштириш. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: БМА, 2010. – 130 б.; Кенжаев И.Г. Суғурта ташкилотларининг молиявий ресурсларини жойлаштириш самарадорлигини ошириш йўллари. Иқтисодиёт фанлари бўйича фалсафа доктори илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: ТМИ, 2019; Халиқулова Г. Суғурта тизими ва уни амал қилиш механизмини такомиллаштириш. Иқтисодиёт фанлари бўйича фалсафа доктори илмий даражасини олиш учун ёзилган дисс. автореферати. – Т.: ТМИ, 2019.

<sup>7</sup> Иминов Т.К., Арипов А.Н. Ўзбекистон ахборот-коммуникация технологиялари соҳаси менежменти асослари. – Т.: Фан ва технология, 2005; Иминова Н.А. Алоқа ва ахборотлаштириш соҳасида иқтисодий рискларни бошқариш. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: ТАТУ, 2011.

ҳисоб тизимини мувофиқлаштиришнинг илмий асослари» мавзуси доирасида бажарилган.

**Тадқиқотнинг мақсади** Ўзбекистонда кибер рискларни суғурталашни ривожлантириш бўйича таклиф ва тавсиялар ишлаб чиқишдан иборат.

**Тадқиқотнинг вазифалари** куйидагилардан иборат:

кибер рисклар тушунчасига доир мавжуд ёндашувларни таҳлил этиш орқали уларнинг мазмун-моҳияти ва иқтисодий оқибатларини ёритиш;

кибер хавфсизликни таъминлашда суғуртанинг ўрнини тадқиқ қилиш ва кибер рискларни суғурталашнинг концептуал асосларини ишлаб чиқиш;

хорижий мамлакатларда кибер рискларни суғурталаш амалиётини ўрганиш ва уни республикамизда қўллаш йўлларини аниқлаш;

Ўзбекистон ахборот технологиялари ва коммуникациялари соҳасида суғурта муносабатлари ҳолатини тадқиқ қилиш ва соҳада замонавий суғурта муносабатларини ривожлантириш борасида таклиф ва тавсиялар ишлаб чиқиш;

Ўзбекистонда кибер хавфсизликни таъминлашнинг муҳим воситаси сифатида кибер рискларни суғурталаш ҳолатини ўрганиш ва таҳлил қилиш;

Ўзбекистонда кибер рискларни суғурталашни ривожлантиришнинг ташкилий-ҳуқуқий асосларини ишлаб чиқиш;

кибер рискларни суғурталашда ахборот тизимлари қийматини баҳолаш услугиётини такомиллаштириш асосида уларни суғурталашнинг иқтисодий механизминини яратиш.

**Тадқиқотнинг объекти** сифатида суғурта ташкилотларининг кибер рискларни суғурталаш бўйича фаолияти олинган.

**Тадқиқотнинг предмети** Ўзбекистонда кибер рискларни суғурталаш жараёнида юзага келадиган иқтисодий муносабатлар ҳисобланади.

**Тадқиқотнинг усуллари.** Диссертацияда таҳлил ва синтез, қиёсий таҳлил, статистик таҳлил, мантиқий фикрлаш, сўровнома ўтказиш, кузатиш, шунингдек математик моделлаштириш каби усуллардан фойдаланилган.

**Тадқиқотнинг илмий янгилиги** куйидагилардан иборат:

кибер рискларни суғурталашда суғурта объектини ахборот макони ва ахборот-коммуникация технологиялари муҳити категориясининг замонавий тушунчасига мослаш мақсадида суғурта фаолияти классификаторига янги «Номоддий активлар суғуртаси» классини киритиш таклиф этилган;

кибер рискларнинг хусусияти, иқтисодий ҳамда ижтимоий оқибатларини ҳисобга олган ҳолда кибер рисклар туркумига кирувчи рисклар тоифасига қараб суғуртанинг ихтиёрий ёки мажбурий шаклларини қўллаш асосланган;

кибер рискларни суғурталашнинг шартлари ва тариф ставкаларини суғурта маҳсулоти истеъмолчиларининг манфаатларига мослаштирилган ягона давлат тизимини яратиш таклиф этилган;

ахборот ресурслари ва тизимлари қийматини баҳолашда суғурта рискига боғлиқликни қўлламаган ҳолда уларни харажат асосида ҳисоблашнинг соддалаштирилган усули ишлаб чиқилган.

**Тадқиқотнинг амалий натижалари** куйидагилардан иборат:



кибер рискларни суғурталаш бўйича ягона давлат тизимини яратиш, ушбу йўналиш бўйича тегишли норматив-ҳуқуқий ҳужжат қабул қилиш, кибер рисклардан суғурталашнинг шакли ва тартибини тасдиқлаш бўйича таклифлар ишлаб чиқилган;

кибер рискларни суғурталаш бўйича ишлаб чиқилган идоравий тусдаги меъёрий ҳужжатларни такомиллаштириш зарурлиги асосланган;

кибер рискларни суғурталаш бўйича суғурта қоидалари ва намунавий суғурта шартномасини ишлаб чиқиш таклиф этилган;

суғурта ташкилотида кибер рискларни суғурталашга ихтисослашган таркибий бўлинма ташкил этиш ва унинг функционал вазифаларини ишлаб чиқиш тавсия этилган;

ахборот ресурслари ва тизимлари қийматини баҳолаш услубиёти такомиллаштирилган ва соддалаштирилган.

**Тадқиқот натижаларининг ишончлилиги** қўлланилган ёндашув ва усулларнинг мақсадга мувофиқлиги, норматив-ҳуқуқий ҳужжатлар, фойдаланилган адабиётлар ва интернет маълумотларининг расмийлиги, жумладан Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ва унинг тизимидаги ихтисослашган ташкилотлар, халқаро суғурта ва бошқа ташкилотларнинг расмий маълумотлари ҳамда ҳисоботларидан фойдаланилганлиги ҳамда тегишли хулоса ва таклифларнинг амалиётга жорий қилинганлиги билан белгиланади.

**Тадқиқот натижаларининг илмий ва амалий аҳамияти.** Тадқиқот натижаларининг илмий аҳамияти ишлаб чиқилган таклифлар Ўзбекистонда кибер рискларни суғурталашнинг услубий асосларини такомиллаштириш, кибер хавфсизликни таъминлашга қаратилган махсус илмий тадқиқотларни амалга оширишда фойдаланиш мумкинлиги билан изоҳланади.

Тадқиқотнинг амалий аҳамияти кибер рискларни суғурталаш тизимини тўлақонли шакллантириш ва талаб даражасида ривожлантириш, бу борада тегишли консалтинг ва олдини олиш тадбирларини амалга ошириб бориш билан бир қаторда кибер рисклар таъсирида етказилган зарарларни бартараф этиш механизмини кенг йўлга қўйишда қўллаш мумкинлиги билан изоҳланади.

**Тадқиқот натижаларининг жорий қилиниши.** Ўзбекистонда кибер рискларни суғурталаш масалалари бўйича ишлаб чиқилган илмий таклифлар ва амалий тавсиялар асосида:

кибер рискларни суғурталашда суғурта объектини ахборот макони ва ахборот-коммуникация технологиялари муҳити категориясининг замонавий тушунчасига мослаш мақсадида суғурта фаолияти классификаторига янги «Номоддий активлар суғуртаси» классини киритиш таклифи Ўзбекистон Республикаси Молия вазирлиги ҳузуридаги Суғурта бозорини ривожлантириш агентлиги томонидан амалиётга жорий этилган (Ўзбекистон Республикаси Молия вазирлиги ҳузуридаги Суғурта бозорини ривожлантириш агентлигининг 2021 йил 9 июндаги КТ/16-02-32-18/839-сон маълумотномаси). Ушбу таклиф Ўзбекистон Республикаси Президентининг

2019 йил 2 августдаги ПҚ-4412-сон қарори билан тасдиқланган «2019-2020 йилларда Ўзбекистон Республикасининг суғурта бозорини ривожлантириш бўйича «Йўл харитаси»га кибер рискларни суғурталашни ишлаб чиқиш ва жорий этиш чора-тадбири сифатида киритилган;

кибер рискларнинг хусусияти, иқтисодий ҳамда ижтимоий оқибатларини ҳисобга олган ҳолда кибер рисклар туркумига кирувчи рисклар тоифасига қараб суғуртанинг ихтиёрий ёки мажбурий шакллари қўллаш таклифи Ўзбекистон Республикаси Молия вазирлиги ҳузуридаги Суғурта бозорини ривожлантириш агентлиги томонидан амалиётга жорий этилган (Ўзбекистон Республикаси Молия вазирлиги ҳузуридаги Суғурта бозорини ривожлантириш агентлигининг 2021 йил 9 июндаги КТ/16-02-32-18/839-сон маълумотномаси). Ушбу таклиф Ўзбекистон Республикаси Президентининг 2019 йил 2 августдаги ПҚ-4412-сон қарори билан тасдиқланган «2019-2020 йилларда Ўзбекистон Республикасининг суғурта бозорини ривожлантириш бўйича «Йўл харитаси»га кибер рискларни суғурталашни ишлаб чиқиш ва жорий этиш чора-тадбири сифатида киритилган;

кибер рискларни суғурталашнинг шартлари ва тариф ставкаларини суғурта маҳсулоти истеъмолчиларининг манфаатларига мослаштиришга қаратилган ягона давлат тизимини яратиш бўйича таклиф Ўзбекистон Республикаси Молия вазирлиги ҳузуридаги Суғурта бозорини ривожлантириш агентлиги томонидан амалиётга жорий этилган (Ўзбекистон Республикаси Молия вазирлиги ҳузуридаги Суғурта бозорини ривожлантириш агентлигининг 2021 йил 9 июндаги КТ/16-02-32-18/839-сон маълумотномаси). Ушбу таклиф Ўзбекистон Республикаси Президентининг 2019 йил 2 августдаги ПҚ-4412-сон қарори билан тасдиқланган «2019-2020 йилларда Ўзбекистон Республикасининг суғурта бозорини ривожлантириш бўйича «Йўл харитаси»га кибер рискларни суғурталашни ишлаб чиқиш ва жорий этиш чора-тадбири сифатида киритилган;

ахборот ресурслари ва тизимлари қийматини баҳолашда суғурта рискига боғлиқликни қўлламаган ҳолда уларни харажат асосида ҳисоблашнинг соддалаштирилган усулини қўллаш бўйича таклифи «UNICON.UZ» давлат унитар корхонаси томонидан амалиётга жорий қилинган («UNICON.UZ» ДУКнинг 2021 йил 14 апрелдаги 1-1/597-сон маълумотномаси). Натижада, «Ахборот тизимлари қийматини ҳисоблаш методикаси» ушбу таклиф асосида қайта ишлаб чиқилган. Янги услубиёт давлат ва хўжалик ҳисобидаги корхона ва ташкилотларнинг мавжуд ахборот ресурслари ва тизимлари бўйича алоҳида ҳисоб юритиши орқали ҳақиқий қийматига яқинлашиш имконини яратган.

**Тадқиқот натижаларининг апробацияси.** Тадқиқот натижалари 6 та илмий-амалий анжуманларда, жумладан 2 та халқаро, 4 та республика миқёсидаги илмий-амалий конференцияларда муҳокамадан ўтказилган.

**Тадқиқот натижаларининг эълон қилинганлиги.** Диссертация мавзуси бўйича жами 12 та илмий иш, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг докторлик диссертациялари асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларда 5 та илмий мақола,

шундан 4 та республика журналларида, 1 та хорижий журналда нашр этилган.

**Диссертациянинг тузилиши ва ҳажми.** Диссертация таркиби кириш, учта боб, хулоса, фойдаланилган адабиётлар рўйхатидан иборат. Диссертация ҳажми 106 бетни ташкил этган.

## ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

**Кириш** қисмида диссертация мавзусининг долзарблиги ва зарурати асосланган, тадқиқотнинг мақсади ва асосий вазифалари, объекти ва предмети тавсифланган, республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, илмий янгилиги ва амалий натижалари баён қилиниб, олинган натижаларнинг илмий ва амалий аҳамияти ёритиб берилган, тадқиқот натижаларининг амалиётга жорий қилиш, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг **«Рақамли иқтисодиётда кибер рискларнинг вужудга келиши ва уларни суғурталашнинг концептуал асослари»** деб номланган биринчи бобида «ахборотлашган жамият», «рақамли иқтисодиёт» атамаларининг юзага келиши ўрганилиб, ахборот-коммуникация технологияларининг жадал ривожланиши натижасида иқтисодиётда ва жамиятда трансформация жараёни юз бераётганлиги, ахборотлашган жамиятнинг шаклланиши, рақамли иқтисодиётга ўтиш жараёни тезлашиб бораётганлиги тадқиқ қилинган, юқори технологик инқилоб содир бўлаётган бундай жамиятда кибер хавфсизликка жиддий таҳдид солаётган янги турдаги рискларнинг, яъни «кибер риск»ларнинг мазмуни, классификацияси ва иқтисодий оқибатлари тадқиқ қилиниб, уларни суғурталашнинг концептуал асослари ўрганилган.

Бугунги кунда рўй бераётган ахборот-коммуникация технологиялари тараққиёти жамият ривожланишининг янги босқичига – ахборотлашган жамиятнинг шаклланишига ва рақамли иқтисодиётга ўтишга технологик базани яратмоқда.

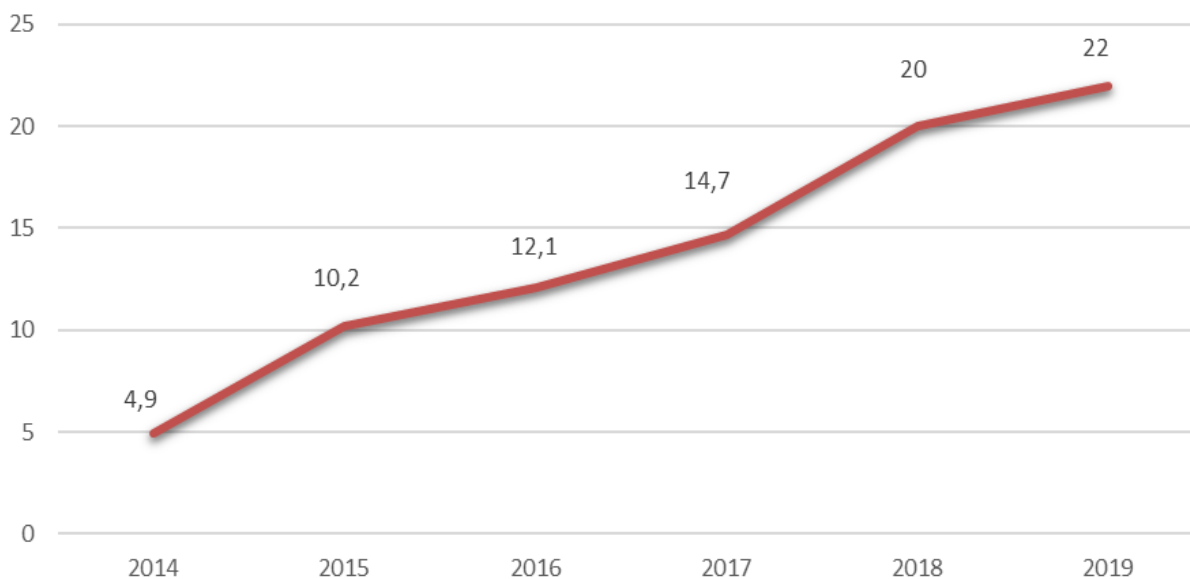
Ҳозирги кунда ривожланаётган давлатларнинг ривожланган давлатлардан фарқи ҳам энг аввало билимлар ва янги технологияларнинг камлиги билан белгиланмоқда, капитал омили эса иккинчи даражали бўлиб қолмоқда. Зеро, жаҳон амалиёти ахборот-коммуникация технологияларининг тараққиёти мамлакатнинг рақобатбардошлигини ошириш, катта оқимдаги ахборотни тўплаш ва умумлаштириш, бошқарувни стратегик даражада ташкил этиш учун кенг имкониятлар яратиб беришда асосий омилга эга эканлигини кўрсатмоқда.

Маълумотларга кўра, 2020 йилда жаҳон бўйича яратилаётган ялпи ички маҳсулотнинг 9 фоизидан ортиғи ахборот-коммуникация технологиялари ҳиссасига тўғри келган. Бундан кўриниб турибдики, замонавий ахборот технологиялари ва дастурий маҳсулотлар даромадли соҳалардан бири

сифатида давлат иқтисодиётини ривожлантиришда муҳим тармоқлардан бирига айланиб бормоқда<sup>8</sup>.

Дарҳақиқат, бундан 20 йил олдин жаҳон аҳолисининг 4,1 фоизигина Интернетдан фойдаланиш имкониятига эга эди. 2019 йилга келиб глобал тармоқдан фойдаланувчилар сони 4,5 млрд. нафардан ошиб кетди. Бу жаҳон аҳолисининг 58,8 фоизи демакдир<sup>9</sup>.

Ўзбекистонда 2019 йил 31 декабрь ҳолатига 22 млн. киши Интернетдан фойдаланмоқда. Ушбу рақам 19 млн. мобил интернет фойдаланувчиларини ҳам ўз ичига олади<sup>10</sup> (1-расм).



**1-расм. Ўзбекистонда Интернет фойдаланувчилари сони, млн. киши<sup>11</sup>**

Расм маълумотларида 5 йил давомида Ўзбекистонда Интернет фойдаланувчилари сони 4,5 баробарга ортганини кўришимиз мумкин.

Келтирилган статистик маълумотлардан хулоса қилиш мумкинки, инсоният ўз ривожланишининг янги палласига қадам қўймоқда. Албатта, инсон фаолиятининг аксарият йўналишларида бўлгани каби ахборотлашган жамият шаклланиб, рақамли иқтисодиётга ўтиш жараёнининг тезлашиб бориши ва ахборот-коммуникация технологияларининг кескин ривожига мос равишда унинг йўналишларига хос янги рисклар юзага келмоқда ва бу рисклар катта миқдордаги иқтисодий талофотларни келтириб чиқармоқда.

Сўнги 20 йил давомида илмий адабиётлар ва бошқа манбаларда «Ахборот рисклари» ёки «Кибер рисклар» тушунчалари тез-тез кўрина бошлади. Бироқ, тадқиқотчилар ва амалиётчиларнинг аксарияти томонидан ушбу атамалар бўйича қабул қилинган аниқ ва тўлиқ талқини ҳали ҳам мавжуд эмас.

<sup>8</sup> «Халқ сўзи» газетаси 24.12.2016 йил сони.

<sup>9</sup> <http://xs.uz/uzkr/post/ozbekistonda-internet-boshqa-davlatlarga-nisbatan-qimmatmi>.

<sup>10</sup> <https://podrobno.uz/cat/tehnp/kolichestvo-internet-polzovateley-v-uzbekistane-sostavlyayet-22-milliona-chelovek/>.

<sup>11</sup> Муаллиф томонидан Интернет маълумотлари асосида ишлаб чиқилган.

«Кибер риск» тушунчаси ҳозирча адабиётда ўзининг тўлиқ таърифига эга эмас. Бу борада турли фикрлар мавжуд. Айримлар бу борада асосан ахборотни турли таъсирлардан ҳимоялашни тушунади, бошқалар эса ахборот рискинни компьютер хавфсизлиги билан боғлайди.

Фикримизча, «Кибер риск» деганда ахборот-коммуникация технологиялари орқали амалга ошириладиган компьютер ва ахборот тизимлари ёки тармоқлари, алоқа тизимлари, ахборот ресурсларига нисбатан учинчи шахсларнинг ноқонуний ҳатти-ҳаракатлари натижасидаги йўқотиш ва/ёки қўшимча харажатлар хавфи тушунилади.

Кибер рискларни иккита катга гуруҳга бўлиш мумкин.

1. Ахборотнинг ходимлар ёки рақобатчилар томонидан хуфёна ўғирланиши;

2. Ахборот узатиш каналларидаги техник носозлик натижасида ахборот йўқотилиши.

Юқорида келтирилган кибер риск гуруҳлари кенг маънода ўз таркибига қуйидагиларни олади:

вируслар таъсири;

компьютер ҳужумлари, яъни хакерлар ва шунга ўхшаш ташқи муҳитдан маълум бир манфаатни кўзлаган ҳолда ҳатти-ҳаракатларни амалга оширувчи ғараз ниятли шахсларнинг таъсири;

корхона ходимларининг ножўя ҳатти-ҳаракатлари оқибатида етказилаётган зарарлар;

корхона сирлари ва махфий маълумотларни ўғирлаш натижасида етказилаётган зиёнлар;

ахборот техник воситалари ва тизимларини ўрнатиш, яратиш ва ишлатишда йўл қўйилиши мумкин бўлган хатолар оқибатида етказилаётган зиёнлар;

турли хил ахборот дастурларининг ишдан чиқиши оқибатида етказилаётган зарарлар ва ҳоказо.

Қуйида келтирилган расмда кибер рискларнинг келиб чиқиши хусусиятларини кетма-кетликда кўришимиз мумкин (2-расм).

Расмдан кўришимиз мумкинки, кибер рисклар даромад кўриш мақсадида қасдан уюштирилган ҳужумлар орқали ёки бирон бир ташкилот ходимининг эҳтиётсизлиги, эътиборсизлиги ҳамда атайин қилган ҳатти-ҳаракатлари оқибатида тасодифий ҳодисаларнинг рўй бериши орқали юзага келади. Натижада, дастлаб ахборот-коммуникация технологияси ускунасига ўрнатилган тизимга таъсир ўтказиб, кейин эса, дастурий таъминотга ва унда мавжуд маълумотлардан фойдаланган ҳолда ғаразли мақсадларини амалга ошириш учун кенг йўл очиб беради, яъни махфий маълумотларни қўлга киритиш орқали бутунлилик принципини бузиш ҳамда тизимдаги барча дастурлардан фойдаланиш имконига эга бўлади. Бунинг оқибатида эса маблағларнинг ўғирланиши, фойданинг бой берилиши ва бошқа товламачиликлардан мислсиз зарарлар кўрилиши мумкин.



**2-расм. Кибер рискнинг келиб чиқиши хусусиятлари<sup>12</sup>**

Сўнгги йилларда кибер рискларнинг салмоғи тобора ортиб бормоқда. «Cybersecurity Ventures» компаниясининг киберхавфсизлик бўйича халқаро экспертлари 2019 йилда жаҳонда ҳар 14 секундда киберхужумлар амалга оширилишини ҳисоблашган. Киберхужумлар сонининг ортиб бориши билан улар таъсирида етказилаётган зарарларнинг салмоғи ҳам кескин кўпаймоқда. Агар, 2018 йилда иқтисодиётнинг турли тармоқларидаги компанияларнинг кўрган умумий зарари 1,5 трлн. АҚШ долларини ташкил этган бўлса, Бутунжаҳон иқтисодий форумининг прогнозига кўра 2022 йилда ушбу кўрсаткич 8 трлн. АҚШ долларига етиши мумкин<sup>13</sup>.

Статистик маълумотларга кўра, Ўзбекистонда ҳам сўнгги йилларда кибер хужумлар сонининг ортиб бориши кузатилмоқда. Бундай салбий ҳолатнинг юзага келиш сабабларидан бири мамлакатимизда ахборот-коммуникация технологияларининг кенг миқёсда жорий қилинаётганлиги ҳисобланади. Масалан, 2018 йилда «UZ» миллий домен зонасида 65 000 га яқин домен мавжуд бўлган бўлса, йил давомида уларнинг сони 74 000 га етди. 2019 йилда Интернет тармоғининг миллий сегменти ахборот тизимлари ва веб-сайтларида 132 000 та кибер ҳавфсизликка таҳдид аниқланган<sup>14</sup>.

Келтирилган рақамлар ва маълумотлардан кўриниб турибдики, рақамли технологиялар тараққий этаётган шароитда кибер рискларнинг салбий иқтисодий оқибатлари кучайиб боради. Шу сабабдан ҳам жаҳон

<sup>12</sup> Тадқиқотлар натижасида муаллиф томонидан ишлаб чиқилган.

<sup>13</sup> Доклад о развитии цифровой экономики в России. Конкуренция в цифровую эпоху: стратегические вызовы для Российской Федерации./ 2018 Всемирный банк.

<sup>14</sup> <http://infocom.uz/2020/03/03/kiberbezopasnost-respubliki-uzbekistan-itogi-2019-goda/>.

хамжамиятида кибер рискларни олдини олиш ва уларнинг салбий иқтисодий оқибатларини камайтириш устувор масалалардан бири бўлиб қолмоқда.

Ахборотни ҳимоя қилиш усули сифатида суғурта танланаётганда, маълумотни йўқотиш ҳаражатлари ва уни ҳимоя қилиш бўйича чоратадбирлар қиймати ўртасида таққослаш амалга оширилиши лозим. Самарадорлик кўрсаткичидан келиб чиқиб, ахборотни ҳимоялашнинг у ёки бу усули танланади.

Кибер суғурта кибер ҳужумлар ва уларнинг салбий оқибатларидан (зарарлардан) ҳимоя қилишнинг иқтисодий усули саналади. Россиялик тадқиқотчи И.К.Иванов ўзининг илмий мақоласида кибер суғуртага қуйидагича таъриф берган: «Кибер суғурта – бизнеси бевосита ёки билвосита маълумотларни ишлаш ёки сақлаш билан боғлиқ ҳар қандай компанияларнинг ахборот рискларини ҳимоя қилишга қаратилган суғурта маҳсулотидир»<sup>15</sup>.

Тадқиқот натижаларининг кўрсатишича, кибер рискларни суғурталаш механизмини яратиш қатор назарий ва амалий масалаларни ҳал этишни тақозо қилади. Бу борада қуйидагиларга эътибор бериш муҳим деб ҳисоблаймиз:

1. Энг аввало бундай механизмнинг норматив-ҳуқуқий асосини етарли даражада шакллантириш лозим. Гап ахборот-коммуникация технологиялари ривожланиши натижасида пайдо бўлаётган янгидан-янги рискларни қонуний жиҳатдан тан олинишини таъминлаш, бу рискларнинг классификациясини ишлаб чиқиш ва такомиллаштириб бориш, рискларни суғурталаш услубиётини ва янги суғурта маҳсулотлари яратиш ҳақида бормоқда.

2. Кибер рискларни суғурталаш механизмнинг муҳим масалаларидан яна бири уларни содир бўлиш оқибатида юзага келиши мумкин бўлган реал зарар миқдорини аниқлаш билан боғлиқ. Чунки, ахборот қиймати ахборот-коммуникация технологиялари субъекти нуктаи назаридан, ушбу ахборотдан кўрадиган манфаати билан ўлчанса, бошқа субъект, шу жумладан суғурталовчи учун бу ахборот ҳеч қандай қийматга эга бўлмаслиги мумкин.

3. Кибер рискларни суғурталашни фақат иқтисодий зарарни қоплаш усули сифатида қарамаслик лозим. Бу усулни қўллаш, энг аввало ахборот объектини чуқур таҳлил этишни ҳамда кибер хавфсизлик тизимини тўлиқ ва атрофлича аудит қилишни тақозо этади. Бундай таҳлил ва аудит қилишнинг асосларини ишлаб чиқиш ҳам кибер рискларни суғурталаш механизмини илмий асослашнинг муҳим босқичи ҳисобланади.

4. Кибер рискларни суғурталаш маҳсулотини ишлаб чиқиш. Бунда рисклар статистикаси асосида суғурта тарифларини белгилаш, рискларнинг хусусиятларини ҳамда суғурталаш шароитларини ҳисобга олган ҳолда суғурта шартномасини яратиш муҳим аҳамият касб этади.

---

<sup>15</sup> Иванов И.К. Кибер-страхование: как обеспечить информационную безопасность бизнесу // Большой портал для малого бизнеса – 2016, №16, С. 13-24.

Кибер рискларни суғурталашда суғурта объекти сифатида ахборот ресурслари (ҳар қандай кўринишдаги ахборотлар – маълумотлар базаси, электрон шаклдаги кутубхоналар ва архивлар, дастурий воситалар) ҳамда молиявий активлар (электрон шаклдаги пул маблағлари ҳамда қимматбаҳо қоғозлар) қабул қилиниши мумкин. Умуман олганда, бу борадаги суғурта полиси ахборотни тўплаш, узатиш, сақлаш ва қайта ишлаш билан боғлиқ барча дастурий-аппарат тузилмаларига хос бўлган рискларни қоплаш имконини бериши лозим.

Диссертациянинг «**Кибер рискларни суғурталашнинг замонавий амалиёти ва унинг таҳлили**» деб номланган иккинчи бобида хорижий мамлакатларда кибер рискларни суғурталашнинг вужудга келиши ва ҳозирги ҳолати тадқиқ қилинган ҳамда Ўзбекистон ахборот технологиялари ва коммуникациялари соҳасида суғурта муносабатларининг ривожланиш ҳолати статистик маълумотлар асосида таҳлил қилинган, бу борада мавжуд муаммолар ўрганилган ва уларни бартараф этиш бўйича таклифлар ишлаб чиқилган. Ўзбекистон ахборот-коммуникация технологиялари соҳасида мавжуд риск-индикаторларни квалитатив (сифат) баҳолаш бўйича социологик тадқиқот натижалари ва кибер рискларни суғурталаш механизмини жорий этиш борасида амалга оширилган тадқиқот ва унинг натижалари келтирилган.

Кибер суғуртанинг келиб чиқишини кўпинча Стивен Хаас номи билан боғлашади. У 1997 йилда «American International Group, Inc» (AIG) билан биргаликда «Интернет хавфсизлиги учун жавобгарлик сиёсати» бўйича биринчи ҳужжатни ёзган<sup>16</sup>. Худди шундай ҳужжат 2000 йилда Лондоннинг Lloyd's суғурта компанияси томонидан ҳам ишлаб чиқилган.

«Кибер суғуртани ривожлантириш бўйича глобал ҳисобот»да<sup>17</sup> қайд этилишича 2025 йилга келиб ушбу йўналишда йиғиладиган суғурта мукофотлари ҳажми 21,4 млрд. АҚШ долларига етади ва шу даврда йиллик ўсиш 27,2 фоизни ташкил этади.

Бугунги кунда кибер суғурта билан шуғулланадиган жаҳоннинг етакчи суғурта компаниялари сирасига қуйидагилар киради: «American International Group, Inc (AIG)», «Allianz Group», «Berkshire Hathaway, Inc.», «Lockton Companies, Inc.», «Chubb Limited», «AXA XL SA», «Tsurich Insurance Group», «Lloyd's Group of London Ltd».

Кибер суғуртанинг қизиқарли дастурларидан бирини Англиянинг Lloyd's компанияси тақдим этган. Полис «Internet Asset and Income Protection Coverage» деб номланиб, унинг муҳим хусусияти хавфсизлик воситалари етказиб берувчисини танлаш имконияти мавжудлиги билан изоҳланади. Бу дастур хавфсизлик тизимида бузилиш ёки унинг ишламай қолиши натижасида ахборот активларини йўқолиши ёки шикаст етиши хавфларини қоплайди<sup>18</sup>.

<sup>16</sup> The Growth and Challenges of Cyber Insurance, Chicago Fed Letter, No. 426, 2019.

<sup>17</sup> Global Cyber Insurance Market (2019-2025).

<sup>18</sup> Косарев А.В. Страхование информационных рисков. – М., 2010.



Россияда кибер рискларни суғурталашнинг пайдо бўлиши ўзининг аниқ санасига эга эмас. Ушбу суғурта турини амалга ошириш бўйича суғурталовчиларнинг айрим ташаббуслари 1997-1999 йилларда бошланган. Шу даврда биринчилардан бўлиб, «Инфострах» ва «Ингосстрах» суғурта компаниялари Россия Федерацияси алоқа вазирлиги билан ушбу соҳада ҳамкорлик қилиш тўғрисида битим тузишган. Ушбу битимга асосан кибер рискларни суғурталашнинг илмий-тадқиқот қисмини Бутунроссия ҳисоблаш техникаси ва ахборотлаштириш муаммолари илмий-тадқиқот институти ўз зиммасига олган. Бироқ, кибер рискларни суғурталашни бошланиш нуқтаси сифатида Россия Федерацияси Президенти томонидан «Россия Федерацияси ахборот хавфсизлиги Доктринаси» тасдиқланган 2000 йил 9 сентябр санасини кўрсатиш тўғрироқ бўлади. Ушбу доктринага биноан кибер хавфсизлик таҳдидларига қарши курашишнинг иқтисодий усуллари сифатида таҳдидлар юз берган тақдирда зарарни қоплашга қаратилган юридик ва жисмоний шахсларнинг кибер рискларни суғурталаш тизимини яратиш кўзда тутилган. Шундан сўнг кўплаб суғурта компаниялари ушбу соҳада фаолият кўрсатиш учун лицензия олишга муваффақ бўлдилар ва бу ҳолат Россия Федерациясида кибер рискларни суғурталаш бозорини шаклланишига шарт-шароит яратди. Ушбу маҳсулотга энг юқори талаб 2000 йилнинг бошларида кузатилди ва суғурта компаниялари юқори миқдорда фойда олиш имкониятига эга бўлди<sup>19</sup>.

Бугунги кунда Россия бозорида кибер суғурта полисини таклиф қилувчи бир қатор суғурта компаниялари мавжуд. «Сбербанк страхование» суғурта компаниясининг прогнозига кўра, Россияда кибер суғурта бозори 2025 йилга келиб 8-10 млрд. рублга етиши мумкин<sup>20</sup>. Таққослаш учун, 2019 йил ўрталарида бу бозорнинг ҳажми 10 млн. рублда баҳоланган.

Умуман, ҳозирги кунда жаҳон бўйлаб кибер рискларни суғурталаш фақатгина корпоратив секторга тақдим этиб келинмоқда. Бунга асосий сабаб шуки, кибер рискларни суғурталашни амалга оширадиган суғурта компаниялари кам миқдорни ташкил қилади ва суғурта хизмати нархи нисбатан юқори (бунда суғурталашдан аввал амалга ошириладиган экспертиза харажатлари ҳам инобатга олинади). Кибер рискларни суғурталаш сегментининг кескин ривожланишига бу йўналишда қонунчиликнинг такомиллашмагани ҳамда бизнеснинг шаффоф эмаслиги, яъни суғурталанаётган субъектларда кутилиши мумкин бўлган зарарни баҳолаш имконияти мавжуд эмаслиги тўсқинлик қилувчи омиллардан ҳисобланмоқда.

Юқорида баён этилганлар билан бир қаторда кибер рискларни суғурталашнинг ривожланишига салбий таъсир этувчи қатор омиллар мавжуд. Буни қуйида келтирилган расм маълумотларидан ҳам кўриш мумкин (3-расм).

<sup>19</sup> Косарев А.В. Страхование информационных рисков. – М., 2010.

<sup>20</sup> <https://tass.ru/ekonomika/7661063>.



### 3-расм. Кибер рискларни суғурталаш бўйича жаҳон савдосига салбий таъсир қилаётган омиллар<sup>21</sup>

Расмдан кўриниб турибдики, кибер рискларни суғурталаш бўйича жаҳон савдосига тўсиқ бўлаётган асосий салбий омиллардан бири кибер рискларни тушунмасликдир.

Тўғри, бундай ҳолат ушбу суғурта турининг янгилиги ва кенг тарқалмаганлиги билан изоҳланади. Бироқ, жаҳон миқёсида юз бераётган рақамлаштириш жараёни киберхавфсизлик масаласини бирламчи поғонага кўтармоқда. Бу ўз навбатида, кибер суғуртага бўлган талабни кескин ортишига, демакки ушбу суғурта турини нафақат корпоратив секторда, балки аҳоли ўртасида кенг оммавийлашишига олиб келади. Бизнинг фикримизча, мижозлар томонидан кибер рискларни тушунмаслик ҳолати мавжуд бўлишига қарамай, яқин истиқболда давлат ва жамият ҳаётининг барча жабҳаларини рақамлаштириш ушбу сегментни кескин ривожланиши учун катта салоҳият мавжудлигидан далолат беради.

Бугунги кунда Ўзбекистон Республикасининг ахборот-коммуникация технологиялари тармоқлари ва воситалари - бу мамлакат иқтисодиётида алоҳида муҳим аҳамиятга молик, такомиллашиб бораётган комплексдир. Чет эллик шериклар ва ҳамкорлар кўмаги билан республикада мазкур соҳани техник ва технологик жиҳатдан қайта жиҳозлаш бўйича салмоқли ишлар амалга оширилмоқда. Ахборот-коммуникация технологияларининг ўсиб бораётган аҳамияти мамлакат иқтисодиётини ривожлантиришда, аҳолига сифатли хизмат кўрсатишда намоён бўлмоқда.

Табиийки, янги технологияларнинг тезкор суръатлар билан ривожланиши улар хусусияти билан боғлиқ турли рискларнинг пайдо бўлиш кўламини кенгайтиради. Иқтисодий тараққиёт ва рисклар миқдорининг ўзгариши ўртасидаги ана шу ўзаро боғлиқликни ўрганиш асосида қуйидаги қонидани таърифлаш мумкин. Яъни, иқтисодиёт техник-технологик

<sup>21</sup> Манба: DELLOITTE UNIVERSITY PRESS, PARTNER RE ADVISEN билан биргаликда.

тараққиётининг ўсиш суръатлари билан рисклар миқдори ва турларининг ортиб бориши ўртасида ўзаро боғлиқлик мавжуд. Бу эса ўз навбатида рискларни бошқаришни, уларга янгича, илғор ёндашувларни узлуксиз равишда қўллаб бориш асосида доимо такомиллаштириб боришни тақозо этади.

Бу ҳолат ахборот-коммуникация технологиялари соҳаси субъектлари фаолиятини сифатли ҳимоя билан таъминлай оладиган замонавий суғурта тизимини шакллантиришни талаб этади. Ўтган давр мобайнида соҳада суғурта муносабатларини шакллантириш ва ривожлантириш йўлида салмоқли ишлар амалга оширилди.

Соҳада суғурта муносабатларини ривожлантириш борасида эришилган натижалар билан бирга ўз ечимини кутаётган муаммолар мавжуд. Улар қуйидагилардан иборат:

1. Соҳада мавжуд корхона ва ташкилотларнинг кўплаб фаолият йўналишлари, ҳамда алоқа объектлари суғурта ҳимояси билан етарли даражада таъминланмай қолмоқда. Булар, авваламбор, эҳтиёткорликни талаб қилувчи ўта нозик қимматбаҳо асбоб-ускуналар, телерадио узатиш станциялари, халқаро лойиҳалар бўйича келтирилаётган қимматбаҳо коммуникация ускуналаридир. Ушбу ҳолатни қуйидаги жадвалда кўришимиз мумкин (1-жадвал).

#### 1-жадвал

#### Ўзбекистон Республикаси ахборот технологиялари ва коммуникациялари соҳасида суғурталанганлик даражаси кўрсаткичи<sup>22</sup>

| Йил  | Кўрсаткичлар              | Асосий воситалар баланси қиймати, млрд. сўм | Транспорт воситалари сони, дона | Ходимлар сони, киши |
|------|---------------------------|---|---------------------------------|---------------------|
| 2012 | Умумий миқдори            | 1 263                                       | 2081                            | 14 796              |
|      | Суғурталанган қисми       | 518,6                                       | 473                             | 6 510               |
|      | Суғурталанганлик даражаси | 41,1 %                                      | 22,7 %                          | 44 %                |
| 2015 | Умумий миқдори            | 1 754,4                                     | 1 658                           | 18 815              |
|      | Суғурталанган қисми       | 274,6                                       | 442                             | 5 724               |
|      | Суғурталанганлик даражаси | 15,6 %                                      | 26,7 %                          | 30,4 %              |
| 2018 | Умумий миқдори            | 2 814                                       | 2 004                           | 19 584              |
|      | Суғурталанган қисми       | 477   | 327                             | 1 277               |
|      | Суғурталанганлик даражаси | 16,9 %                                      | 16,3 %                          | 6,5 %               |

Жадвалдан кўришиб турибдики, соҳада суғурталанганлик даражаси йилдан йилга пасайиб борган. Таъкидлаш жоизки, соҳа ташкилотлари мажбурий суғурта турларидан тўла фойдаланиб келмоқдалар. Ваҳоланки,

<sup>22</sup> Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг Хайъати материаллари асосида муаллиф томонидан тайёрланган.

мажбурий суғурта турлари бўйича фақатгина жабрланган шахсларга етказилган зарарлар қопланади.

2012 йилнинг якунлари бўйича тизимдаги корхона ва ташкилотлардан йиғилган суғурта мукофотлари ҳажмининг «ALSKOM» суғурта компанияси умумий портфелидаги улуши 42,1 фоизни ташкил этган бўлса, 2018 йилнинг якунлари бўйича бу кўрсаткич атиги 7,9 фоизни (4,7 фоизи ихтиёрий, 3,2 фоизи мажбурий суғурта турларига туғри келади) ташкил этди<sup>23</sup>.

Мавжуд муаммони бартараф этиш учун ахборот-коммуникация технологиялари соҳаси корхона ва ташкилотларининг суғурта муносабатларини ривожлантиришга бўлган фаоллигини ошириш талаб этилади. Бунинг учун соҳа корхона ва ташкилотларининг йиллик бизнес-режа ва харажатлар сметасида суғурта ҳимояси учун ажратилган маблағларни чораклар кесимида тўлиқ ўзлаштириш, бунда биринчи навбатда мулк, асбоб-ускуналар (қимматбаҳо ва давлат аҳамиятига молик объектларни, телекоммуникация кабель хўжаликлари, махсус алоқа боғламалари) ва транспорт воситаларини турли рисклардан, ходимларни ижтимоий ҳимоялашга қаратилган ҳаёт ва соғлиқни бахтсиз ҳодисалардан ҳамда тиббий суғурта ҳимояси билан таъминлаш таклиф этилади.

2. Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги тизимидаги корхона ва ташкилотларда «риск-менежмент» тизимининг шаклланишига етарли эътибор берилмаяпти. Холбуки, ахборот-коммуникация технологиялари ривожлангани сари рисклар кўлами ҳам кенгайиб боради.

Мавжуд муаммони бартараф этиш учун соҳа корхона ва ташкилотларида замонавий «риск-менежмент» тизимини шакллантириш, яъни рискларни бошқариш ҳамда суғурта муносабатларини тартибга солиш бўйича вазифаларни бажаришни махсус бўлимга ёки алоҳида ходимга юклаш, корхонанинг фаолиятга хос рискларини ўрганиш, аниқлаш ва уларни олдини олиш тизимини йўлга қўйиш таклиф этилади.

3. Кибер рискларни суғурталаш механизмидан ахборот-коммуникация технологиялари соҳаси корхона ва ташкилотлари етарли даражада фойдаланилмайди. Мазкур йўналишни ривожлантириш ҳамда тизимда кибер суғуртани кенг жорий этиш мақсадида Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг тегишли буйруғи қабул қилинган ҳамда тизимдаги корхона ва ташкилотларга аниқ вазифалар белгиланган. Шундай бўлишига қарамай, соҳадаги йирик корхона ва ташкилотлар белгиланган вазифаларга эътиборсиз муносабатда бўлмоқда.

Мавжуд муаммони бартараф этиш учун кибер рискларни суғурталаш тизимини янги босқичга кўтариш ва кенг оммалаштириш талаб этилади. Бунинг учун Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги томонидан қуйидаги қўшимча чора-тадбирларни амалга оширилишини ўринли деб ҳисоблаймиз:

---

<sup>23</sup> «ALSKOM» суғурта компаниясининг маълумотлари.

1. Ахборот ресурслари ва тизимлари қиймати ҳамда кибер рисклар таъсирида етказилган зарар миқдорини баҳолаш тизимини такомиллаштириш.

2. Қуйидаги йўналишларда фаолиятни ташкил этиш:

- кибер хавфсизлик даражасини экспертиза қилиш;
- кибер рисклар таъсирида етказилган зарарни баҳолаш;
- кибер рискларни суғурта қилиш тизимини кенг оммалаштириш;
- суғурталанганлик ҳолатини доимий мониторинг қилиш.

3. Соҳа ходимларининг кибер хавфсизлик йўналишида малакаларини ошириш ва бу йўналишда кадрлар тайёрлаш тизимини йўлга қўйиш.

4. Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ва ахборот-коммуникация технологиялари соҳасида фаолият юритувчи субъектлар ўртасида тузиладиган лицензия келишувига кибер рискларни суғурталаш зарурлиги тўғрисидаги талабларни киритиш.

5. Суғурта компанияларида кибер рискларни суғурта қилиш борасида тегишли вазифаларни амалга оширишга ихтисослашган таркибий бўлинмани ташкил этиш ва унинг асосий вазифаларини белгилаш.

Қайд этиб ўтилган вазифаларнинг бажарилиши Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги тизимида суғурта муносабатларини ривожлантиришга, пировардида, тизимда фаолият юритувчи корхона ва ташкилотларнинг барқарор фаолият юритилишини таъминлашга хизмат қилади.

2010 йилда диссертант ва бошқа тадқиқотчилар томонидан таклиф этилган услубиётга мувофиқ, ахборот-коммуникация технологиялари муҳити элементлари ҳаракатининг риск-индикаторларини квалитатив (сифат) баҳолаш социологик тадқиқот ўтказиш йўли билан амалга оширилган. Мазкур социологик тадқиқот Ўзбекистон алоқа ва ахборотлаштириш агентлиги (ҳозирда Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги)нинг 2010 йил 4 майдаги 27-ф-сонли фармойишига асосан Тошкент ахборот технологиялари университети ва «ALSKOM» суғурта компанияси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Социологик тадқиқотлар институти билан ҳамкорликда Ўзбекистон ахборот-коммуникация технологиялари соҳаси таркибига кирувчи корхона ва ташкилотларнинг раҳбар ходимлари ва мутахассисларидан иборат респондентлар ўртасида «Ўзбекистон ахборот-коммуникация технологиялари соҳасида риск-менежментнинг ҳолати ва ривожланиш истикболлари» мавзусида ўтказилган. Социологик тадқиқотнинг натижалари бугунги кунда ҳам ўз долзарблигини йўқотган эмас.

Ўзбекистон ахборот-коммуникация технологиялари соҳасининг 34 та субъектида рискларни бошқариш бўйича раҳбар ва мутахассислар ўртасида ўтказилган социологик сўровнинг муҳим хулосаларидан бири шуки, рисклардан умуман қочиш эмас, балки яхши тизимли таҳлил иши орқали

хўжалик элементларининг ҳаракатини белгиланган йўналишлардан четлашиб кетмаслигини, яъни оқибати оғир рискларга йўлиқиб қолмаслигини узлуксиз кузатиб бориш муҳимроқдир. Бундан мақсад элементнинг ҳаракати давомида унинг риск томон оғишини ўз вақтида аниқлаш ва тегишли чора кўришдир. Ушбу хулоса моҳиятан риск тоифаларининг юқорида ифодалаб берилган янги талқинини ҳамда ундан келиб чиқадиган рискларни бошқаришга янги ёндашувнинг мазмунини тасдиқлайди.

Тадқиқот натижаларини ҳисобга олган ҳолда ҳамда кибер хавфсизлик устуворлигини таъминлаш мақсадида Ўзбекистон алоқа ва ахборотлаштириш агентлиги (ҳозирда Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги)га республикада кибер рискларни комплекс суғурта қилиш механизминини ишлаб чиқиш ва жорий этиш ташаббуси билан чиқилди. Бу ташаббус мазкур давлат органининг 2005 йилдаги кенгайтирилган Ҳайъат мажлисида маъқулланган. Ҳайъат ўз қарори билан кибер рискларни суғурталашнинг илмий асосларини ўрганиш бўйича илмий-тадқиқот ишлари ва унинг асосида тегишли меъёрий база ишлаб чиқиш дастурини тасдиқлаган. Бу борада ишчи гуруҳ ташкил этилиб, унинг таркибига мазкур диссертация муаллифи ҳам киритилган.

Ўтказилган тадқиқотлар натижасида қуйидаги меъёрий ҳужжатлар ишлаб чиқилди:

1. Ахборот рискларини суғурта қилиш қоидалари. Қоидалар суғурта қилиш тартиби ва шартларини белгилайди.

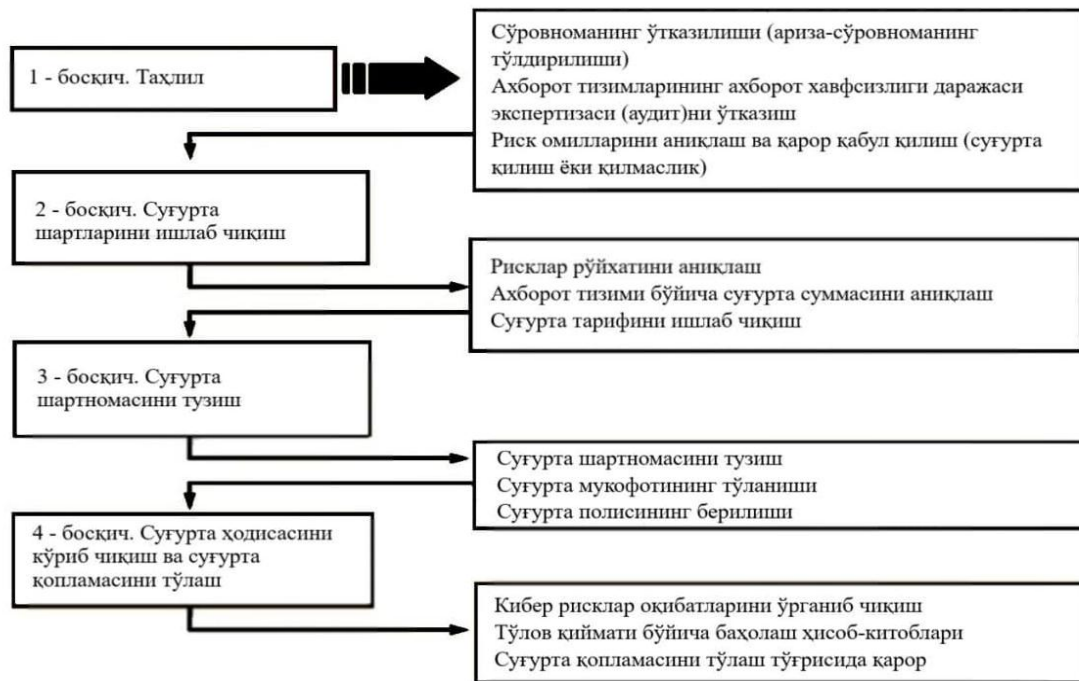
2. Ахборот тизимлари қийматини ҳисоблаш методикаси. Унда ахборот ресурсларнинг йўқ бўлиб кетиш ҳолатида уни қайта тиклашга кетадиган қийматнинг ҳисоби келтирилган.

3. Зарарни баҳолаш ва суғурта қопламаси суммасини белгилаш методикаси. Унда рискларни аниқлаш, зарар ва таҳдидни баҳолаш, шунингдек, кибер рискларини суғурта қилишда мумкин бўлган зарарни аниқлаш, ҳамда етказилган зарар бўйича тўланадиган суғурта қопламаси миқдорини аниқлаш кўзда тутилган.

4. Ахборот тизимлари хавфсизлиги экспертизаси (аудит)ни ўтказиш бўйича йўриқнома. Ушбу йўриқнома тармоқда ахборот ҳимояси бўйича мавжуд камчиликларни аниқлаш ва ахборотнинг йўқолиши билан боғлиқ ҳодисани текширишга мўлжалланган ахборот тизимлари экспертизасини ўтказиш тартибини белгилайди.

Яратилган меъёрий ҳужжатларнинг янгилигини инобатга олиб, Ўзбекистон алоқа ва ахборотлаштириш агентлиги (ҳозирда Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги)нинг 2009 йил 11 майдаги 150-сон буйруғи билан мазкур ҳужжатларни соҳанинг айрим корхона ва ташкилотларида тажриба тарзида қўлланилиши белгиланди ва бу борада амалга оширилиши лозим бўлган чора-тадбирлар режаси тасдиқланди.

Кибер рискларни суғурталаш борасида яратилган механизмни тажриба тарзида қўллаш қуйидаги босқичларда амалга оширилди (4-расм).



**4-расм. Кибер рискларини суғурта қилиш жараёнини амалга ошириш босқичлари<sup>24</sup>**

Яратилган меъёрий ҳужжатларни тажриба тарзида қўллаш уларни амалиётда синаб кўриш ва мавжуд камчиликларни аниқлаш имконини берди. Диссертант томонидан аниқланган камчилик ва муаммоларни бартараф этиш юзасидан таклифлар ишлаб чиқилган. Аниқланган камчиликларни бартараф этган ҳолда меъёрий ҳужжатларни амалиётда кенг жорий этиш мумкин саналади.

Диссертациянинг «**Ўзбекистонда рақамли иқтисодиётни жорий этиш шароитида кибер рискларни суғурталашни ривожлантириш йўллари**» деб номланган учинчи бобида Ўзбекистоннинг рақамли иқтисодиётга ўтиш шароитида кибер рискларни суғурталашни кенг жорий этиш ва ривожлантириш борасида аниқ таклифлар ишлаб чиқилган ҳамда ахборот ресурслари ва тизимлари қийматини баҳолаш услубиётини такомиллаштириш бўйича илмий хулоса ва таклифлар ишлаб чиқилган.

Энг янги рақамли технологиялар ва дастурларга таянган замонавий иқтисодиётнинг ривожланиши иқтисодиёт ва унинг тармоқларини ривожланиш суръатини ошириш, иқтисодиёт субъектлари ўртасида ўзаро муносабатларни оптималлаштириш, таннархни пасайтириш орқали даромад миқдорини ошириш ва шу каби юқори самарадорлик кўрсаткичларини таъминлашга хизмат қилади.

Ўзбекистонда сўнгги йилларда рақамли иқтисодиётга ўтиш борасида илдам қадамлар қўйилди. Миллий иқтисодиётимизни тубдан модернизация

<sup>24</sup> Муаллиф томонидан ишлаб чиқилган.

қилиш бўйича олиб борилаётган кенг камровли ислохотлар доирасида мамлакатимиз ижтимоий-иқтисодий ҳаёти ва давлат бошқаруви тизимига рақамли технологияларни жорий этиш борасида қатор чора-тадбирлар амалга оширилди. Хусусан, Ўзбекистон Республикаси Президентининг 2018 йил 3 июлдаги ПҚ-3832-сон «Ўзбекистон Республикасида рақамли иқтисодиётни ривожлантириш чора-тадбирлари тўғрисида»ги қарорининг қабул қилиниши мамлакатимизда рақамли иқтисодиётни ривожлантиришда муҳим қадам бўлиб, унда энг муҳим вазифалар белгилаб берилди.

Бундан ташқари Ўзбекистон Республикаси Президенти Ш.Мирзиёев 2020 йил 25 январда Олий Мажлисга Мурожаатномасида кўтарилган масала ва мақсадлардан келиб чиқиб, Ўзбекистонда 2020 йил – «Илм, маърифат ва рақамли иқтисодиётни ривожлантириш йили» деб эълон қилинди ва бу борада Президент фармони қабул қилинди ва Давлат дастури тасдиқланди.

Ҳужжатда мамлакатимизда иқтисодиётнинг барча тармоқларини сўнгги ахборот технологиялари ва дастурларини кенг жорий қилиш орқали рақамлаштириш билан бирга киберхавфсизлик бўйича ҳам қатор чоралар белгиланган. Ушбу чоралардан энг муҳими Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида»ги Қонуни лойиҳасини ишлаб чиқиш саналади. Зеро, рақамли иқтисодиётни жорий қилиш кибертаҳдидларни вужудга келишига сабаб бўлади.

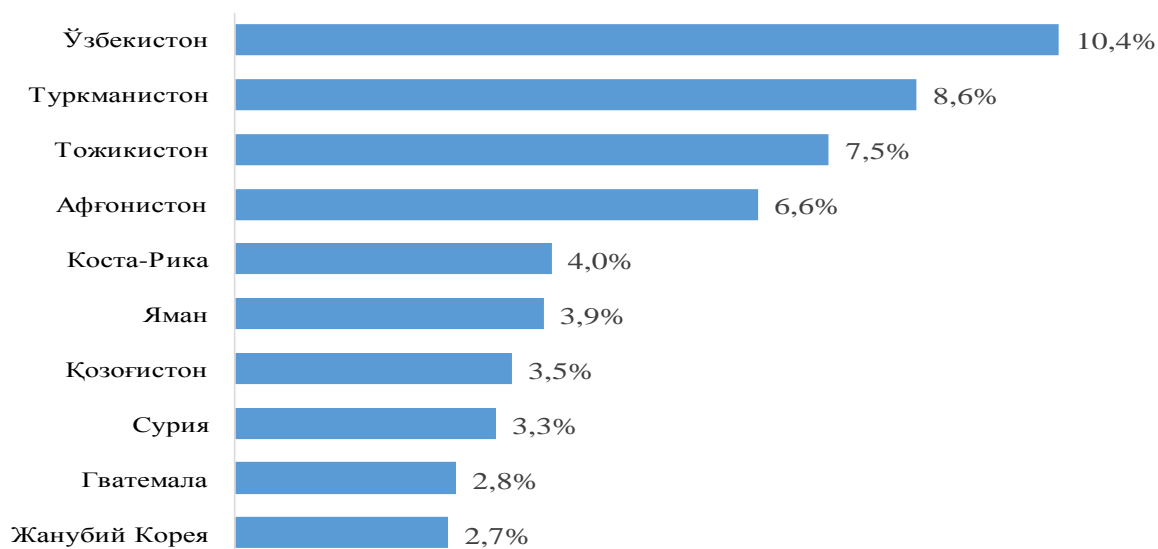
Дарҳақиқат, Ўзбекистонда ҳам бошқа давлатларда бўлгани сингари киберхужумлар сонининг ортиши кузатилмоқда. Биргина 2019 йилнинг 9 ойида 8 миллион дон шундай ҳолат аниқланиб, уларнинг бир қисми ўта хавфли даражада бўлган. Бу ҳақда Ўзбекистон Республикаси Бош вазири А.Арипов «Очиқ инновациялар» халқаро форумида алоҳида тўхталиб ўтган. Шу сабабдан мамлакатда рақамли маълумотларнинг хавфсизлигини таъминлаш бўйича комплекс дастур қабул қилинган бўлиб, унинг доирасида киберхавфсизлик соҳасида 70 та турли тартибга солувчи ҳужжатлар қабул қилинган. А.Ариповнинг қайд этишича, мамлакатимиздаги барча давлат муассасалари электрон алмашинувни ахборот узатишнинг ҳимояланган тизими орқали амалга ошира бошлади. Кўрилган чоралар Ўзбекистонни киберхавфсизлик бўйича глобал индексда 40 поғонага кўтарилиб, 175 мамлакат орасида 52-ўринга чиқишини таъминлади<sup>25</sup>.

2020 йилда банк вирусли ҳужумларидан зарар кўрганлар сони бўйича Ўзбекистон мамлакатлар рейтингда биринчи ўринни эгаллади. 2020 йили Ўзбекистонда фойдаланувчиларнинг 10,4 фоизи банк вирус ҳужумига учраган (5-расм).

---

<sup>25</sup> Манба: [https://sputniknews.ru/novosti\\_uzbekistan/20191023/1030087801/uzbekistan-stolknulsya-rostom-kiberatak.html](https://sputniknews.ru/novosti_uzbekistan/20191023/1030087801/uzbekistan-stolknulsya-rostom-kiberatak.html).





Хужумга учраган фойдаланувчилар улуши

### 5-расм. 2020 йилда банк вирусли хужумлари кузатилган мамлакатлар рейтингини<sup>26</sup>

«Илм, маърифат ва рақамли иқтисодиётни ривожлантириш йили» Давлат дастурида киберхавфсизлик борасида белгиланган вазифа ва топшириқларнинг амалга оширилиши, шубҳасиз, киберхужумлар оқибатида кўриладиган зарарларни камайтиришга хизмат қилади. Шу билан бирга, жаҳон амалиётида киберхавфсизликни таъминлаш борасида кенг оммалашиб бораётган кибер рисклардан суғурталаш услубини Ўзбекистонда ривожлантириш киберхужумлар оқибатида етказиладиган зарарларни бартараф этишда юқори самара беради, деб ҳисоблаймиз. Мазкур услуб суғурта ташкилотлари томонидан ахборот муносабатлари субъектларига кибер хавфсизликка таҳдид солинганда кўриладиган иқтисодий зарарни қоплаш бўйича кафолат беришга асосланади.

2020 йил Ўзбекистонни рақамли технологияларга асосланган иқтисодиётга трансформация қилиш бўйича янги босқичга кўтарилишига тurtки бўлган йил бўлди. Юқорида келтирилган фикрлар асосида мамлакатимизни рақамли иқтисодиётга ўтиши кибер рискларни суғурталаш тизимини ривожлантириш ва кенг оммалаштиришга даъват қилади. Бу борада қуйидаги таклифларни амалга оширишни мақсадга мувофиқ, деб ҳисоблаймиз:

1. Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида»ги Қонуни лойиҳасига Ўзбекистонда кибер рискларни суғурталашни ривожлантириш масалаларини киритиш лозим.

2. Кибер рискларни суғурталаш бўйича тегишли норматив-ҳуқуқий ҳужжатни қабул қилиш мақсадга мувофиқ. Мазкур ҳужжат билан кибер рискларни суғурталашнинг шакли ва тартибини тасдиқлаш талаб этилади.

Фикримизча, Ўзбекистонда кибер рискларни суғурталаш ахборот хавфсизлигини таъминлашнинг муҳим воситаси эканлигини эътиборга олиб,

<sup>26</sup> Манба: <https://www.statista.com/statistics/325226/countries-by-users-attacked-by-financial-malware/#statistic> Container.

кибер рискларнинг хусусияти, иқтисодий ҳамда ижтимоий оқибатларини ҳисобга олган ҳолда кибер рисклар туркумига кирувчи рисклар тоифасига қараб суғуртанинг ихтиёрий ёки мажбурий шакллари кўллаш мақсадга мувофиқ.

3. Ўзбекистон Республикасида суғурта фаолияти классификатори ахборот ресурслари ва ахборот тизимларини суғурталашнинг махсус классига, шунингдек, бундай турдаги суғурталашни ўтказиш шартлари бўйича талаб ва мазмунга эга эмас. Шунинг учун амалиётда ҳозиргача кибер рискларни суғурталашни мулкӣ суғурта турлари классига ўтказиш тажриба қилинмоқда. Бу ахборот макони ва ахборот-коммуникация технологиялари муҳити категориясининг замонавий тушунчасига мос келмайди. Шу сабабли, Ўзбекистон Республикасида амалда бўлган суғурта фаолияти классификаторига янги «18-класс – «Номоддий активлар суғуртаси»ни киритишни таклиф этамиз.

4. Кибер рискларни суғурталашда ахборотнинг қийматини баҳолаш борасида такомиллашган услубиётни яратиш мақсадга мувофиқ. Зеро, бугунги кунда ушбу йўналишда юзага келаётган энг катта муаммо бу ахборотнинг аниқ қийматини аниқлаш ҳисобланади.

Келтирилган таклифларни амалга оширилиши ушбу йўналишда суғурта муносабатларини тўлақонли шакллантириш ва талаб даражасида ривожлантириш, бу борада тегишли консалтинг ва олдини олиш тадбирларини амалга ошириб бориш билан бир қаторда рисклар таъсирида етказилган зарарларни фаолият барқарорлигига таъсир этмаган ҳолда бартараф этиш механизмининг кенг йўлга қўйишни таъминлайди.

Ўзбекистон алоқа ва ахборотлаштириш агентлиги (ҳозирда Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги)нинг 2008 йил 1 декабрдаги 332-сон буйруғи билан тасдиқланган амалдаги «Ахборот тизимлари қийматини ҳисоблаш методикаси» бўйича ахборот ресурслари ва тизимлари қийматини баҳолашда уларни сотиб олиш, яратиш ва амалга киритиш билан боғлиқ харажатлардан келиб чиқилади. Яъни, ахборот тизимини баҳолаш ахборот ресурслари, ахборот технологиялари ва алоқа воситалари ҳамда кибер рискларига қарши ҳаракат механизмларини тиклаш учун талаб этиладиган харажатлардан келиб чиқиб амалга оширилади.

Тадқиқот натижаларининг кўрсатишича, мазкур Методиканинг 3.3-бандида суғурта ҳодисаси юз берганда ахборот тизимларини тиклаш қийматини ҳисоблаш бўйича асосий кўрсаткичлар кўрсатиб ўтилган. Аммо, олдиндан қандай суғурта ҳодисаси рўй бериши мумкинлигини, аниқроқ қилиб айтганда, шу бандда кўрсатиб ўтилганидек ахборот ресурсини тиклаш вақтини, тиклаш учун жалб этиладиган мутахассисларнинг сонини, ахборот ресурсини тиклаш учун ижарага олинадиган усқунанинг қийматини инобатга олишнинг имконияти мавжуд эмас.

Тадқиқот натижаларига асосланиб, ахборот ресурслари ва тизимлари қийматини ҳисоблаш борасида ишлаб чиқилган қуйидаги содалаштирилган услубиётни жорий этиш тавсия этилади:

- ахборот ресурси қийматини ҳисоблашда ходимнинг (ахборот ресурсини таъминловчи мутахассиснинг) ўртача ойлик иш ҳақи, ахборот ресурси бўйича иш олиб боровчи ходимларнинг сони ва ахборот ресурсидан фойдаланиш даври (ишга туширилган санадан суғуртага қабул қилинаётган санагача) кўпайтмаси ҳисобга олинади;

- ахборот тизими қийматини ҳисоблашда ахборот технологияларининг баланс қиймати, дастурий таъминотларнинг баланс қиймати ва ахборот ресурсларининг қиймати йиғиндиси олинади.

## ХУЛОСА

Ўзбекистонда кибер рискларни суғурталаш масалалари мавзусида олиб борилган илмий тадқиқотлар натижасида қуйидаги хулосалар шакллантирилди:

1. Ўрганиш натижалари ва таҳлиллар шуни кўрсатмоқдаки, кибер рисклар ва ҳужумлар сонининг ортиб бориши билан улар таъсирида етказилаётган зарарларнинг салмоғи ҳам кескин кўпаймоқда. Шу сабабдан ҳам киберхавфсизлик масаласи ҳозирги замон жамиятининг долзарб ва ўта муҳим масаласига айланди.

2. Амалга оширилган тадқиқот натижалари киберхавфсизликни таъминлашда риск-менежментнинг ўрни муҳимлигини тасдиқлади. Кибер рискларни суғурталаш механизми ҳозирги замон риск-менежмент тизимининг иқтисодий усули сифатида ўрганилди ва унинг концептуал асослари таҳлил қилинди. Ахборотни ҳимоя қилиш усули сифатида суғурта танланаётганда, маълумотни йўқотиш харажатлари ва уни ҳимоя қилиш бўйича чора-тадбирлар қиймати ўртасида таққослаш амалга оширилиши лозим.

3. Тадқиқот натижалари кибер рискларни суғурталаш бўйича жаҳон савдосига тўсиқ бўлаётган асосий сабаб кибер рискларни тушунмаслик ҳисобланишини кўрсатди. Тўғри, бундай ҳолат ушбу суғурта турининг янгилиги ва кенг тарқалмаганлиги билан изоҳланади. Бироқ, жаҳон миқёсида юз бераётган рақамлаштириш жараёни киберхавфсизлик масаласини бирламчи поғонага кўтармоқда. Бу ўз навбатида, кибер суғуртага бўлган талабни кескин ортишига, демакки ушбу суғурта турини нафақат корпоратив секторда, балки аҳоли ўртасида кенг оммалашшига олиб келади. Бугунги кунда кибер рискларни тушунмаслик ҳолати мавжуд бўлишига қарамай, истикболда ушбу сегментни кескин ривожланиши учун катта салоҳият мавжудлигидан далолат беради, деб ҳисоблаймиз.

4. Ўзбекистонда ахборот-коммуникация технологияларининг тезкор суръатлар билан ривожланиши уларнинг хусусияти билан боғлиқ рискларнинг пайдо бўлиш тезлигини ҳам оширади. Бу ўз навбатида, мазкур соҳа субъектлари фаолиятини сифатли ҳимоя билан таъминлай оладиган замонавий суғурта тизимини шакллантиришни талаб этади. Бу борада ишлаб чиқилган таклиф ва тавсияларни амалда қўлланилиши соҳада суғурта муносабатларини ривожлантиришга, пировардида, тизимдаги корхона ва

ташкilotларнинг барқарор фаолият юритилишини таъминлашга хизмат қилади.

5. Ахборот ресурслари ва тизимлари хавфсизлиги даражасини экспертиза (аудит) қилиш ҳамда уларнинг қийматини баҳолашни суғурталанувчилар ҳисобидан амалга оширилишини жорий этиш мақсадга мувофиқ. Ахборот ресурслари ва тизимлари хавфсизлик даражасини экспертиза қилиш суғурта қилиш ёки қилмасликдан қатъий назар амалга оширилиши лозим. Бу риск-менежментнинг муҳим талабларидан бири саналади. Зеро, ахборот ресурслари ва тизимларининг эгаси хавфсизлик даражасини доимий мониторинг қилиб бориши ва шунга кўра тегишли хавфсизлик чора-тадбирларни ишлаб чиқиши ва амалга ошириши талаб этилади. Хавфсизлик даражаси юқори бўлган ҳолатда суғурта ҳимоясига эҳтиёж мавжуд бўлмайди ёки суғурта ҳимояси арзон нархда амалга оширилади.

6. Ўзбекистонда кибер рискларни суғурталаш ахборот хавфсизлигини таъминлашнинг муҳим воситаси эканлигини инобатга олиб, кибер рискларнинг хусусияти, иқтисодий ҳамда ижтимоий оқибатларини ҳисобга олган ҳолда кибер рисклар туркумига кирувчи рисклар тоифасига қараб суғуртанинг ихтиёрий ёки мажбурий шакллари қўллаш мақсадга мувофиқ.

7. Ўзбекистон Республикасида суғурта фаолияти классификатори ахборот ресурслари ва ахборот тизимларини суғурталашнинг махсус классига, шунингдек, бундай турдаги суғурталашни ўтказиш шартлари бўйича талаб ва мазмунга эга эмас. Шунинг учун амалиётда ҳозиргача кибер рискларни суғурталашни мулкӣ суғурта турлари классига ўтказиш тажриба қилинмоқда. Бу ахборот макони ва ахборот-коммуникация технологиялари муҳити категориясининг замонавий тушунчасига мос келмайди. Шу сабабли, Ўзбекистон Республикасида амалда бўлган суғурта фаолияти классификаторига янги «18-класс – «Номоддий активлар суғуртаси» классини киритиш мақсадга мувофиқ.

8. Ахборот ресурслари ва тизимлари қийматини баҳолашда суғурта рискига боғлиқликни қўлламаган ҳолда уларни харажат усулида ҳисоблаш мақсадга мувофиқ.

**НАУЧНЫЙ СОВЕТ DSc.03/30.12.2019.I.17.01  
ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ ПРИ  
ТАШКЕНТСКОМ ФИНАНСОВОМ ИНСТИТУТЕ**

---

**ТАШКЕНТСКИЙ ФИНАНСОВЫЙ ИНСТИТУТ**

**ХАСАНОВ ФАРРУХ РАВШАНОВИЧ**

**ВОПРОСЫ СТРАХОВАНИЯ КИБЕР РИСКОВ В УЗБЕКИСТАНЕ**

**08.00.07 – Финансы, денежное обращение и кредит**

**АВТОРЕФЕРАТ**  
**диссертации доктора философии (Doctor of Philosophy) по экономическим наукам**

**город Ташкент – 2022 год**

Тема диссертации доктора философии (Doctor of Philosophy) зарегистрирована Высшей аттестационной комиссией при Кабинете Министров Республики Узбекистан за №В2020.2.PhD/Iqt1372

Диссертация выполнена в Ташкентском финансовом институте.

Автореферат диссертации на трех языках (узбекском, русском, английском (резюме)) размещен на веб-странице Научного совета (www.tfi.uz) и Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).


- Научный руководитель:** Шеннаев Хужаёр Мусурманович  
доктор экономических наук (Dsc), доцент
- Официальные оппоненты:** Кузиева Наргиза Рамазоновна  
доктор экономических наук, профессор
- Хамидулин Михаил Борисович  
доктор экономических наук, профессор
- Ведущая организация:** Ташкентский Государственный экономический университет

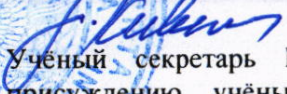
Защита диссертации состоится «28» 01 2022 года в 16:00 ч. на заседании Научного совета DSc.03/30.12.2019.I.17.01 по присуждению ученых степеней при Ташкентском финансовом институте. Адрес: 100000, г.Ташкент, ул. Амира Темура, 60а. Тел.: (99871) 234-53-34, факс: (99871) 234-46-26, e-mail: ilmiykengash@tfi.uz.

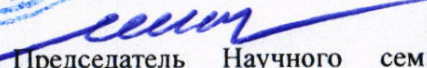
С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского финансового института (зарегистрировано под номером №251). Адрес: 100000, г.Ташкент, ул. Амира Темура, 60а. Тел.: (71) 234-53-34, e-mail: admin@tfi.uz.

Автореферат диссертации разослан «14» 01 2022 года.  
(протокол реестра №10 от «14» 01 2022 года).



  
**Т.З.Тешабаев**  
Председатель Научного совета по присуждению учёных степеней, доктор экономических наук, профессор

  
**Ф.К.Холмаматов**  
Учёный секретарь Научного совета по присуждению учёных степеней, доктор философии по экономическим наукам (PhD), доцент

  
**И.Н.Кузиев**  
Председатель Научного семинара при Научном совете по присуждению учёных степеней, доктор экономических наук, профессор

## **ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))**

**Актуальность и необходимость темы диссертации.** Открылась новая эра для мирового сообщества. Это объясняется проникновением информационно-коммуникационных технологий во все сферы и отрасли. Повседневная деятельность людей стала тесно связана с информационно-коммуникационными технологиями. Большинство стран мира начали принимать систему цифровой экономики, и эти изменения в конечном итоге служат благосостоянию человечества. В то же время быстрое проникновение информационных и коммуникационных технологий в нашу повседневную жизнь создает новые риски, угрожающие кибербезопасности. Эти риски известны в международной практике как киберриски, и их негативные последствия могут иметь пагубные последствия в глобальном масштабе. Генеральный секретарь ООН Антониу Гутерриш не случайно прокомментировал ситуацию: «Цифровая экономика может создать новые угрозы, включая угрозы кибербезопасности, ослабление незаконной экономической деятельности и нарушение конфиденциальности...»<sup>1</sup>. По этой причине кибербезопасность становится одной из самых актуальных проблем мирового сообщества, и повсеместное внедрение и развитие системы страхования киберрисков считается перспективным направлением в решении этих проблем.

В мировой практике научно изучается ряд методов и инструментов системы управления рисками, направленных на обеспечение кибербезопасности, в частности, предотвращение киберрисков и снижение их негативных последствий. Эти исследования сосредоточены на технических средствах кибербезопасности, таких как криптографическая защита и шифрование данных, сбор средств, распределение рисков (диверсификация), стандартизация (сертификация, лицензирование). Однако, эти исследования неадекватно рассматривают вопросы страхования киберрисков, поэтому существует потребность в научных исследованиях в этой области.

Быстрые шаги, предпринятые в Узбекистане для дальнейшего развития информационно-коммуникационной системы, внедрения цифровой экономики, в свою очередь, требуют разработки механизма управления кибербезопасностью. В стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан на 2017-2021 годы отмечено «расширение и улучшение объема и качества новых видов страховых, лизинговых и других финансовых услуг, привлечение капитала и развитие фондового рынка как альтернативного источника размещения свободных ресурсов предприятий, финансовых институтов и населения»<sup>2</sup>. Поэтому необходимость развития системы страхования киберрисков в сфере кибербезопасности, в частности, необходимость соответствующего научно-методического подхода, а также развития и совершенствования действующих

<sup>1</sup> Дорожная карта Генерального секретаря ООН по цифровому сотрудничеству. <https://www.un.org/ru/content/digital-cooperation-roadmap/>.

<sup>2</sup> Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги Фармони.

нормативных документов, определяет актуальность выбранной темы исследования.

Данная диссертационная работа в определенной степени способствует реализации поставленных задач Указами Президента Республики Узбекистан от 7 февраля 2017 года УП-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан», от 2 марта 2020 года УП-5953 «О Государственной программе реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах в «Год науки, просвещения и цифровой экономики», постановлением Президента Республики Узбекистан от 2 августа 2019 года ПП-4412 «О мерах по реформированию и обеспечению ускоренного развития страхового рынка Республики Узбекистан», а также другими нормативно-правовыми актами, относящимся к этим сферам.

**Соответствие исследований приоритетам развития науки и технологий республики.** Данное диссертационное исследование выполнено в рамках приоритетного направления науки и технологий в республике I. «Духовно-нравственное и культурного развития демократического и правового общества, формирование инновационной экономики».

**Степень изученности проблемы.** Вопросы страхования киберрисков исследованы в трудах западных ученых Дж.П.Кесана и Н.Шетти, Р.Беме, Р.Пала<sup>3</sup>. Работа экономистов СНГ А.Н.Иващенко, С.А.Смирнова, Н.В.Косыгиной, Е.В.Небольсиной, Н.И.Артамонова<sup>4</sup> посвящена рынку киберстрахования и методологии киберстрахования. Ученые и специалисты нашей страны С.С.Гуломов, Т.К.Иминов, Р.Х.Хусанов, Н.Р.Кузиева, М.Б.Хамидулин, К.М.Кулдошев, Х.М.Шеннаев, Б.Б.Ашрафханов, М.А.Мирсадилов, А.А.Ядгаров, А.Давлатов, И.Х.Абдурахманов, Б.С.Гайбуллаев, И.Мавлонова<sup>5</sup> изучали различные аспекты страховой

<sup>3</sup> Kesan J.P., Majuca R.P., Yurcik W.J. The Economic Case of Cyberinsurance; Shetty N., Schwartz G., Felegyhazi M., Walrand J. Competitive Cyber-Insurance and Internet Security. In: Workshop on Economics of Information Security (WEIS). University College London, 2009; Böhme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework; Pal R., Golubchik L., Psounis K. A Novel Cyber-Insurance Model.

<sup>4</sup> Ivashchenko A.N., Sharko I.A. [The world cyber risk insurance market: Opportunities and obstacles for development in the Republic of Belarus]. Материалы IX Международной научно-практической конференции студентов «Национальная экономика Республики Беларусь: проблемы и перспективы развития». Минск, 2016, С. 196–202; Смирнов С.А. Страхование киберрисков в России: анализ состояния и перспективы развития // Сборник научных работ / под ред. Г.Д. Дроздова. СПб., 2015. С. 303–306; Kosygina N.V., Anpilogova V.S. [Cyber risks and their insurance in the sphere of banking services]. Материалы II Международной научно-практической конференции «Актуальные вопросы экономики и финансов в условиях современных вызовов российского и мирового хозяйства». Самара, 2014, С. 203–204; Nebol'sina E.V. [Cyber risks as a global problem of the modern world]. Strakhovoe delo = Insurance Business, 2016, no. 1, pp. 22–28; Артамонов Н.И. Управление киберрисками в системе риск-менеджмента предприятий малого и среднего бизнеса // Страхование. 2015. № 4. С. 53–57.

<sup>5</sup> Гуломов С.С., Боев Х.И. Валюта, кредит, молия ва суғурта муаммолари. – Т.: Мехнат, 1998; Иминов Т. Суғурта бозори ислохотлари ривожланиш босқичида. – Т.: Халқ сўзи, 2021, №5(7785); Хусанов Р.Х., Ядгаров А.А. Бозор иқтисодийи шароитида суғурта тизими. – Т.: Янги аср авлоди, 2005. – 79 б.; Kuzieva N.R., Ashurova N.B., Ollokulova F.M. Business Processes In The Insurance System And Their Features. International Journal of Advanced Science and Technology Vol. 29, No. 7, (2020), pp. 7908-7913; Хамидулин М.Б., Мирсадилов М.А. Страхование. Учебно-методическое пособие. Ташкентский филиал ФГБОУ ВО «РЭУ им.Г.В.Плеханова», 2019; Қўлдошев Қ.М. Суғурта бозори, Т.: Иқтисод-молия, 2010. – 110 б.; Шеннаев Х. Суғурта иши. – Т.: Турон-иқбол, 2006. – 224 б.; Ашрафханов Б., Мирсадилов М. Развитие страхового законодательства Республики Узбекистан. – Т.: Рынок, деньги и кредит, 2002, №11-12. – 30 с.; Давлатов А. Автофукарлик жавобгарлигининг химояси. – Т.: Бозор, пул ва кредит, 2008, №9. – 54-56 б., Абдурахманов И. Мажбурий суғурта ижтимоий-иқтисодий ўсиш омили. – Т.: Бозор, пул ва кредит. 2009, №5. – 32-33 б.; Гайбуллаев Б. Регулирование инвестиционной деятельности страховщиков. – Т.: Бозор, пул ва кредит, 2009, №5, – 50-53 с., Мавлонова И. Суғурта-ижтимоий ва иқтисодий манфаатлар химояси. – Т.: Бозор, пул ва кредит, 2009, №10 – 53-55 б.



деятельности. Кроме того, Х.М.Шеннаев, М.Х.Ходжаева, М.Т.Аскарлова, Т.М.Баймуратов, А.С.Нуруллаев, К.М.Кулдошев, И.Х.Абдурахмонов, И.Г.Кенжаев, Г.Халикулова<sup>6</sup> защитили кандидатскую и докторскую диссертацию по страхованию.

В научных трудах экономистов Т.К. Иминова, А.Н. Арипова и Н.А. Иминовой<sup>7</sup> отражены вопросы риск-менеджмента, обеспечения кибербезопасности в сфере информационно-коммуникационных технологий. В этих исследованиях страхование киберрисков частично рассмотрено как один из способов обеспечения кибербезопасности и в этом отношении даны общие соображения.

Следует отметить, что до настоящего времени в нашей стране не проводилась отдельная исследовательская работа, посвященная вопросу киберстрахования. Поэтому, глубокое изучение механизма страхования киберрисков и разработка предложений и рекомендаций по его широкому внедрению и развитию явились основой для выбора темы данной диссертации и постановки исследовательских задач. Данная научная работа является первой научной исследовательской работой по страхованию киберрисков в нашей стране.

**Связь темы диссертации с планами научно-исследовательских работ высшего учебного заведения, где выполнена работа.** Данная диссертационная работа выполнена в рамках стратегического направления плана научно-исследовательских работ Ташкентского финансового института на тему «Научные основы координации финансовой, банковской и бухгалтерской систем в цифровой экономике».

**Целью исследования** является разработка предложений и рекомендаций по развитию страхования киберрисков в Узбекистане.

**Задачи исследования** заключается в следующем:

описание сущности и экономических последствий киберрисков путем анализа существующих подходов к их понятию;

изучить роль страхования в обеспечении кибербезопасности и разработать концептуальные основы страхования киберрисков;

---

<sup>6</sup> Шеннаев Х.М. Ўзбекистон Республикасида суғурта фаолиятини ривожлантириш йўналишлари. И.ф.д. (Dsc) илмий даражасини олиш учун ёзилган диссертация автореферати, Т.: ТМИ, 2021; Ходжаева М.Х. Суғурта фаолияти бухгалтерия ҳисоби ва аудитининг ҳозирги аҳоли ва уни такомиллаштириш йўллари. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати, – Т.: БМА, 2001. – 130 б.; Аскарлова М.Т. Развитие системы страхования в обеспечении экономического роста в условиях рыночных преобразований в Республики Узбекистан. Автореферат диссертации на соискание ученой степени к.э.н., – Т.: Институт экономики АН РУз, 2003. – 132 с.; Баймуратов Т.М. Ўзбекистонда суғурта фаолияти ва уни солиққа тортиш механизмини такомиллаштириш. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: Давлат ва жамият қурилиши академияси, 2004. – 125 б.; Нуруллаев А.С. Ўзбекистонда фермер ва деҳқон хўжалиқларини суғурталаш масалалари. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: БМА, 2007; Қўлдошев Қ.М. Суғурта бозорини ривожлантириш ва бошқариш муаммолари. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: БМА, 2009. – 130 б.; Абдурахмонов И.Х. Ўзбекистон Республикасида жавобгарликни суғурталашнинг амалиётини такомиллаштириш. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: БМА, 2010. – 130 б.; Кенжаев И.Ғ. Суғурта ташкилотларининг молиявий ресурсларини жойлаштириш самарадорлигини ошириш йўллари. Иқтисодиёт фанлари бўйича фалсафа доктори илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: ТМИ, 2019; Халикулова Г. Суғурта тизими ва уни амал қилиш механизмини такомиллаштириш. Иқтисодиёт фанлари бўйича фалсафа доктори илмий даражасини олиш учун ёзилган дисс. автореферати. – Т.: ТМИ, 2019.

<sup>7</sup> Иминов Т.К., Арипов А.Н. Ўзбекистон ахборот-коммуникация технологиялари соҳаси менежменти асослари. – Т.: Фан ва технология, 2005; Иминова Н.А. Алоқа ва ахборотлаштириш соҳасида иқтисодий рискларни бошқариш. И.ф.н. илмий даражасини олиш учун ёзилган диссертация автореферати. – Т.: ТАТУ, 2011.

изучить практику страхования киберрисков в зарубежных странах и определить пути ее применения в нашей республике;

исследование состояния страховых отношений в сфере информационных технологий и коммуникаций Узбекистана и разработка предложений и рекомендаций по развитию современных страховых отношений в этой сфере;

изучение и анализ состояния страхования киберрисков, как важного инструмента обеспечения кибербезопасности в Узбекистане;

разработка организационно-правовой базы развития страхования киберрисков в Узбекистане;

создание экономического механизма страхования киберрисков на основе совершенствования методологии оценки стоимости информационных систем.

**Объектом исследования** являются деятельность страховых организаций по страхованию киберрисков.

**Предметом исследования** являются экономические отношения, возникающие в процессе страхования киберрисков в Узбекистане.

**Методы исследования.** В диссертации использованы такие методы, как анализ и синтез, сравнительный анализ, статистический анализ, логическое мышление, проведение опроса, наблюдение, а также математическое моделирование.

**Научная новизна исследования** заключается в следующем:

в целях адаптации объекта страхования при страховании киберрисков к современному понятию категории информационного пространства и среды информационно-коммуникационных технологий предложено включить в классификатор страховых услуг новый класс «Страхование нематериальных активов»;

обосновано применение добровольных и обязательных форм страхования в зависимости от категории рисков, входящих в состав киберрисков, с учетом свойственности киберрисков, их экономических и социальных последствий;

предложено создание единой государственной системы с приведением условий и тарифных ставок страхования киберрисков интересам потребителей страховых продуктов;

разработана упрощенная методика расчета стоимости информационных ресурсов и систем на расходной основе без использования зависимости от страховых рисков.

**Практические результаты исследования** заключаются в следующем:

разработаны предложения по созданию единой государственной системы страхования киберрисков, принятию соответствующих нормативно-правовых актов в этом направлении, утверждению формы и порядка страхования киберрисков;

обоснована необходимость разработки ведомственных нормативных документов по страхованию киберрисков;

предложена разработка правил страхования и типового договора страхования киберрисков;

рекомендовано создание в страховой организации структурного подразделения, специализированного на страховании киберрисков и разработка его функциональных обязанностей;

совершенствована и упрощена методология оценки стоимости информационных ресурсов и систем.

**Достоверность результатов исследования** обусловлена целесообразностью использованных подходов и методов, официальностью нормативно-правовых актов, использованной литературы и интернет сведений, в том числе использованием официальных данных и отчетов Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан и подведомственных специализированных организаций, международных страховых и других организаций и внедрением на практике соответствующих заключений и предложений.

**Научная и практическая значимость результатов исследования.** Научная значимость результатов исследования заключается в том, что разработанные предложения могут быть использованы для совершенствования методологической базы страхования киберрисков в Узбекистане, проведения специальных научных исследований, направленных на обеспечение кибербезопасности.

Практическая значимость исследования заключается в полном формировании и развитии системы страхования киберрисков на необходимом уровне, возможностью широкого применения механизма урегулирования ущербов, причиненных киберрисками, наряду с реализацией соответствующих консультационных и профилактических мер.

**Внедрение результатов исследований.** На основе разработанных научных предложений и практических рекомендаций по вопросам страхования киберрисков в Узбекистане:

предложение по включению в классификатор страховых услуг нового класса «Страхование нематериальных активов», в целях адаптации объекта страхования при страховании киберрисков к современному понятию категории информационного пространства и среды информационно-коммуникационных технологий внедрено на практике Агентством по развитию страхового рынка при Министерстве финансов Республики Узбекистан (Справка Агентства по развитию страхового рынка при Министерстве финансов Республики Узбекистан №КТ/16-02-32-18/839 от 9.06.2021 года). Данное предложение внесено в «Дорожную карту» по развитию страхового рынка Республики Узбекистан на 2019-2020 годы», утвержденной постановлением Президента Республики Узбекистан от 2 августа 2019 года №ПП-4412, в качестве меры по развитию и внедрению страхования киберрисков;

предложение по применению добровольных и обязательных форм страхования в зависимости от категории рисков, входящих в состав

киберрисков, с учетом свойственности киберрисков, их экономических и социальных последствий внедрено на практике Агентством по развитию страхового рынка при Министерстве финансов Республики Узбекистан (Справка Агентства по развитию страхового рынка при Министерстве финансов Республики Узбекистан №КТ/16-02-32-18/839 от 9.06.2021 года). Данное предложение внесено в «Дорожную карту» по развитию страхового рынка Республики Узбекистан на 2019-2020 годы», утвержденной постановлением Президента Республики Узбекистан от 2 августа 2019 года №ПП-4412, в качестве меры по развитию и внедрению страхования киберрисков;

предложение по созданию единой государственной системы с приведением условий и тарифных ставок страхования киберрисков интересам потребителей страховых продуктов внедрено на практике Агентством по развитию страхового рынка при Министерстве финансов Республики Узбекистан (Справка Агентства по развитию страхового рынка при Министерстве финансов Республики Узбекистан №КТ/16-02-32-18/839 от 9.06.2021 года). Данное предложение внесено в «Дорожную карту» по развитию страхового рынка Республики Узбекистан на 2019-2020 годы», утвержденной постановлением Президента Республики Узбекистан от 2 августа 2019 года №ПП-4412, в качестве меры по развитию и внедрению страхования киберрисков;

предложение по применению упрощенной методики расчета стоимости информационных ресурсов и систем на расходной основе без использования зависимости от страховых рисков внедрено на практике Государственным унитарным предприятием «UNICON.UZ» (Справка ГУП «UNICON.UZ» №1-1/597 от 14.04.2021 года). В результате «Методика расчета стоимости информационных систем» заново разработана на основе данного предложения. Новая методика позволила приблизиться к реальной стоимости существующих информационных ресурсов и систем государственных и хозяйственных предприятий и организаций путем их отдельного учета.

**Апробация результатов исследования.** Результаты исследования обсуждены на 6 научно-практических конференциях, в том числе 2 международных и 4 республиканских.

**Опубликованность результатов исследования.** По теме диссертации опубликовано всего 12 научных работ, в том числе 5 научных статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов докторских диссертаций, из них 4 в республиканских журналах, 1 в зарубежном журнале.

**Структура и объем диссертации.** Диссертация состоит из введения, трех глав, заключения и списка использованной литературы. Объем диссертации составляет 106 страниц.

## ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и востребованность темы диссертации, описана цель и основные задачи, объект и предмет исследования, показана соответствие приоритетам развития науки и технологий республики, изложены научная новизна и практические результаты, освещена научная и практическая значимость полученных результатов, приведены сведения апробации внедрения результатов исследования на практике, опубликованные работы и структура диссертации.

В первой главе диссертации под названием **«Возникновение киберрисков в цифровой экономике и концептуальные основы их страхования»** изучено возникновение терминов «информационное общество», «цифровая экономика», исследован процесс трансформации в экономике и обществе в результате стремительного развития информационно-коммуникационных технологий, формирование информационного общества, ускорение процесса перехода к цифровой экономике, в таком обществе, где происходит высокотехнологичная революция, изучены сущность, классификация и экономические последствия новых видов рисков, представляющих серьезную угрозу кибербезопасности, то есть «киберрисков», а также концептуальные основы их страхования.

Происходящий сегодня прогресс информационно-коммуникационных технологий создает технологическую базу для перехода к новому этапу развития общества – формированию информационного общества и цифровой экономики.

В настоящее время отличие развивающихся стран от развитых также определяется прежде всего дефицитом знаний и новых технологий, в то время как фактор капитала остается второстепенным. Ведь мировая практика показывает, что развитие информационно-коммуникационных технологий является ключевым фактором повышения конкурентоспособности страны, создания широких возможностей для сбора и обобщения большого потока информации, организации управления на стратегическом уровне.

Согласно данным, в 2020 году на информационно-коммуникационные технологии приходилось более 9 процентов мирового ВВП. Из этого видно, что современные информационные технологии и программные продукты становятся одной из важнейших отраслей в развитии экономики государства как одной из прибыльных отраслей<sup>8</sup>.

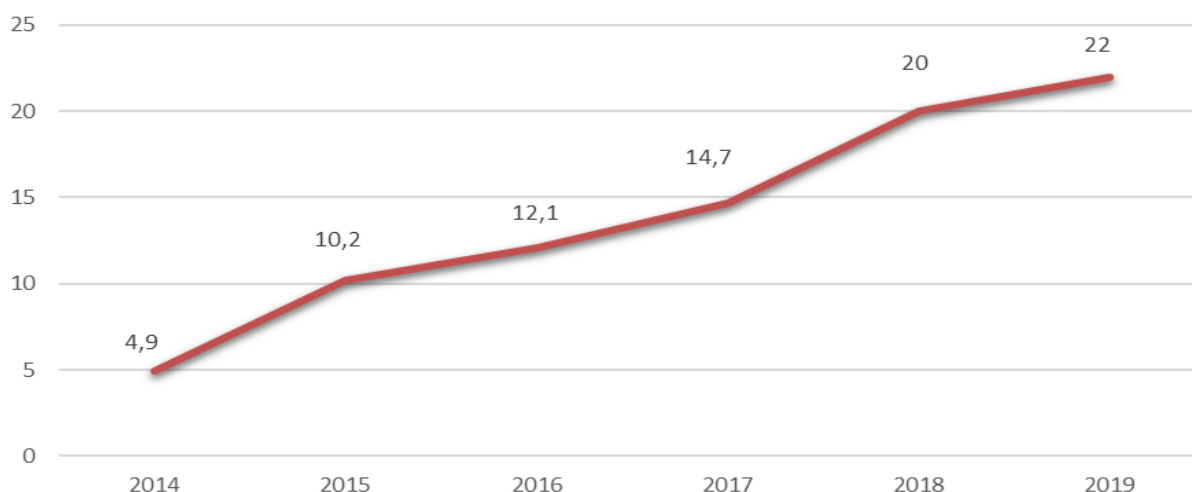
Действительно, 20 лет назад только 4,1 процента населения мира имели доступ к Интернету. Количество пользователей глобальной сети к 2019 году превысило 4,5 млрд. человек. Это означает 58,8 процентов населения мира<sup>9</sup>.

В Узбекистане по состоянию на 31 декабря 2019 года Интернетом пользуются 22 млн. человек. В эту цифру также входят 19 млн. пользователей мобильного интернета<sup>10</sup> (Рис. 1).

<sup>8</sup> Газета «Халқ сўзи» от 24.12.2016 года.

<sup>9</sup> <http://xs.uz/uzkr/post/ozbekistonda-internet-boshqa-davlatlarga-nisbatan-qimmatmi>.

<sup>10</sup> <https://podrobno.uz/cat/tehnol/kolichestvo-internet-polzovateley-v-uzbekistane-sostavlyaet-22-milliona-chelovek/>.



**Рис. 1. Количество пользователей Интернетом в Узбекистане, млн. чел.<sup>11</sup>**

На Рис. 1 видим, что за 5 лет количество пользователей Интернета в Узбекистане увеличилось в 4,5 раза.

Из приведенных статистических данных можно сделать вывод, что человечество вступает в новый этап своего развития. Конечно, как и в большинстве сфер человеческой деятельности, в связи с формированием информационного общества, ускорением процесса перехода к цифровой экономике и бурным развитием информационно-коммуникационных технологий возникают новые риски, характерные для его направлений и эти риски приводят к огромным экономическим потерям.

В течение последних 20 лет в научной литературе и других источниках стали чаще появляться понятия «Информационные риски» или «Кибер риски». Однако, до сих пор не существует точной и полной интерпретации, принятой большинством исследователей и практиков в отношении этих терминов.

Понятие «Киберриск» пока не имеет своего полного определения в литературе. На этот счет существуют разные мнения. Некоторые в этом плане в основном понимают защиту информации от различных воздействий, другие связывают информационный риск с компьютерной безопасностью.

По нашему мнению, под «Киберриском» понимается риск потерь и/или дополнительных убытков в результате неправомерных действий третьих лиц в отношении компьютерных и информационных систем или сетей, систем связи, информационных ресурсов, осуществляемых посредством информационно-коммуникационных технологий.

Киберриски можно разделить на две большие группы.

1. Скрытая кража информации сотрудниками или конкурентами;
2. Потеря информации в результате технического сбоя в каналах передачи информации.

Вышеупомянутые группы киберрисков в широком смысле включают в себя:

<sup>11</sup> Разработан автором на основе Интернет данных.

воздействие вирусов;

компьютерные атаки, т.е. воздействие хакеров и тому подобных лиц с корыстными намерениями, совершающих действия, преследующие определенный интерес со стороны внешней среды;

убытки, причиненные неправомерными действиями работников предприятия;

ущерб, причиненный в результате хищения тайны предприятия и конфиденциальной информации;

повреждения, вызванные ошибками, которые могут быть допущены при монтаже, создании и эксплуатации информационно-технических средств и систем;

ущерб, вызванный сбоями различных информационных программ и т.д.

На рисунке ниже мы можем последовательно увидеть особенности происхождения кибер-рисков (Рис. 2).



**Рис. 2. Особенности происхождения киберриска<sup>12</sup>**

Из Рис. 2 мы видим, что киберриски возникают либо в результате преднамеренных атак с целью получения прибыли, либо в результате случайных событий, вызванных небрежностью, невнимательностью и преднамеренными действиями сотрудника какой либо организации. В результате, воздействуя сначала на систему, установленную на оборудовании информационно-коммуникационной технологии, а затем на программное обеспечение и используя информацию, содержащуюся в нем, открываются широкие возможности для реализации корыстных целей, т.е. получив конфиденциальную информацию, можно нарушить принцип целостности и получить доступ ко всем программам в системе. Следствием этого может стать непревзойденный ущерб от хищения средств, утраты прибыли и других вымогательств.

В последние годы доля кибер-рисков неуклонно растет. Международные эксперты по кибербезопасности компании «Cybersecurity Ventures» подсчитали, что в 2019 году в мире кибератаки происходили каждые 14 секунд. С ростом числа кибератак резко возрастает и объем ущерба,

<sup>12</sup> Разработано автором на основе результатов исследования.

причиняемого ими. Если, в 2018 году общий ущерб, который понесли компании из разных секторов экономики, составил 1,5 трлн. долларов США, то по прогнозу Всемирного экономического форума к 2022 году этот показатель может достичь 8 трлн. долларов США<sup>13</sup>.

По статистике, в Узбекистане в последние годы также наблюдается рост числа кибератак. Одной из причин такого негативного явления является широкомасштабное внедрение информационно-коммуникационных технологий в нашей стране. Например, если в 2018 году в национальной доменной зоне «UZ» насчитывалось около 65 000 доменов, то за год их число достигло 74 000. В 2019 году в информационных системах и веб-сайтах национального сегмента сети Интернет было выявлено 132 000 угроз кибербезопасности<sup>14</sup>.

Как видно из приведенных цифр и данных, негативные экономические последствия киберрисков усиливаются по мере развития цифровых технологий. По этой причине предотвращение киберрисков и снижение их негативных экономических последствий остается одним из приоритетных вопросов в мировом сообществе.

При выборе страхования в качестве способа защиты информации следует провести сравнение между стоимостью потери информации и стоимостью мероприятий по ее защите. Исходя из показателя эффективности, выбирается тот или иной способ защиты информации.

Киберстрахование считается экономическим методом защиты от кибератак и их негативных последствий (ущербов). Российский исследователь И.К.Иванов своей научной статье дал следующее определение киберстрахованию: «Киберстрахование – это страховой продукт, бизнес которого прямо или косвенно направлен на защиту информационных рисков любых компаний, связанных с обработкой или хранением информации»<sup>15</sup>.

Результаты исследования показывают, что создание механизма страхования кибер-рисков требует решения ряда теоретических и практических вопросов. Считаем, что в этом отношении важно обратить внимание на следующее:

1. Прежде всего, необходимо адекватно сформировать нормативно-правовую базу такого механизма. Речь идет об обеспечении законодательного признания новых рисков, возникающих в результате развития информационно-коммуникационных технологий, разработке и совершенствовании классификации этих рисков, методологии страхования рисков и создании новых страховых продуктов.

2. Еще один из важных вопросов механизма страхования киберрисков связан с определением размера реального ущерба, который может возникнуть в результате их возникновения. Потому что, если ценность информации измеряется с точки зрения субъекта информационно-коммуникационных технологий его интересом к этой информации, то для

---

<sup>13</sup> Доклад о развитии цифровой экономики в России. Конкуренция в цифровую эпоху: стратегические вызовы для Российской Федерации. / 2018 Всемирный банк.

<sup>14</sup> <http://infocom.uz/2020/03/03/kiberbezopasnost-respubliki-uzbekistan-itogi-2019-goda/>.

<sup>15</sup> Иванов И.К. Кибер-страхование: как обеспечить информационную безопасность бизнесу // Большой портал для малого бизнеса – 2016, №16, С. 13-24.



другого субъекта, в том числе для страховщика, эта информация может не иметь никакой ценности.

3. Страхование киберрисков не следует рассматривать только как метод компенсации экономического ущерба. Применение данного метода требует, прежде всего, глубокого анализа информационного объекта и проведения полного и всестороннего аудита системы кибербезопасности. Разработка основ такого анализа и аудита также является важным этапом научного обоснования механизма страхования киберрисков.

4. Разработка продукта по страхованию киберрисков. При этом важное значение имеет установление страховых тарифов на основе статистики рисков, разработка договора страхования с учетом особенностей рисков и условий страхования.

В качестве объектов страхования при страховании киберрисков могут быть приняты информационные ресурсы (информации в любом виде – информационные базы данных, библиотеки и архивы в электронной форме, программные средства) и финансовые активы (денежные средства и ценные бумаги в электронной форме). В целом, страховой полис в этом отношении должен обеспечивать покрытие рисков, присущих всем программно-аппаратным структурам, связанным со сбором, передачей, хранением и обработкой информации.

Во второй главе диссертации под названием **«Современная практика страхования киберрисков и ее анализ»** исследовано возникновение и современное состояние страхования киберрисков в зарубежных странах, а также на основе статистических данных проанализировано состояние развития страховых отношений в сфере информационных технологий и коммуникаций Узбекистана, изучены существующие проблемы и разработаны предложения по их устранению. Представлены результаты социологического исследования по квалификативной (качественной) оценке существующих риск-индикаторов в сфере информационно-коммуникационных технологий Узбекистана и исследования по внедрению механизма страхования киберрисков.

Происхождение кибербезопасности часто связывают с именем Стивена Хааса. В 1997 году он совместно с «American International Group, Inc» (AIG) написал первый документ по «Политике ответственности за безопасность Интернета»<sup>16</sup>. Аналогичный документ был разработан в 2000 году Лондонской страховой компанией Lloyd's.

В «Глобальном отчете по развитию киберстрахования»<sup>17</sup> отмечается, что к 2025 году объем собираемых страховых премий в этом направлении составит 21,4 млрд. долларов США, а годовой прирост в тот период составит 27,2 процентов.

К ведущим мировым страховым компаниям, занимающимся сегодня киберстрахованием, относятся: «American International Group, Inc (AIG)», «Allianz Group», «Berkshire Hathaway, Inc.», «Lockton Companies, Inc.», «Chubb Limited», «АНА XL SA», «Tsurich Insurance Group», «Lloyd's Group of London Ltd».

<sup>16</sup> The Growth and Challenges of Cyber Insurance, Chicago Fed Letter, No. 426, 2019.

<sup>17</sup> Global Cyber Insurance Market (2019-2025).

Одну из интересных программ кибербезопасности представила английская компания Lloyd's. Полис получил название «Internet Asset and Income Protection Coverage», важной особенностью которого является возможность выбора поставщика средств защиты. Эта программа компенсирует риски потери или повреждения информационных активов в результате взлома системы безопасности программы или ее сбоя<sup>18</sup>.

Появление страхования киберрисков в России не имеет своей точной даты. Некоторые инициативы страховщиков по осуществлению этого вида страхования начались в 1997-1999 годах. В этот период страховые компании «Инфострах» и «Ингосстрах» одними из первых заключили соглашение с Министерством связи Российской Федерации о сотрудничестве в этой сфере. В соответствии с этим соглашением научно-исследовательскую часть страхования киберрисков взял на себя Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации. Однако правильнее будет указать в качестве отправной точки начала страхования киберрисков дату 9 сентября 2000 года, когда Президентом Российской Федерации была утверждена «Доктрина информационной безопасности Российской Федерации». В соответствии с настоящей доктриной в качестве экономических методов борьбы с угрозами кибербезопасности предусмотрено создание системы страхования киберрисков юридических и физических лиц, направленной на возмещение ущерба в случае возникновения угроз. После этого многим страховым компаниям удалось получить лицензию на деятельность в этой сфере, и это обстоятельство создало предпосылки для формирования рынка страхования киберрисков в Российской Федерации. Наибольший спрос на этот продукт наблюдался в начале 2000-х годов, и страховые компании получили возможность получить высокие суммы прибыли<sup>19</sup>.

На сегодняшний день на российском рынке существует ряд страховых компаний, предлагающих полисы киберстрахования. По прогнозу страховой компании «Сбербанк страхование», рынок киберстрахования в России к 2025 году может достичь 8-10 млрд. рублей<sup>20</sup>. Для сравнения, в середине 2019 года объем этого рынка оценивался в 10 млн. рублей.

В целом, в настоящее время страхование киберрисков во всем мире предоставляется только корпоративному сектору. Основная причина этого заключается в том, что страховые компании, занимающиеся страхованием киберрисков, составляют малое количество и стоимость страховой услуги относительно высока (при этом также учитываются расходы на экспертизу, которые должны быть выполнены до страхования). Одним из факторов, препятствующих бурному развитию сегмента страхования киберрисков, является несовершенство законодательства в этом направлении и непрозрачность бизнеса, то есть невозможность оценки ожидаемого ущерба у страхуемых субъектов.

---

<sup>18</sup> Косарев А.В. Страхование информационных рисков. – М., 2010.

<sup>19</sup> Косарев А.В. Страхование информационных рисков. – М., 2010.

<sup>20</sup> <https://tass.ru/ekonomika/7661063>.

Наряду с вышеописанными, существует ряд факторов, негативно влияющих на развитие страхования киберрисков. Это также можно увидеть из данных рисунка ниже (Рис. 3).



**Рис. 3. Негативно влияющие факторы на мировую торговлю по страхованию киберрисков<sup>21</sup>**

Как видно из рисунка, одним из основных негативных факторов, препятствующих мировой торговле по страхованию киберрисков, является непонимание киберрисков.

Правда, такая ситуация объясняется новизной и отсутствием широкого распространения данного вида страхования. Тем не менее, процесс цифровизации, происходящий во всем мире, ставит вопрос кибербезопасности на первое место. Это, в свою очередь, приведет к резкому росту спроса на киберстрахование, а значит, и широкой популярности этого вида страхования не только в корпоративном секторе, но и среди населения. На наш взгляд, несмотря на наличие непонимания киберрисков со стороны клиентов, цифровизация всех аспектов жизни государства и общества в ближайшей перспективе свидетельствует о наличии большого потенциала для бурного развития данного сегмента.

Сегодня отрасли и средства информационно-коммуникационных технологий Республики Узбекистан - это совершенствующийся комплекс, имеющий особое значение в экономике страны. При поддержке зарубежных партнеров в республике проводится значительная работа по техническому и технологическому перевооружению данной сферы. Растущее значение информационно-коммуникационных технологий проявляется в развитии экономики страны, предоставлении качественных услуг населению.

Естественно, стремительное развитие новых технологий расширяет масштабы возникновения различных рисков, связанных с их свойственностью. На основе изучения этой взаимосвязи между

<sup>21</sup> Источник: DELLOITTE UNIVERSITY PRESS совместно с PARTNER RE ADVISEN.

экономическим прогрессом и изменением величины рисков можно сформулировать следующее правило. То есть, существует взаимосвязь между темпами роста технико-технического прогресса экономики и увеличением количества и видов рисков. Это, в свою очередь, требует постоянного совершенствования управления рисками на основе непрерывной поддержки новых, передовых подходов к ним.

Это обстоятельство требует формирования современной системы страхования, способной обеспечить качественную защиту деятельности субъектов сферы информационно-коммуникационных технологий. За истекший период проведена значительная работа по формированию и развитию страховых отношений в сфере.

Наряду с достигнутыми результатами по развитию страховых отношений в сфере существуют проблемы, которые ждут своего решения. Они состоят из следующих:

1. Многие направления деятельности имеющихся в сфере предприятий и организаций, а также объекты связи остаются недостаточно обеспеченными страховой защитой. Это, прежде всего, дорогостоящие оборудования, требующее осторожности, телерадиовещательные станции, дорогостоящие коммуникационные оборудования, поставляемые по международным проектам. Мы можем увидеть это состояние в таблице ниже (Таблица 1).

**Таблица 1**

**Показатель уровня застрахованности в сфере информационных технологий и коммуникаций Республики Узбекистан<sup>22</sup>**

| Год  | Показатели               | Балансовая стоимость основных средств, млрд. сум | Количество транспортных средств, штук | Количество сотрудников, человек |
|------|--------------------------|--|---------------------------------------|---------------------------------|
| 2012 | Общее количество         | 1 263  | 2081                                  | 14 796                          |
|      | Застрахованная часть     | 518,6  | 473                                   | 6 510                           |
|      | Уровень застрахованности | 41,1 %   | 22,7 %                                | 44 %                            |
| 2015 | Общее количество         | 1 754,4  | 1 658                                 | 18 815                          |
|      | Застрахованная часть     | 274,6  | 442                                   | 5 724                           |
|      | Уровень застрахованности | 15,6 %   | 26,7 %                                | 30,4 %                          |
| 2018 | Общее количество         | 2 814  | 2 004                                 | 19 584                          |
|      | Застрахованная часть     | 477  | 327                                   | 1 277                           |
|      | Уровень застрахованности | 16,9 %   | 16,3 %                                | 6,5 %                           |

Как видно из Таблицы 1, уровень застрахованности в сфере из года в год снижался. Следует отметить, что организации сферы в полной мере пользуются обязательными видами страхования. При этом, по видам обязательного страхования возмещаются только убытки, причиненные потерпевшим лицам.

Если по итогам 2012 года доля объема собранных страховых премий от предприятий и организаций системы в общем портфеле страховой компании

<sup>22</sup> Разработано автором на основе материалов Коллегии Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан.

«ALSKOM» составила 42,1 процента, то по итогам 2018 года этот показатель составил всего 7,9 процента (4,7 процента приходится на добровольные, 3,2 процента на обязательные виды страхования)<sup>23</sup>.

Для решения сложившейся проблемы требуется повышение активности предприятий и организаций сферы информационно-коммуникационных технологий в развитии страховых отношений. Для этого предлагается полностью освоить средства в разрезе кварталов, выделенные на страховую защиту в годовом бизнес-плане и смете расходов предприятий и организаций сферы, при этом в первую очередь обеспечить страховой защитой имущество, оборудования (объекты, представляющие ценность и государственную значимость, кабельные хозяйства телекоммуникаций, узлы специальной связи) и транспортные средства от различных рисков, а также жизнь и здоровье от несчастных случаев и медицинское страхование работников, направленное на их социальную защиту.

2. Недостаточное внимание уделяется формированию системы «риск-менеджмент» на предприятиях и организациях системы Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан. Тем не менее, по мере развития информационно-коммуникационных технологий масштабы рисков будут расширяться.

Для решения сложившейся проблемы предлагается сформировать современную систему «риск-менеджмента» на предприятиях и в организациях сферы, то есть возложить на специальный отдел или отдельного сотрудника выполнение задач по управлению рисками и регулированию страховых отношений, наладить систему изучения, выявления и предупреждения рисков, присущих деятельности предприятия.

3. Механизм страхования киберрисков недостаточно используется предприятиями и организациями сферы информационно-коммуникационных технологий. В целях развития данного направления и широкого внедрения киберстрахования в системе принят соответствующий приказ Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан, а также определены конкретные задачи для предприятий и организаций системы. Несмотря на это, крупные предприятия и организации отрасли игнорируют поставленные задачи.

Для устранения существующей проблемы требуется вывести систему страхования киберрисков на новый уровень и широко ее популяризировать. Для этого, считаем целесообразным, осуществление Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан следующих дополнительных мер:

1. Совершенствование системы оценки стоимости информационных ресурсов и систем, а также размера ущерба, причиненного киберрисками.

2. Организация деятельности в следующих направлениях:

- проведение экспертизы уровня кибербезопасности;
- оценка ущерба, причиненного киберрисками;
- широкая популяризация системы страхования киберрисков;

---

<sup>23</sup> Данные страховой компании «ALSKOM».

- проведение постоянного мониторинга состояния застрахованности.

3. Повышение квалификации работников сферы в области кибербезопасности и налаживание системы подготовки кадров в этом направлении.

4. Внесение требований о необходимости страхования киберрисков в лицензионное соглашение, заключаемое между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и субъектами, осуществляющими деятельность в сфере информационно-коммуникационных технологий.

5. Создание в страховых компаниях структурного подразделения, специализирующегося на реализации соответствующих задач по страхованию киберрисков и определение его основных задач.

Выполнение указанных задач будет способствовать развитию страховых отношений в системе Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан и, в конечном счете, обеспечению осуществления устойчивой деятельности предприятий и организаций, функционирующих в системе.

В соответствии с методикой, предложенной диссертантом и другими исследователями, в 2010 году проводилась квалификационная (качественная) оценка риск-индикаторов движения элементов среды информационно-коммуникационных технологий путем проведения социологического исследования. Данное социологическое исследование было проведено в соответствии с распоряжением Узбекского агентства связи и информатизации (ныне Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан) № 27-ф от 4 мая 2010 года Ташкентским университетом информационных технологий и страховой компанией «ALSKOM» совместно с Институтом социологических исследований при Кабинете Министров Республики Узбекистан на тему «Состояние и перспективы развития риск-менеджмента в сфере информационно-коммуникационных технологий Узбекистана» среди респондентов из числа руководящих сотрудников и специалистов предприятий и организаций, входящих в сферу информационно-коммуникационных технологий Узбекистана. Результаты социологического исследования не утратили своей актуальности и на сегодняшний день.

Одним из важных выводов социологического опроса, проведенного среди руководителей и специалистов по управлению рисками в 34 субъектах сферы информационно-коммуникационных технологий Узбекистана, является то, что гораздо важнее вовсе не избегать рисков, а через хорошую системную аналитическую работу постоянно следить за тем, чтобы движение экономических элементов не отклонялось от намеченных направлений, то есть не подвергалось рискам с тяжелыми последствиями. Целью этого является своевременное выявление отклонений элемента в сторону риска во время его движения и принятие соответствующих мер. Этот вывод, по сути, подтверждает изложенную выше новую трактовку категорий риска и вытекающих из нее положений нового подхода к управлению рисками.

С учетом результатов исследования и в целях обеспечения приоритета кибербезопасности Узбекскому агентству связи и информатизации (ныне Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан) была предложена инициатива по разработке и внедрению в республике механизма комплексного страхования киберрисков. Эта инициатива была одобрена на расширенном заседании Коллегии данного государственного органа в 2005 году. Коллегия своим решением утвердила программу научно-исследовательских работ по изучению научных основ страхования киберрисков и разработки на ее основе соответствующей нормативной базы. В этом направлении была создана рабочая группа, в состав которой вошел и автор данной диссертации.

В результате проведенных исследований были разработаны следующие нормативные документы:

1. Правила страхования информационных рисков. Правила устанавливают порядок и условия страхования.

2. Методика расчета стоимости информационных систем. В нем приводится расчет стоимости, которая идет на восстановление информационного ресурса в случае его исчезновения.

3. Методика оценки ущерба и установления суммы страхового возмещения. В ней предусматривается определение рисков, оценка ущерба и угроз, определение возможного ущерба при страховании киберрисков, а также определение размера выплачиваемого страхового возмещения по нанесенному ущербу.

4. Инструкция по проведению экспертизы (аудита) безопасности информационных систем. Данная инструкция определяет порядок проведения экспертизы информационных систем, предназначенной для выявления имеющихся недостатков по защите информации в сети и расследования инцидента, связанного с потерей информации.

Учитывая новизну разработанных нормативных документов, приказом Узбекского агентства связи и информатизации (ныне Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан) от 11 мая 2009 года № 150 было определено о применении опытного внедрения данных документов на отдельных предприятиях и организациях сферы и утвержден план мероприятий, которые необходимо предпринять в этом направлении.

Опытное внедрение созданного механизма страхования киберрисков осуществлялось на следующих этапах (Рис. 4).

Опытное внедрение созданных нормативных документов позволило апробировать их на практике и выявить имеющиеся недостатки. Диссертантом разработаны предложения по устранению выявленных недостатков и проблем. При устранении выявленных недостатков возможно широкое внедрение нормативных документов на практике.

В третьей главе диссертации под названием **«Пути развития страхования киберрисков в условиях внедрения цифровой экономики в Узбекистане»** разработаны конкретные предложения по широкому внедрению и развитию страхования киберрисков в условиях перехода

Узбекистана к цифровой экономике, а также разработаны научные заключения и предложения по совершенствованию методики оценки стоимости информационных ресурсов и систем.



**Рис. 4. Этапы реализации процесса страхования киберрисков<sup>24</sup>**

Развитие современной экономики, опирающейся на новейшие цифровые технологии и программное обеспечение, будет способствовать повышению темпов развития экономики и ее отраслей, оптимизации взаимодействия между субъектами экономики, увеличение объема доходов за счет снижения себестоимости и обеспечению подобных высоких показателей эффективности.

В Узбекистане за последние годы были предприняты резкие шаги по переходу на цифровую экономику. В рамках осуществляемых широкомасштабных реформ по коренной модернизации национальной экономики осуществлен ряд мер по внедрению цифровых технологий в социально-экономическую жизнь страны и систему государственного управления. В частности, важным шагом в развитии цифровой экономики в нашей стране стало принятие постановления Президента Республики Узбекистан от 3 июля 2018 года № ПП-3832 «О мерах по развитию цифровой экономики в Республике Узбекистан», в котором определены важнейшие задачи.

Кроме того, исходя из вопросов и целей, поднятых Президентом Республики Узбекистан Ш.Мирзиёевым 25 января 2020 года в Послании Олий Мажлису, в Узбекистане 2020 год объявлен «Годом развития науки, просвещения и цифровой экономики», в связи с чем принят указ Президента и утверждена Государственная программа.

Документ предусматривает ряд мер по кибербезопасности наряду с цифровизацией всех секторов экономики страны путем широкого внедрения

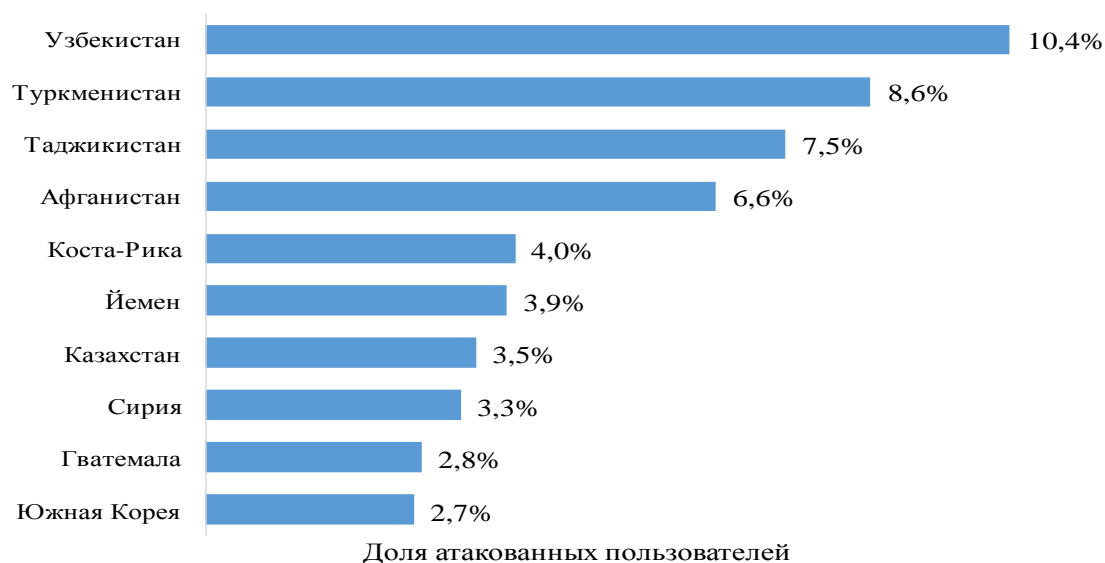
<sup>24</sup> Разработано автором.



новейших информационных технологий и программ. Наиболее важных из этих мер является разработка проекта Закона Республики Узбекистан «О кибербезопасности». Ведь внедрение цифровой экономики приведет к возникновению киберугроз.

Действительно, в Узбекистане, как и в других странах, наблюдаются рост кибератак. Только за 9 месяцев 2019 года было выявлено более 8 миллионов подобных случаев, причем некоторые из них были на крайне опасном уровне. Об этом Премьер-министр Республики Узбекистан А.Арипов особо отметил на международном форуме «Открытые инновации». По этой причине в стране принята комплексная программа по обеспечению безопасности цифровой информации, в рамках которой принято 70 различных нормативных документов в области кибербезопасности. А.Арипов отметил, что все государственные учреждения в нашей стране начали осуществлять электронный обмен через защищенную систему передачи информации. Принятые меры позволили Узбекистану подняться на 40 позиций в глобальном индексе по кибербезопасности и занять 52 место среди 175 стран<sup>25</sup>.

В 2020 году Узбекистан занял первое место в рейтинге стран по количеству пострадавших от вирусных атак банков. В 2020 году в Узбекистане 10,4 процентов пользователей подверглись вирусной атаке банка (Рис. 5).



**Рис. 5. Рейтинг стран, в которых в 2020 году наблюдались вирусные атаки банков<sup>26</sup>**

Реализация задач и поручений по кибербезопасности, определенных в Государственной программе «Год развития науки, просвещения и цифровой экономики», несомненно, будет способствовать снижению ущерба от кибератак. Вместе с тем, считаем, что развитие в Узбекистане широко

<sup>25</sup> Источник: [https://sputniknews.ru/novosti\\_uzbekistan/20191023/1030087801/uzbekistan-stolknulsya-rostom-kiberatak.html](https://sputniknews.ru/novosti_uzbekistan/20191023/1030087801/uzbekistan-stolknulsya-rostom-kiberatak.html).

<sup>26</sup> Источник: <https://www.statista.com/statistics/325226/countries-by-users-attacked-by-financial-malware/#statistic-Container>.

распространенного в мировой практике метода страхования киберрисков в сфере обеспечения кибербезопасности будет иметь высокую эффективность в устранении ущерба, причиненного в последствии кибератак. Данная методика основана на предоставлении страховыми организациями субъектам информационных отношений гарантий по возмещению экономического ущерба при угрозах кибербезопасности.

2020 год стал годом, который придаст импульс на поднятие на новый этап по трансформации Узбекистана в экономику, основанную на цифровых технологиях. Переход нашей страны к цифровой экономике, основанный на вышеизложенных моментах, призывает на развитие и широкую популяризацию системы страхования киберрисков. Считаем целесообразным реализовать следующие предложения в этом отношении:

1. В проект Закона Республики Узбекистан «О кибербезопасности» следует включить вопросы развития страхования киберрисков в Узбекистане.

2. Целесообразно принять соответствующий нормативно-правовой акт по страхованию киберрисков. Данным документом требуется утвердить форму и порядок страхования киберрисков.

По нашему мнению, принимая во внимание, что страхование киберрисков в Узбекистане является важным инструментом обеспечения информационной безопасности, учитывая свойственность киберрисков, их экономические и социальные последствия, целесообразно применение добровольных или обязательных форм страхования в зависимости от категории рисков, входящих в состав киберрисков.

3. Классификатор страховой деятельности в Республике Узбекистан не имеет специального класса страхования информационных ресурсов и информационных систем, а также требований и содержания по условиям проведения такого вида страхования. Поэтому на практике пока экспериментируют перевод страхования киберрисков в класс имущественных видов страхования. Это не соответствует современному понятию категории информационного пространства и среды информационно-коммуникационных технологий. В связи с этим предлагаем включить в действующий в Республике Узбекистан классификатор страховой деятельности новый «18-класс – «Страхование нематериальных активов».

4. Целесообразно создать усовершенствованную методику оценки стоимости информации в страховании киберрисков. Ведь самая большая проблема, возникающая сегодня в этом направлении, это определение точной стоимости информации.

Реализация описанных предложений позволит полноценное формирование и развитие на должном уровне страховых отношений в данном направлении, наряду с проведением соответствующих консультационных и профилактических мероприятий в этом направлении, наладить широкое внедрение механизма устранения ущерба, причиненного рисками, без влияния на стабильность деятельности.

В соответствии с действующей «Методикой расчета стоимости информационных систем», утвержденной приказом Узбекского агентства связи и информатизации (ныне Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан) от 1 декабря 2008 г.

№ 332, при оценке стоимости информационных ресурсов и систем, учитываются затраты, связанные с их приобретением, созданием и внедрением. То есть, оценка информационной системы производится исходя из затрат, необходимых для восстановления информационных ресурсов, информационных технологий и средств связи, а также механизмов противодействия киберрискам.

Результаты исследования показывают, что в п. 3.3 настоящей Методики указаны основные показатели по расчету стоимости восстановления информационных систем при наступлении страхового случая. Однако, невозможно заранее определить, какой страховой случай может произойти, а точнее, как указано в данном пункте, время восстановления информационного ресурса, количество специалистов, привлекаемых для восстановления, стоимость оборудования, арендованного для восстановления информационного ресурса.

На основании результатов исследования рекомендуется внедрить следующую упрощенную методику, разработанную в отношении расчета стоимости информационных ресурсов и систем:

- при расчете стоимости информационного ресурса учитывается среднемесячная заработная плата работника (специалиста, обеспечивающего информационный ресурс), умноженная на количество работников, выполняющих работу над информационным ресурсом, и период использования информационного ресурса (с даты ввода в эксплуатацию до даты принятия к страхованию);
- при расчете стоимости информационной системы учитывается сумма балансовой стоимости информационных технологий, балансовой стоимости программного обеспечения и стоимости информационных ресурсов.

## **ЗАКЛЮЧЕНИЕ**

В результате проведенных научных исследований по вопросам страхования киберрисков в Узбекистане сформулированы следующие выводы:

1. Результаты исследования и анализ показывают, что с ростом числа киберрисков и атак вес ущерба, причиняемого ими, также резко возрастает. По этой причине вопрос кибербезопасности стал актуальным и чрезвычайно важным вопросом современного общества.

2. Результаты проведенного исследования подтвердили важность роли риск-менеджмента в обеспечении кибербезопасности. Изучен механизм страхования киберрисков как экономический метод современной системы риск-менеджмента и проанализированы ее концептуальные основы. При выборе страховки в качестве способа защиты информации следует провести сравнение между расходами потери информации и стоимостью мероприятий по ее защите.

3. Результаты исследования показали, что основной причиной, препятствующей мировой торговле страхованием киберрисков, является непонимание киберрисков. Правда, такая ситуация объясняется новизной и отсутствием широкого распространения данного вида страхования. Тем не

менее, процесс цифровизации, происходящий во всем мире, ставит проблему кибербезопасности на первое место. Это, в свою очередь, приведет к резкому росту спроса на киберстрахование, а значит, и широкой популярности этого вида страхования не только в корпоративном секторе, но и среди населения. Несмотря на то, что на сегодняшний день существует ситуация непонимания киберрисков, считаем, что это свидетельствует о том, что в перспективе существует большой потенциал для быстрого развития этого сегмента.

4. Стремительное развитие информационно-коммуникационных технологий в Узбекистане также увеличивает скорость возникновения рисков, связанных с их свойствами. Это, в свою очередь, требует формирования современной системы страхования, способной обеспечить качественную защиту деятельности субъектов данной сферы. Практическое применение разработанных предложений и рекомендаций будет способствовать развитию страховых отношений в сфере и, в конечном счете, обеспечению устойчивого функционирования предприятий и организаций системы.

5. Целесообразно внедрить проведение экспертизы (аудита) уровня безопасности информационных ресурсов и систем и оценки их стоимости за счет страхователей. Экспертиза уровня безопасности информационных ресурсов и систем должна проводиться независимо от того, страхуются или нет. Это является одним из главных требований риск-менеджмента. В конце концов, владелец информационных ресурсов и систем должен постоянно проводить мониторинг уровня безопасности и, соответственно, разрабатывать и внедрять соответствующие меры безопасности. В случае высокого уровня безопасности необходимость в страховой защите отсутствует или страховая защита осуществляется по низкой цене.

6. Принимая во внимание, что страхование киберрисков в Узбекистане является важным инструментом обеспечения информационной безопасности, учитывая свойственность киберрисков, их экономические и социальные последствия, целесообразно применять добровольные или обязательные формы страхования в зависимости от категории рисков, входящих в состав киберрисков.

7. Классификатор страховой деятельности в Республике Узбекистан не имеет специального класса страхования информационных ресурсов и информационных систем, а также требований и содержания по условиям проведения такого вида страхования. Поэтому на практике пока экспериментируют перевод страхования киберрисков в класс имущественных видов страхования. Это не соответствует современному понятию категории информационного пространства и среды информационно-коммуникационных технологий. В связи с этим предлагаем включить в действующий в Республике Узбекистан классификатор страховой деятельности новый «18-класс – «Страхование нематериальных активов».

8. При оценке стоимости информационных ресурсов и систем целесообразно рассчитывать их на расходной основе без использования зависимости от страховых рисков.

**THE SCIENTIFIC COUNCIL DSc. 03/30.12.2019. I.17.01  
AWARDING SCIENTIFIC DEGREES AT  
TASHKENT INSTITUTE OF FINANCE**

---

**TASHKENT INSTITUTE OF FINANCE**

**KHASANOV FARRUKH RAVSHANOVICH**

**ISSUES OF CYBER RISKS INSURANCE IN UZBEKISTAN**

**08.00.07 - Finance, money circulation and credit**

**ABSTRACT**  
**of the dissertation of the doctor of philosophy (PhD) on economic sciences**

**Tashkent city - 2022 year**

**The theme of dissertation of Doctor of Philosophy (PhD) was registered under the number B2020.2.PhD/Iqt1372 at the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan.**

Doctoral (PhD) dissertation has been prepared at Tashkent institute of finance.

The abstract of the dissertation is posted in three languages (Uzbek, Russian and English (summary)) on the website of the Scientific Council (www.tfi.uz) and on the website «ZiyoNET» Informational and educational portal (www.ziynet.uz).

**Scientific supervisor:** **Shennaev Xujayor Musurmanovich**  
Doctor of Science in Economics (Dsc), Docent

**Official opponents:** **Kuzieva Nargiza Ramazonovna**  
Doctor of Science in Economics, Professor  
**Xamidulin Mixail Borisovich**  
Doctor of Science in Economics, Professor

**Leading organization:** **Tashkent State University of Economics**

The defense of the dissertation will take place on 01 «28», 2022 at 16:00 at the meeting of the Scientific Council 03/30.12.2019.I.17.01. at Tashkent institute of finance. Address: 100000, 60a, Amir Temur Street, Tashkent city; Tel: (71) 234-53-34, fax: (99871) 234-46-26; e-mail: ilmiykengash@tfi.uz.

The dissertation (PhD) is available at the Information resource center of the Tashkent institute of finance (registered No. 257). Address: 100000, 60a, Amir Temur Street, Tashkent city. Phone: (99871) 234-53-34; fax: (99871) 234-46-26, e-mail: admin@tfi.uz.

The abstract of the dissertation was distributed on «14» 01 2022.  
(mailing report № 70 dated «14» 01 2022).



*T.Z. Teshabaev*

**T.Z. Teshabaev**

Chairman of the Scientific Council for awarding scientific degrees, Doctor of Science in Economics, Professor

*F.K. Kholmamatov*  
**F.K. Kholmamatov**  
Scientific Secretary of the Scientific Council for awarding scientific degrees, Doctor of Philosophy of Science in Economics (PhD), Docent

*I.N. Kuziev*  
**I.N. Kuziev**  
Chairman of the Scientific Seminar under the Scientific Council for awarding scientific degrees, Doctor of Science in Economics, Professor

## INTRODUCTION (abstract of the dissertation (PhD))

**The aim of the research** is to develop proposals and recommendations for the development of cyber risk insurance in Uzbekistan.

**Research objectives are as following:**

description of the essence and economic consequences of cyber risks by analyzing existing approaches to their concept;

to study the role of insurance in ensuring cybersecurity and develop a conceptual framework for cyber risk insurance;

to study the practice of cyber risk insurance in foreign countries and determine the ways of its application in our republic;

research of the state of insurance relations in the field of information technologies and communications of Uzbekistan and development of proposals and recommendations for the development of modern insurance relations in this area;

study and analysis of the state of cyber risk insurance as an important tool for ensuring cybersecurity in Uzbekistan;

development of the organizational and legal framework for the development of cyber risk insurance in Uzbekistan;

creation of an economic mechanism for cyber risk insurance based on improving the methodology for assessing the cost of information systems.

**The research object** is the activities of insurance organizations for the insurance of cyber risks.

**The scientific novelty of the research** is as follows:

in order to adapt the object of insurance when insuring cyber risks to the modern concept of the category of information space and the environment of information and communication technologies, it is proposed to include a new class of «Insurance of intangible assets» in the classifier of insurance services;

the use of voluntary and mandatory forms of insurance is justified depending on the category of risks included in the cyber risks, taking into account the nature of cyber risks, their economic and social consequences;

it is proposed to create a unified state system with the reduction of conditions and tariff rates of cyber risk insurance to the interests of consumers of insurance products;

a simplified methodology has been developed for calculating the cost of information resources and systems on an expense basis without using dependence on insurance risks.

**Implementation of research results.** Based on the developed scientific proposals and practical recommendations on cyber risk insurance in Uzbekistan:

proposal for inclusion in the classifier of insurance services of a new class «Insurance of intangible assets», in order to adapt the object of insurance in the insurance of cyber risks to the modern concept of the category of information space and the environment of information and communication technologies implemented in practice by the Insurance market development Agency under the Ministry of finance of the Republic of Uzbekistan (Reference №KT/16-02-32-18/839 of the Insurance market development Agency under the Ministry of finance of the Republic of Uzbekistan of June 9, 2021). This proposal is included in the

«Roadmap» for the development of the insurance market of the Republic of Uzbekistan for 2019-2020», approved by the Decree of the President of the Republic of Uzbekistan № PP-4412 dated August 2, 2019, as a measure for the development and implementation of cyber risk insurance;

proposal for the use of voluntary and mandatory forms of insurance, depending on the category of risks included in the cyber risks, taking into account the nature of cyber risks, their economic and social consequences implemented in practice by the Insurance market development Agency under the Ministry of finance of the Republic of Uzbekistan (Reference №KT/16-02-32-18/839 of the Insurance market development Agency under the Ministry of finance of the Republic of Uzbekistan of June 9, 2021). This proposal is included in the «Roadmap» for the development of the insurance market of the Republic of Uzbekistan for 2019-2020», approved by the Decree of the President of the Republic of Uzbekistan № PP-4412 dated August 2, 2019, as a measure for the development and implementation of cyber risk insurance;

proposal to create a unified state system with the reduction of conditions and tariff rates of cyber risk insurance to the interests of consumers of insurance products implemented in practice by the Insurance Market Development Agency under the Ministry of Finance of the Republic of Uzbekistan (Reference №KT/16-02-32-18/839 of the Insurance Market Development Agency under the Ministry of Finance of the Republic of Uzbekistan of June 9, 2021). This proposal is included in the «Roadmap» for the development of the insurance market of the Republic of Uzbekistan for 2019-2020», approved by the Decree of the President of the Republic of Uzbekistan № PP-4412 dated August 2, 2019, as a measure for the development and implementation of cyber risk insurance;

proposal for the application of a simplified methodology for calculating the cost of information resources and systems on an expense basis without the use of dependence on insurance risks implemented in practice by the State Unitary Enterprise «UNICON.UZ» (Reference №1-1/597 of the State Unitary Enterprise «UNICON.UZ» of April 14, 2021). As a result, the «Methodology for calculating the cost of information systems» has been re-developed on the basis of this proposal. The new methodology made it possible to approach the real cost of existing information resources and systems of state and economic enterprises and organizations by taking them into account separately.

**Approbation of scientific results.** The results of the research were discussed at 6 scientific and practical conferences, including 2 international and 4 republican ones.

**Publication of research results.** 12 academic papers have been published on the topic of the dissertation, including 5 scientific articles in scientific publications, which are recommended by the Supreme Attestation Commission of the Republic of Uzbekistan for the publication of the main scientific results of doctoral dissertations, of these, 4 are in republican journals, 1 in a foreign journal.

**The structure and scope of the dissertation.** The dissertation consists of an introduction, three chapters, conclusion and a list of used literature. The volume of the dissertation is 106 pages.



**ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ**  
**СПИСОК ОПУБЛИКОВАННЫХ РАБОТ**  
**LIST OF PUBLISHED WORKS**

**I бўлим (часть I; Part I)**

1. Khasanov Farrukh. Cyber insurance in Uzbekistan: status and prospects for development. //ACADEMICIA: An International Multidisciplinary Research Journal <https://saarj.com>, Vol. 11, Issue 2, February 2021. (№23; SJIF-7.492).

2. Хасанов Ф.Р. Ўзбекистонда ахборот хатарларини суғурта қилишнинг услубий асослари. // «Бозор, пул ва кредит» журнали. – Тошкент. 2010. №11 (162). 60-63-б. (08.00.00; №4).

3. Хасанов Ф.Р. Рақамли иқтисодиётнинг таҳдидлари – кибер-суғуртани ривожлантиришга даъват. // «Халқаро молия ва ҳисоб» илмий-электрон журнали. – Тошкент. 2021. №6. /.(08.00.00. № 19).

4. Хасанов Ф.Р. Необходимость развития киберстрахования в условиях внедрения цифровой экономики в Узбекистане. Материалы международной научно-практической видеоконференции на тему: «Тенденции и перспективы инновационного развития в условиях цифровой экономики».-Екатеренбург-Ташкент. 2021. 238-240 стр.

5. Хасанов Ф.Р. Рақамли иқтисодиёт шароитида иқтисодий барқарорликни таъминлашда кибер рискларни суғурталашнинг концептуал асослари. «Рақамли иқтисодиёт шароитида ишлаб чиқаришни ташкил этиш ва бошқариш: назария ва амалиёт» мавзусида халқаро илмий-амалий конференция.-Тошкент. 2021. 916-917 б.

6. Хасанов Ф.Р. Кибер рискларни суғурталаш амалиёти. «Кичик саноат зоналари салоҳиятини аниқлашнинг инновацион электрон таъминотини шакллантириш истиқболлари» мавзусида олий ўқув юртлараро илмий-амалий конференция материаллари тўплами. -Тошкент. 2021. 345-348 б.

7. Хасанов Ф.Р. Ахборот хавфсизлигини таъминлашнинг ташкилий асослари. «Ўзбекистонда суғурта бозорининг ривожланиш истиқболлари» Республика илмий-амалий конференцияси материаллари тўплами. -Тошкент. 2012. 82-84 б.

**II бўлим (часть II; Part II)**

8. Хасанов Ф., Тураббаев Б. Страхование информационных рисков: обзор мировой практики и состояние формирования в Узбекистане. // «Aloqa Dunyosi». –Тошкент. 2007, №3 (9). 57-61-б.

9. Иминов Т.К., Хасанов Ф.Р., Нуриддинова А.Г., Иминова Н.А., Мухитдинов А.Х. Ахборот коммуникация технологиялари соҳасида иқтисодий рискларнинг социологик таҳлили. // «Молия». – Тошкент. 2011. №5-6. 125-129-б. (08.00.00; №12).

10. Иминов Т.К., Хасанов Ф.Р. Перспективы развития страхования информационных рисков в Узбекистане. // «O'zbekiston iqtisodiy axborotnomasi». – Тошкент. 2015. №2/2015. (08.00.00; №1).

11. Иминов Т.К., Хасанов Ф.Р., Юлдашев А.Қ. АКТ соҳасида суғурта муносабатларининг ривожланиш ҳолати ва истиқболлари. «Глобаллашув шароитида Ўзбекистон Республикасида ахборотлашган жамиятни шакллантириш муаммолари» Республика илмий-услубий семинар материаллари тўплами.-Тошкент. 2015. 114-120 б.

12. Иминов Т.К., Хасанов Ф.Р. Страхование информационных рисков – веление времени. «Глобаллашув шароитида Ўзбекистон Республикасида ахборотлашган жамиятни шакллантириш муаммолари» Республика илмий-услубий семинар материаллари тўплами. - Тошкент. 2015. 120-127 б.

Автореферат «Молия» журнали таҳририятида таҳрирдан ўтказилди

Босишга рухсат этилди: 07.01.2022 Бичими: 60x84 1/8 «Times New Roman»  
гарнитурда рақамли босма усулда босилди.  
Шартли босма табағи 4,2. Адади: 100. Буюртма: № 7.

«DAVR MATBUOT SAVDO» МЧЖ  
босмахонасида чоп этилди.  
100198, Тошкент, Қўйлик, 4-мавзе, 46.