



KIBERXAVFSIZLIK SOHASI RISKLARNI SUG'URTA QILISH ZARURLIGI

Shuxratov Shohrux Sherzod o'g'li
Bank-moliya akademiyasi magistranti

НЕОБХОДИМОСТЬ СТРАХОВАНИЯ РИСКОВ КИБЕРБЕЗОПАСНОСТИ

Шухратов Шохрух Шерзод угли
Магистрант Банковско-финансовой академии

THE NEED FOR INSURANCE OF CYBER SECURITY RISKS

Shukhratov Shokhrukh Sherzod o'g'li
Graduate student of the Banking and Finance Academy

Annotatsiya: Kiber xujumlar rivojlanotgan vaqtda uni oldini olish maqsadida kiber hujumlardan korxona, tashkilotlarni himolash va sug'urtalash muhim hisoblanadi. Kiber hujumlar soni axborat texnologiyalar rivojlangani sari ortib bormoqda. Shu bois hozirgi vaqtda kiber risklarni sug'urta qilish eng samarali yo'llardan biri hisoblanadi. Risklarni sug'urta qilish korxona, tashkilotlar harajatlarini ma'lum bir miqdorda kamaytiradi. Iqtisodiyoti rivojlangan shu bilan bir qatorda xorijiy mamlakatlarda kiber risklarni sug'urta qilish ancha rivajlangan va o'zini natijalarini berib kelmoqda.

Tayanch so'zlar: Kiber hujum, kiberxavsizlik, sug'urta, xorijiy mamlakatlar, risklar, zaifliklar, davlat, kiber sug'urta.

Аннотация: В условиях стремительного развития кибератак важным аспектом является защита и страхование предприятий и организаций. С развитием информационных технологий количество кибератак продолжает расти. Поэтому в настоящее время страхование киберрисков считается одним из наиболее эффективных способов защиты. Страхование рисков позволяет в определенной степени сократить расходы предприятий и организаций. В экономически развитых, а также в зарубежных странах страхование киберрисков достаточно развито и дает свои положительные результаты.

Ключевые слова: Кибератака, кибербезопасность, страхование, зарубежные страны, риски, уязвимости, государство, киберстрахование.

Abstract: Amidst the rapid evolution of cyberattacks, protecting and insuring enterprises and organizations is crucial for prevention. The number of cyberattacks is increasing alongside the advancement of information technology. Therefore, cyber risk insurance is currently considered one of the most effective methods. Risk insurance reduces the costs of enterprises and organizations to a certain extent. In economically developed and foreign countries, cyber risk insurance is well-developed and has been yielding significant results.



Keywords: *Cyberattack, cybersecurity, insurance, foreign countries, risks, vulnerabilities, state, cyber insurance.*

KIRISH

O'zbekiston iqtisodiyotini rivojlantirish maqsadida bir qator strategiyalar ishlab chiqarilmoqda, bunga misol qilib "Harakatlar strategiyasidan-Taraqiyot strategiyasi sari" tamoyiliga asosan yetti ustivor yo'nalishdan iborat 2022-2026 yillarga mo'ljallangan Yangi O'zbekistonning "Taraqqiyot strategiyasi"⁹⁴ ishlab chiqilgan bo'lib, elektron hukumat xavfsizligini oshirish ularning rivojlanishi uchun aniq ishlanmalar mavjud.

O'zbekiston Respublikasi Prezidentining 05.10.2020 yildagi PF-6079-son farmoniga asosan "Raqamli O'zbekiston — 2030" strategiya⁹⁵ga asosan raqamli iqtisodiyotni rivojlantirish yo'llari belgilangan. Iqtisodiyot rivojlangani sari unga bo'lgan havf-hatarlar soni oshishi kuzatilishi mumkin.

Shuningdek, inson huquqlarini ta'minlash, davlat organlarining hisobdorligi va ochiqqligini kuchaytirish hamda fuqarolik jamiyati institutlari, ommaviy axborot vositalarining roli, aholi va jamoat birlashmalarining siyosiy faolligini oshirish bo'yicha tizimli ishlar amalga oshirildi.

Milliy iqtisodiyotni isloh qilish borasida tashqi savdo, soliq va moliya siyosatini liberallashtirish, tadbirkorlikni qo'llab-quvvatlash va xususiy mulk daxlsizligini kafolatlash, qishloq xo'jaligi mahsulotlarini chuqur qayta ishlashni tashkil etish hamda hududlarni jadal rivojlantirishni ta'minlash bo'yicha ta'sirchan choralar ko'rildi.

"Kiberxavfsizlik markazi" DUK tomonidan o'tgan yil mobaynida⁹⁶ O'zbekiston Respublikasi davlat idoralarining 81 ta rasmiy veb- resurslari amaldagi axborot va kiberxavfsizlik talablariga javob berishi darajasini aniqlash bo'yicha ekspertizadan o'tkazildi. Ekspertiza natijalariga ko'ra, jami bo'lib mazkur resurslarda 316 ta turli xavf toifalariga oid kiberxavfsizlik zaifliklari aniqlandi.

Aniqlangan zaifliklarning 81% (255 ta) yuqori darajali xavf toifasiga tegishli ekanligi kuzatildi. Ushbu toifadagi zaifliklar veb-resurslarga yohud ma'lumotlar bazasiga ma'murlik huquqini qo'lga kiritgan holda, ularga ruxsatsiz kirish va/yoki maxfiy (konfidensial) ma'lumotlarni olish hamda veb-resursning manba kodini qo'lga kiritish imkoniyatini vujudga keltirishi bois, veb-resurslarga kiberxavfsizlik tamoyillarini izchil tadbiiq etilishi talabini dolzarblashtiradi.

Adabiyotlar sharhi

Ko'p yillar davomida axborot xavfsizligi muhim ishlardan biri bo'lib kelmoqda. Xorijiy adabiyotlarda kiberxavfsizlik sug'urtasiga o'zining fikr mulohazalarini bildirishgan⁹⁷. Kiberjinoyatlar soni doimiy ravishda o'sib bormoqda va bu ko'proq kompaniyalar ma'lumotlarning buzilishi, to'lov dasturlari va kiberxavfsizlikning

⁹⁴ O'zbekiston Respublikasi Prezidentining 28.01.2022 yildagi PF-60-son farmoni.

⁹⁵ O'zbekiston Respublikasi Prezidentining 05.10.2020 yildagi PF-6079-son farmoni.

⁹⁶ <https://csec.uz/> internet sahifasi asosida muallif tomonidan yozildi.

⁹⁷ <https://www.trendmicro.com/>



boshqa shakllari xavfi ostida qolishlarini anglatadi. Kiberxavfsizlik platformangizdagi turli xil vositalar va yechimlar kompaniyangizni himoya qilishga va bu buzilishlar sodir bo'lguncha ularni to'xtatishga yordam berishi mumkin bo'lsada, tashkilotingiz kiberxavf hodisasi tufayli o'g'irlangan har qanday nozik ma'lumotlar uchun javobgar bo'lishi mumkin. Kibersug'urta bilan kompaniyaning kiberxavfsizlik hujumidan kelib chiqadigan har qanday zararni to'lash majburiyati minimallashtiriladi, bu esa falokat yuz bergan taqdirda moliyaviy oqibatlarni yengillashtiradi.

Elektron ma'lumotlarning har qanday yo'qolishi, murosaga kelishi yoki o'g'irlanishi biznesingizga salbiy ta'sir ko'rsatishi mumkin. Bu sizning kompaniyangizga bo'lgan ishonchni yo'qotishni o'z ichiga olishi mumkin, bu ishonchsiz mijozlar bazasini yoki bunday hujumdan tiklanishdan kelib chiqadigan potentsial moliyaviy xarajatlarni anglatadi. Kiber sug'urta ushbu moliyaviy xavfni kamaytirishga yordam beradi va biznesingizni cho'ntagidan to'lashdan saqlaydi.

Kibersug'urta quyidagi muammolarni bartaraf etishga yordam beradi:

- Yuridik to'lovlar;
- Ta'sir qilingan mijozlarning shaxsiy identifikatorlarini tiklash qiymati;
- Buzilgan ma'lumotlarni qayta tiklash narxi (masalan, to'lov dasturi bilan bog'liq ish);
- Buzilgan kompyuter tizimlariga har qanday zararni tuzatishning umumiy qiymati;
- Har qanday mumkin bo'lgan ma'lumotlar buzilishi haqida mijozlarni xabardor qilishning moliyaviy xarajatlari.

Kiberhujum sodir bo'lgan taqdirda, aksariyat kiber sug'urta polislari ma'lumotlar yoki elektron tizimlar yo'qolgan, shikastlangan, o'g'irlangan yoki yo'q qilingan taqdirda moliyaviy va obro'ga oid xarajatlarni qoplaydi. Bunga birinchi tomon xarajatlari (sug'urtani sotib oluvchi tashkilot duch keladigan) va uchinchi tomon xarajatlari (boshqa tashkilotlar yoki jismoniy shaxslar duch keladigan) kiradi.

Birinchi tomon kompensatsiyasi quyidagi xarajatlarni o'z ichiga oladi:

- Kiberjinoyatlarni tekshirish;
- Xavfsizlik buzilishi tufayli ma'lumotlar va kompyuter tizimini tiklash yo'qolgan;
- Korxonaning yopilishi tufayli daromad yo'qotildi;
- Xakerlik da'volari, shu jumladan to'lovlar;
- Xabar berish to'lovlari (agar qoidalar tashkilotlardan ta'sirlangan uchinchi tomonlarni xabardor qilishni talab qilsa).

Sug'urtani sotib olgan tashkilotga qarshi da'vo natijasida uchinchi tomon xarajatlari quyidagilarni o'z ichiga oladi:

- Zarar va hisob-kitoblar;
- Huquqiy himoya xarajatlari;



- Yevropa Ittifoqining ma'lumotlarni himoya qilish bo'yicha umumiy reglamenti (GDPR) yoki shunga o'xshash qoidalarni buzgan da'volar⁹⁸.

Kiber javobgarlik sug'urtasi ma'lumotlarning buzilishi va biznesingizga kiberhujumlar bilan bog'liq xarajatlarni qoplashi mumkin. Ushbu xarajatlar kiber hodisa tufayli yo'qolgan daromad, buzilishdan zarar ko'rgan mijozlarni xabardor qilish bilan bog'liq xarajatlar, buzilgan ma'lumotlarni qayta tiklash xarajatlari, shikastlangan kompyuter tizimlarini ta'mirlash xarajatlari va boshqalarni o'z ichiga olishi mumkin⁹⁹.

Sayohatchilarning kiber qamrovi kiberhujumning halokatli moliyaviy oqibatlariga qarshi muhim kafolat bo'lishi mumkin. Sayohatchilar biznesingizning tavakkalchilik darajasiga qarab moslashtirilgan sug'urta yechimlarini taklif qiladilar, bunda quyidagi masalalarni hal qilish mumkin bo'lgan qamrov variantlari mavjud:

- sud-tibbiy tekshiruvlar;
- sud xarajatlari;
- tartibga soluvchi mudofaa xarajatlari / jarimalar;
- inqirozni boshqarish xarajatlari;
- biznesning uzilishi;
- kiber tovlamachilik va yaxshilash.

Tadqiqot metodologiyasi

Ushbu maqola metodologiyasida tahlil va sintez, ilmiy abstraktsiya, umumlashtirish, qiyosiy nazariy talqin usullari qo'llaniladi. Bundan tashqari, maqolaning ilmiy asosini olimlarning mahalliy va xorijiy ilmiy nashrlardagi tadqiqotlaridan olingan xalqaro ma'lumotlar tashkil etadi.

Muhokamalar va natijalar

Kiberxafsizlik sug'urtasi bo'yicha xorijiy davlatlar tajribasidan kelib chiqib shuni aytishimiz mumkinki kiber sug'urta deganda kiber javobgarlik sug'urtasi sifatida ham tanilgan, tashkilotga kiber bilan bog'liq xavfsizlik buzilishi yoki shunga o'xshash hodisalardan tiklanish bilan bog'liq xarajatlarni kamaytirishga yordam berish uchun mo'ljallangan. Ushbu sug'urta turi birinchi tomonning zararlari yoki uchinchi shaxslarning da'volari bilan bog'liq xarajatlarni qoplaydi. Biroq, siyosatlar sezilarli darajada farq qiladi va yuqori profilli kiberhujumlar landshaftni o'zgartirishda davom etmoqda.

Kiber sug'urta talablari sug'urta provayderlari va siyosat turlari bo'yicha farq qiladi. Korxonalar qamrab olish huquqiga ega bo'lishlari kerak bo'lgan ba'zi umumiy talablar mavjud. Talablar quyidagilardan iborat:

1. Xatarlarni baholash: Sug'urta kompaniyalari ko'pincha tashkilotning xavf profilini tushunish uchun keng qamrovli xavfni baholashni talab qiladi. Ushbu baholash biznesni kiberhujumlarga duchor qilishi mumkin bo'lgan zaifliklarni aniqlashga yordam beradi.

⁹⁸ <https://www.bluevoyant.com/>

⁹⁹ <https://www.travelers.com/>



2. Xavfsizlik nazorati: Kompaniyalar mustahkam xavfsizlik nazoratiga ega bo'lishi kerak. Bunga xavfsiz kirishni boshqarish, xavfsizlik devorlari, so'nggi nuqtani aniqlash va javob berish (EDR) va ko'p faktorli autentifikatsiya (MFA) kiradi.

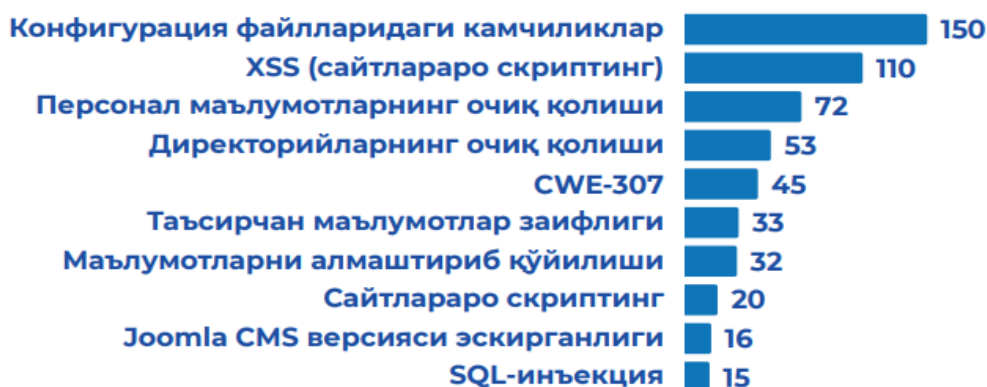
3. Hodisalarga javob berish rejasi: Korxonalarda kiber hodisani samarali boshqarish uchun hodisalarga batafsil javob rejasi bo'lishi kerak. Ushbu reja buzilishni aniqlash, bartaraf etish, yo'q qilish va bartaraf etish bo'yicha qadamlarni, shuningdek, jamoatchilik bilan aloqalar strategiyasini o'z ichiga olishi kerak.

4. Muntazam yangilanishlar va yamoqlar: Tizimlar, ilovalar va qurilmalarni (jumladan, noutbuklarni) muntazam yangilash va tuzatish ma'lum zaifliklardan himoyalani uchun juda muhimdir.

5. Xodimlarni o'qitish: Fishing hujumlari, to'lov dasturlari va kiberjinoyatlarning boshqa shakllari haqida xodimlarni muntazam ravishda o'qitish juda muhimdir. Xodimlar xavfsiz internet amaliyotlari va potentsial kiber tahdidlarni qanday aniqlash haqida xabardor bo'lishi kerak.

6. Qoidalarga muvofiqlik: Kompaniyalar tegishli kiberxavfsizlik qoidalariga rioya qilishlari kerak. Bunga Tarmoq infratuzilmasi (NERC) Kritik infratuzilmani himoya qilish (CIP) qoidalari kabi standartlar kiradi.

Ushbu talablarga javob berish nafaqat kiber sug'urta qoplamasini olishga yordam beradi, balki tashkilotning umumiy kiberxavfsizlik pozitsiyasini mustahkamlaydi.



1-rasm¹⁰⁰. "Kiberxavfsizlik" DUK markazi mutahasislar tomonidan bartaraf qilingan zaifliklar. Yuqorida ko'rtaslangan rasmdagi muammolar o'tgan yilning mos davriga nisbatan 3% ga kamaygan.

Davlat idoralari veb-resurslarida aniqlangan kiberxavfsizlik xodisalari o'rganilganda veb-resurslarda mavjud bo'lgan quyidagi zaifliklar sababli kelganligi kuzatiladi:

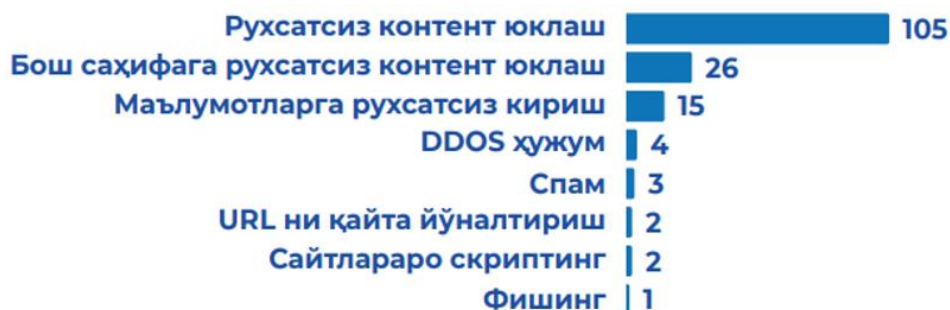
- foydalanuvchi kontentini tekshirish va filtirlashning mavjud emasligi;
- kodlashdagi zaifliklar (PHP-plaginalari, csrf-zaifliklari, kross-brauzer zaifliklari va boshqalar);
- zaif parol ximoyasi.

Shu o'rinda alohida ta'kidlash joizki, so'ngi paytlarda xalqaro axborot xavfsizligining zamonaviy manzarasida jiddiy o'zgarishlarishlarni keltirib

¹⁰⁰ <https://csec.uz/>



chiqarayotgan jahon miqiyosida asosiy “kuch markazi” o’rtasidagi geosiyosiy qarama-qarshiliklarning keskinlashuvi asnosida, global kibermakon yuzaga kelayotgan siyosiy-harbiy to’qnashuvlarning asosiy maydonlaridan biriga aylanib ulgurganligi, respublikamiz muhim axborot infratuzilmasining kiberxavfsizlik xolatiga ta’sir ko’rsatuvchi global omil sifatida yuzaga chiqmoqda.



2-rasm¹⁰¹. Aniqlangan kiberxavfsizlik xodisalari turlari. Yuqoridagi rasmdan korishimiz mumkinki internet tarmog’ining milliy segmentdagi veb-resurslarining doimiy monitoringi jarayonida jami 158 ta kiberxavfsizlik xodisasi aniqlangan. Maskur vaziyatda, turli ekspert xisob-kitoblarga ko’ra, dunyo miqiyosida yaqin uch yilda kiberjinoyatchilikdan ko’rilgan global zarar yiliga 15% ga o’sib borgan holda, 8 trillion AQSH dollarini, 2025-yilga borib esa 10.5 trillion AQSH dollarini tashkil etishi taxmin qilinmoqda. Shu bilan birga, tobora raqamlashtirilayotgan tashkilot va korxonalarning, “narsalar interneti” qurilmalari va turli toifadagi iste’molchilarni turli kiberjinoyatlardan ximoya qilish zaruriyati 2021-yildan 2025-yilgacha bo’lgan davr mobaynida umumjahon darajasida kiberxavfsizlik maxsulotlari va xizmatlariga yo’naltiriladigan xarajatlar miqiyosida 1.75 trillion AQSH dollariga yetishiga olib kelishi ta’kitlanmoqda.



3-rasm¹⁰². Kiberxujimlar turlari kesimida.

Shuni aytishimiz mumkinki monitoring tizimiga ulangan veb-resurslarga uyushtirilgan kiberxujumlarning turlari orasida eng ko’p qo’llanilganlari ko’rsatilgan. “Kiberxavfsizlik markazi” DUKda mavjud ma’lumotlarning taxliliga ko’ra, respublikamizda davlat va xo’jalik boshqaruvi organlarining axborot tizimlarida

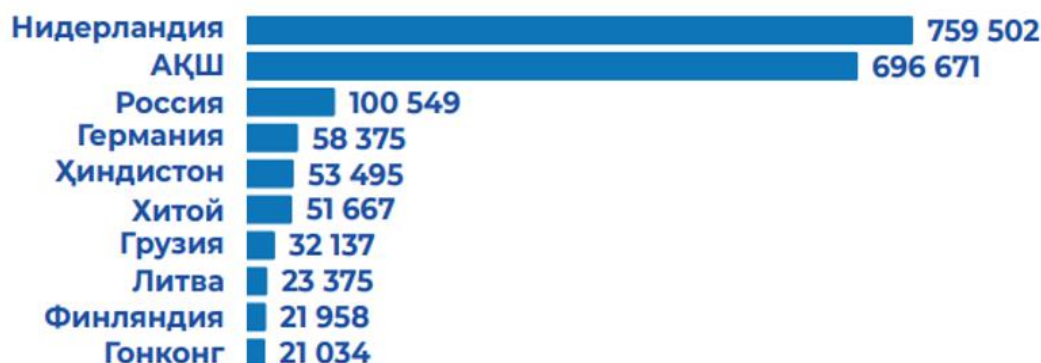
¹⁰¹ <https://csec.uz/>

¹⁰² <https://csec.uz/>



raqamlashtirish tadbirlarini shiddan bilan amalga oshirilishi bilan bir qatorda but izimlarga bo'lgan kibertaxdidlarning xavflilik darajasining jiddiylashuvi xamda son-sifat ko'rsatgichlari jihatidan o'sish tendensiyasi kuzatilmoqda¹⁰³.

Rasmiy veb-resurslarni axborat va kiberxavfsizlik talablari bo'yicha davomida umumiy hisobda 677 ta veb-resursda jami bo'lib, 1186 ta zaiflik aniqlandi. Ulardan 1022 tasi davlat organlari veb-resurslariga to'g'ri keladi. Buning natijasida 2023- yilda davlat tshkilotlariga tegishli veb-resurslarda aniqlanib bartaraf etilmagan 46 ta zaifliklarning 36 tasi bartaraf etildi, 7 ta veb-resursning ish faoliyati vaqtincha to'xtatildi.



4-rasm¹⁰⁴ Kiberhujumlar davlatlar kesimida. 2023-yilda amalga oshirilgan kiberhujumlarning geografik jihatdan taluqliligi taxliliga ko'ra, quyida keltirilgan davlatlarda eng ko'p kiberhujumlar kuzatilgan.

"Kiberxavfsizlik markazi" DUK tomonidan bir qancha davlat idoralarining axborat tizimi va resurslarini axborat va kiberxavfsizlik talablariga muvofiqligi espertizasi yuzasidan amalga oshirilgan tadbirlar jarayonida qator kamchilik va zaifliklar aniqlanishi natijasida umumiy xisobda 25.7 milliondan ziyod O'zbekiston Respublikasi fuqorolarining shaxsiy ma'lumotlari sizib chiqishiga, axboratning yo'q qilinishi xamda qalbakilashtirilishiga, tizimning ma'lumotlar omborini yuklab olish imkonini beruvchi salbiy xolat va omillar bartaraf etildi¹⁰⁵.

Xulosa

Kiberhavfsizlik zaifliklar kelib chiqishining asosiy sabablari sifatida quyda to'xtalib o'tamiz:

- Axborat tizimi va resurslarni ishlab chiqish jarayonida yo'l qo'yilgan xatoliklar;
- Axborat tizimi va resurslarni ishlab chiqishda axborat va kiberxavhsizlik talablarini;
- Axborat tizimi va resurslarni ishlab chiqilgandan so'ng autsors kompaniya mutaxassislari yoki tashkilotning AKT mutaxassislari tomonidan muntazam ravishda texnik qo'llab quvvatlash ishlari olib borilmasligi;
- AKT va kiberhavfsizlik soxasida malakali mutaxassislar yetishmasligi;
- Kiberhavfsizlik masalalarini xal etishda yetarli darajada moliyalashtirilmaslik.

¹⁰³ <https://csec.uz/>

¹⁰⁴ <https://csec.uz/>

¹⁰⁵ <https://csec.uz/>



Jahonning rivojlangan, rivojlanayotgan davlatlarida kiberrisklarni sug'urta qilish ancha rivojlangan. Bu o'zining samarasini, foydasi berib kelmoqda. Hozirgi vaqtga yurtimizda ham axborat havfsizligi yuzasidan sezilarli kamchilklar kelib chiqmoqda. Joriy yilning hozirgi vaqtiga kelib O'zbekiston sug'urta bozorida 38 ta sug'urta kompaniyasi o'z ish faoliyatini olib bormoqda.

Sug'urta bozorida haligacha keberrisklarini sug'urtasi bo'yicha ish qilinmagan. Sug'urta kompaniyalarimiz kiberhavflardan sug'urta qilish praduktini ishlab chiqishsa sug'urta kompaniyalar daromadini ham oshirishga yordam beradi.

Korxona va tashkilotlar uchun kiberrisklarni sug'urta qilish, ko'rayotgan zararlarini bir buncha kamaytiradi.

Kiberhujumlar soni yildan yilga o'rtayotganligini hisobga olgan holda shuni aytishimiz mumkinki, bu masalaning oqilona yechimi sifatida kiberrisklarni sug'urta qilish bo'yicha ishlar olib borilishi kerak deb hisoblaymiz.

FOYDALANILGAN ADABIYOTLAR RO'YHATI:

1. O'zbekiston Respublikasi Prezidentining 28.01.2022 yildagi PF-60-son farmoni.
2. O'zbekiston Respublikasi Prezidentining 05.10.2020 yildagi PF-6079-son farmoni.
3. <https://csec.uz/> internet sahifasi asosida muallif tomonidan yozildi.
4. <https://www.trendmicro.com/>
5. <https://www.bluevoyant.com/>
6. <https://www.travelers.com/>
7. <https://csec.uz/>