KIBERHUJUMLAR VA ULARNING ELEKTRON TIJORATGA TA'SIRI

Djalalov Jamoliddin Muzafarovich
TATU, "Menejment va marketing" kafedrasi katta o'qituvchisi

Annotasiya

Axborot texnologiyalarining tezkor rivojlanishi dunyo bo'ylab turli sohalarni sezilarli darajada o'zgartirdi, elektron tijorat esazamonaviy iqtisodiyotning muhim qismiga aylandi. O'zbekistonda ham raqamli makonning rivojlanishi bilan biznes tranzaksiyalarida yangi davr boshlandi, bu esa ham imkoniyatlar, ham qiyinchiliklarni keltirib chiqarmoqda. Onlayn xaridlar va raqamli to'lovlar ommalashar ekan, iste'molchilar va bizneslar xavfsizligini ta'minlash uchun kuchli kiberxavfsizlik choralarini qo'llash zaruriyati ortib bormoqda.

Elektron tijoratdagi kiberxavfsizlik – bu ma'lumotlar, tarmoqlar va tizimlarni kibertahdidlardan himoya qilish uchun mo'ljallangan turli amaliyotlarni o'z ichiga olgan murakkab sohadir. O'zbekiston sharoitida bu, infratuzilma, me'yoriy-huquqiy baza va jamoatchilikning xabardorligi bilan bog'liq o'ziga xos muammolarni hal qilishni talab etadi. Mamlakat global raqamli iqtisodiyotga integratsiyalashishga intilar ekan, elektron tijorat platformalarini kiberhujumlardan himoya qilish ishonchni mustahkamlash va barqaror o'sishni ta'minlash uchun juda muhimdir.

Kalit so'zlar: elektron tijorat, kiberxavfsizlik, tarmoq, Onlayn xaridlar, biznes tranzaksiyalari, domen, kiberhujum

Аннотация

Ускоренное развитие информационных технологий значительно изменило различные сферы во всем мире, а электронная коммерция стала важной частью современной экономики. С развитием цифрового пространства в Узбекистане началась новая эра в бизнес-транзакциях, что создает как возможности, так и трудности. По мере популяризации онлайн-покупок и цифровых платежей возрастает необходимость применения сильных мер кибербезопасности для обеспечения безопасности потребителей и бизнеса.

Кибербезопасность в электронной коммерции — это сложная область, включающая в себя различные практики защиты данных, сетей и систем от киберугроз. В условиях Узбекистана это требует решения конкретных проблем, связанных с инфраструктурой, нормативно-правовой базой и информированностью общественности. Поскольку страна стремится интегрироваться в глобальную цифровую экономику, защита платформ электронной коммерции от кибератак имеет решающее значение для укрепления доверия и обеспечения устойчивого роста.

Ключевые слова: электронная коммерция, кибербезопасность, сеть, онлайн-закупки, бизнес-транзакции, домен, кибератака

Abstract

The rapid development of information technology has significantly changed various industries around the world, and e-commerce has become an important part of the modern economy. With the development of the digital space in Uzbekistan, a new era has begun in business transactions, which creates both opportunities and difficulties. As online shopping and digital payments become more popular, there is an increasing need for strong cybersecurity measures to keep consumers and businesses safe.

Cybersecurity in e-commerce is a complex field that encompasses a variety of practices designed to protect data, networks, and systems from cyber threats. In the conditions of Uzbekistan, this requires solving specific problems related to infrastructure, regulatory framework and public awareness. As the country strives to integrate into the global digital economy, protecting e-commerce platforms from cyber attacks is critical to building trust and ensuring sustainable growth.

Keywords: e-commerce, cyber security, network, online shopping, business transactions, domain, cyber attack

KIRISH

O‘zbekiston Respublika Prezidentining 28.01.2022-yildagi “2022 — 2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi PF-60-son[1] Farmon loyihasida O‘zbekistonda kiberjinoyatchilikning oldini olish tizimi yaratish belgilab qo‘yilgan. 2023—2026-yillar uchun O‘zbekistonning kiberxavfsizlik strategiyasi ishlab chiqish rejalashtirilgan bo‘lib, bu esa o‘z navbatida “uz” domen zonasi internet-makonining kiberxavfsizligini ta’minlashning asosiy yo‘nalishlarini belgilaydi. Elektron hukumat, energetika, raqamli iqtisodiyot tizimlari va muhim axborot infratuzilmasiga taalluqli boshqa yo‘nalishlarni himoya qilish bo‘yicha kompleks vazifalar tuzib chiqiladi.

Shuningdek, 2022-yil o‘tkazilgan yig‘ilishda davlatimiz rahbari “Yilning birinchi chorakning o‘zida axborot tizimlariga chetdan 200 dan ortiq kiberhujum uyushtirilgan. Shuning uchun bugun kiberxavfsizlik to‘g‘risida Qonunni imzoladim.Bu yangi Qonun hozirgi zamon tahdidlariga qarshi kurashish uchun huquqiy asos bo‘ladi”, deb ta’kidlab o‘tgan. Shu yilning o‘zida O‘zbekiston Respublikasining qonunchilik palatasi tomonidan 2022-yil 25-fevralda qabul qilingan Senat tomonidan 2022-yil 17-martda ma’qullangan “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-сон[2] Qonun kuchga kirgan. Ushbu Qonun sohada ko‘plab yangi imkoniyatlarni ma’muriy- huquqiy asoslarni belgilab berdi. Hamda, barcha yo‘nalishlarda, jumladan, elektron tijoratda ham uchraydigan barcha kiberjinoyatlar yoki axborot xavfsizligiga tahdid soluvchi omillar, Qonunda ko‘rsatilgan tartibda hal qilinib, jinoyatchilarga keltirilgan zarar turiga va hajmiga ko‘ra jazo turi qo‘llaniladi.

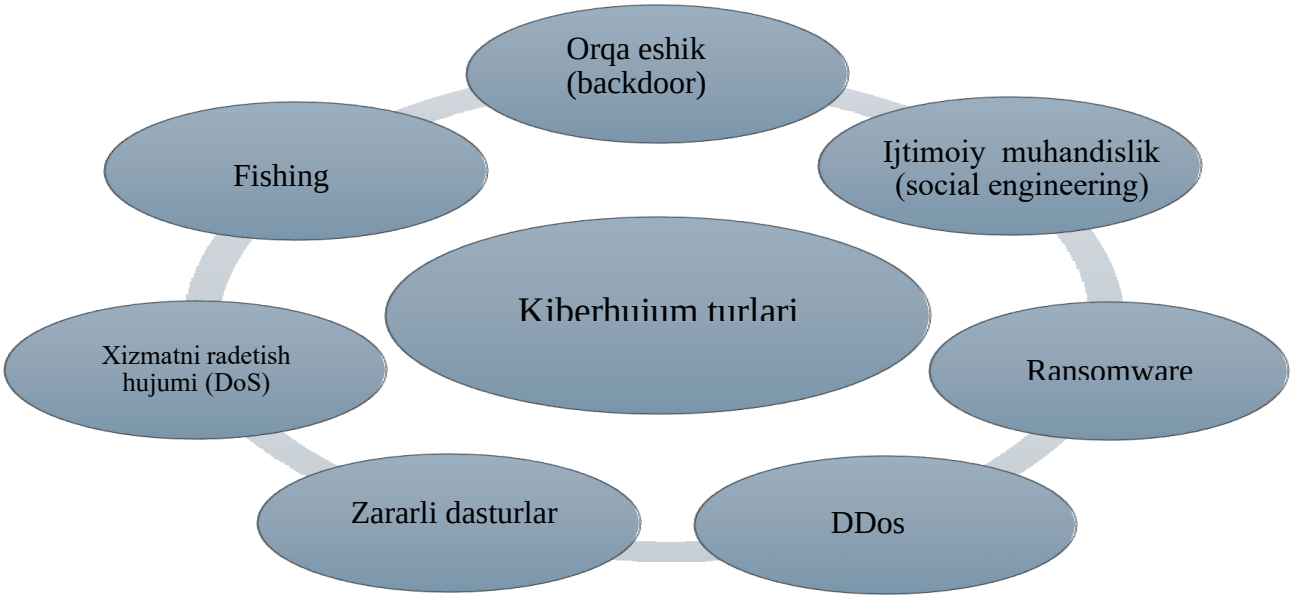
ADABIYOTLAR SHARHI

[1] https://lex.uz/docs/-5841063
[2] https://www.lex.uz/uz/docs/-5960604

Hozirgi kunda, axborot texnologiyalari va raqamli dunyoning rivojlanishi bilan birga, bizning kundalik hayotimiz ham tubdan o‘zgarmoqda. Har kuni milliardlab odamlar internetga ulanib, turli xizmatlardan foydalanadi, muloqot qiladi, ishlarini bajaradi va ma’lumot almashadi. Bu jarayonlar bizga qulaylik va samaradorlikni olib keladi, lekin ayni paytda yangi xavf-xatarlar va tahdidlarni hamkeltirib chiqarmoqda. Shu munosabat bilan, kiberxavfsizlik masalasi birlamchi ahamiyat kasb etmoqda. Kiberxavfsizlik — bu axborotni, tizimlarni va tarmoqlarnikiber hujumlardan himoya qilish bo‘yicha choralar tizimi bo‘lib, uning asosiymaqsadi bizning raqamli dunyoda xavfsizligimizni ta’minlashdir.

Texnologiya yuksalayotgan bir davrda, kiberxavfsizlik faqatgina IT mutaxassislari uchun emas, balki har bir inson uchun ham muhim masalaga aylanmoqda. Kiberxavfsizlik bilan shug‘ullanish — bu bizning shaxsiy hayotimizni, biznes faoliyatimizni va davlat xavfsizligini himoya qilish demakdir. Bu borada sodir bo‘ladigan hujumlar ko‘pincha kiber jinoyatlar, kiber terrorizm, va hatto davlatlararo kiber urushlar ko‘rinishida namoyon bo‘ladi. Shuning uchun, kiberxavfsizlikni kuchaytirish va yangi texnologiyalarni joriy etish orqali tahdidlarga qarshi kurashish zamon talabidir.

Kiberxavfsizlikning ahamiyati, uning asosiy xususiyatlari va strategiyalari bizga qanday qilib raqamli dunyoda xavfsiz va barqaror yashashni o‘rgatadi. Bu esa, o‘z navbatida, bizning jamiyatimizning raqamli kelajagini ta’minlash uchun mustahkam poydevor yaratadi. Kiberxavfsizlikni ta’minlash, faqatgina texnik choralar bilan cheklanib qolmasdan, balki ijtimoiy ongni oshirish, xavfsizlik madaniyatini shakllantirish va global hamkorlikni rivojlantirish orqali amalga oshirilishi lozim. Ko‘pgina korxonalar endi o‘zlarining korporativ risklarni boshqarishning bir qismi sifatida axborot risklarini boshqarishni ham o‘z ichigaolmoqda(1-rasm).



1-rasm. Kiberhujum turlari[1]

[1] O‘rganilgan ma’lumotlar asosida muallif tomonida tuzildi.

Orqa eshik (backdoor) — bu kompyuter tizimida, mahsulotda yoki o‘rnatilgan qurilmadass (router kabi) oddiy autentifikatsiya yoki shifrlashni chetlab o‘tish usuli. Kiberhujumchilar ko‘pincha kompyuterga masofaviy kirishni ta’minlash, ochiq matnli pasportlarga kirish, qattiq disklarni o‘chirish yoki bulut ichida ma’lumotlarni uzatish uchun orqa eshiklardan foydalanadilar. Backdoor, shuningdek, dasturning yashirin qismi, alohida dastur, apparat yoki operatsion tizimlarning proshivkalarida kod shaklida ham bo‘lishi mumkin. Ba’zi orqa eshiklar yashirincha o‘rnatilgan bo‘lsa-da, boshqa orqa eshiklar ataylab va ma’lum shaklda o‘rnatilgan bo‘ladi. Ular ishlab chiqaruvchiga foydalanuvchi parolini tiklash usulini taqdim etish kabi qonuniy foydalanishga ega. Ushbu qonuniy orqa eshiklar noto‘g‘ri sozlanganda ma’lumotlar sizib chiqishiga olib kelishi mumkin, natijada shaxsiy ma’lumotlar o‘g‘irlanishi uchun ishlatilishi mumkin bo‘lgan maxfiy ma’lumotlar va shaxsiy ma’lumotlarga kirish mumkin bo‘ladi.

METODOLOGIYA

Kiberhujumlar zamonaviy dunyoning eng jiddiy tahdidlaridan biriga aylangan bo‘lib, ularning elektron tijoratga ta’siri beqiyos darajada oshib bormoqda. Raqamli iqtisodiyotning tez rivojlanishi va internet orqali amalga oshirilayotgan savdo hajmining ortishi bilan, onlayn platformalar kiberxavfsizlik masalalariga ko‘proq e’tibor qaratishga majbur bo‘lmoqda. Kiberhujumlar - elektron tijorat kompaniyalarining ma’lumotlar bazalariga, mijozlarining shaxsiy va moliyaviy ma’lumotlariga jiddiy xavf tug‘diradi. Ushbu tahdidlar nafaqat kompaniyalarga moliyaviy zarar keltiradi, balki mijozlarning ishonchini yo‘qotish va brendning obro‘siga putur yetkazish orqali uzoq muddatli salbiy oqibatlarga olib kelishi mumkin. Shuning uchun, elektron tijorat sub’ektlari kiberxavfsizlikni ta’minlash bo‘yicha zamonaviy texnologiyalar va strategiyalarni tatbiq etishga katta ahamiyat berishlari lozim.

Veb-saytlar va ilovalar pul o‘tkazish, xarid qilish yoki boshqa manfaatdor tomonlarga ma’lumot sotishdan potentsial foyda keltirishi sababli asosiy maqsad bo‘lgan kredit karta raqamlarini saqlaydigan onlayn brokerlik hisoblari va oziq-ovqat yetkazib berish ilovalari bilan moliyaviy tizimning bir qismiga aylanib bormoqda. Kommunal va sanoat uskunalari Energetika sektori uchun muhim infratuzilmaga hujum tabiiy ofatga o‘xshash server buzilishi oqibatlari bilan uzoq vaqt davomida katta hududlarda quvvat yo‘qotilishiga olib kelishi mumkin. Aviatsiyaning muhim infratuzilmasi hisob-kitoblarga tayanadi va elektr uzilishi yoki parvoz aloqasidagi uzilish butun dunyo bo‘ylab seziladigan kaskadli ta’sirga ega bo‘lishi mumkin. Bundan tashqari, samolyotlarda Wi-Fi-ning joriy etilishi ko‘pincha xavfli Wi-Fi tarmog‘idan foydalanadigan yo‘lovchilar uchun yana bir potentsial hujum vektorini anglatadi. Kompyuter va noutbuklar foydalanuvchi kompyuterlari parollar yoki moliyaviy hisob ma’lumotlarini yig‘ish uchun umumiy maqsadlardir. Ushbu xavf smartfonlar, planshetlar, aqlli soatlar va boshqa internetga ulangan qurilmalarning o‘sishi bilan

bog‘liq bo‘lib, ular ko‘pincha joylashuv va yurak urishi kabi shaxsiy ma’lumotlarni to‘playdi.

Korporatsiyalar turli sabablarga ko‘ra umumiy nishonlar bo‘lib, shaxsiy ma’lumotlarni o‘g‘irlashdan tortib, tashviqot, sabotaj yoki nishonlarga josuslik qilish uchun kiber urushda qatnashmoqchi bo‘lgan shaxslar va xorijiy hukumatlar tomonidan ma’lumotlar buzilishigacha olib kelishi mumkin. Avtomobillar tobora ko‘proq kruiz nazorati, dvigatel vaqtini belgilash, blokirovkaga qarshi tormozlar, xavfsizlik kamarlarini tortgichlar, eshik qulflari, xavfsizlik yostiqchalari va ko‘plab modellardagi kompyuterlar tomonidan boshqariladigan haydovchiga yordam berish tizimi bilan kompyuterlashtirilgan. Bu esa o‘z navbatida turli kiberhujumlarga uchrashiga olib kelishi mumkin. Bort qurilmalari va uyali tarmoqlar bilan aloqa qilish uchun Wi-Fi va Bluetooth-ning joriy etilishi kiberhujumlar xavfini oshirdi, o‘z-o‘zidan boshqariladigan avtomobillar yanada murakkab bo‘lishi kutilmoqda.

TAHLIL VA NATIJALAR

Hukumat va harbiy tizimlar odatda kiber urushda qatnashmoqchi bo‘lgan faollarva xorijiy hukumatlar tomonidan hujumga uchraydi. Kasalxona ichidagi diagnostika uskunalari kabi tibbiy tizimlar va yurak stimulyatori va insulin nasoslari kabi implantatsiya qilingan qurilmalar o‘limga olib kelishi mumkin bo‘lgan zaifliklarga ega hujum nishoni hisoblanadi. Tibbiy ma’lumotlar ko‘pincha shaxsiy ma’lumotlarni o‘g‘irlash, tibbiy sug‘urta firibgarligi va retsept bo‘yicha dori-darmonlar yoki dam olish maqsadlarida yoki qayta sotish uchun bemorlarni taqlid qilishda foydalanish uchun mo‘ljallangan(1-jadval).

1-jadval

2023-yilda ma’lumotlar buzilishi 10 taligi tahlili[1]

№	Tashkilot nomi	Soha	Joylashgan davlat	Ma’lumotlar buzilishi soni	Ma’lumotl ar chop etilgan oy
1	DarkBeam	Kiberxavfsizlik	Buyuk Britaniya	3,800,000,000	sentabr
2	Real Estate Wealth Network	Qurilish/ ko‘chmas mulk	AQSh	1,523,776,691	Dekabr
3	Indian Council of Medical Research (ICMR)	Sog‘liqnisaqlash	Hindiston	815,000,000	Oktabr
4	Kid Security	IT xizmatlari/ dasturlash	Qozog‘iston	300,000,000	Noyabr
5	Twitter (X)	IT xizmatlari/ dasturlash	AQSh	220,000,000	Yanvar
6	TuneFab	IT xizmatlari/ dasturlash	Gongkong	151,000,000	Dekabr
7	D Dori Media Group	Media	Isroil	100,000,000	Dekabr
8	Tigo	Telekom	Gongkong	100,000,000	Iyul
9	SAP SE Bulgaria	ITxizmatlari/ dasturlash	Bolgariya	95,592,696	Noyabr
10	LuxotticaGroup	Ishlab chiqarish	Italiya	70,000,000	May

[1] https://infocom.uz/kiberxavfsizlik-statistikasi/

2023-yilda onlayn firibgarlik AQSh korxonalariga sezilarli darajada zarar yetkazdi, FBI ma'lumotlariga ko'ra, yo'qotishlar 12,5 milliard dollardan oshdi. Bu o'tgan yilga nisbatan 22% ko'proqdir. Eng katta zarar investitsion firibgarliklardan kelib chiqqan bo'lib, 4,57 milliard dollarni tashkil etdi, bu ko'pincha kripto valyuta investitsiyalari firibgarliklarining 53% ga oshishi bilan bog'liq. Biznes elektron pochta kompromisi yana bir muhim omil bo'lib, 2,9 milliard dollar zarar keltirdi.

2023-yilda eng ko'p xabar qilingan firibgarlik phishing sxemalari bo'ldi, 298,000dan ortiq shikoyat bilan, bu barcha xabar qilingan hodisalarning taxminan 34% ini tashkil etdi. Bundan tashqari, ransomware hujumlari ham sezilarli darajada oshdi, ayniqsa sog'liqni saqlash, ishlab chiqarish va hukumat infratuzilmalari kabi tanqidiysektorlarni nishonga oldi.

Umuman olganda, kiber jinoyatchilikning o'sishi turli omillar, jumladan, kiber jinoyatchilarning o'sib borayotgan murakkabligi va firibgarlik faoliyatlari uchun raqamli vositalardan foydalanishning ko'payishi bilan bog'liq. FBIning Internet Jinoyat Shikoyat Markazi (IC3) ushbu masalalarni hal qilishda muhim rol o'ynamoqda, shikoyatlarni yig'ish, hodisalarni tekshirish va o'g'irlangan mablag'larni tiklashda yordam berishda davom etmoqda.

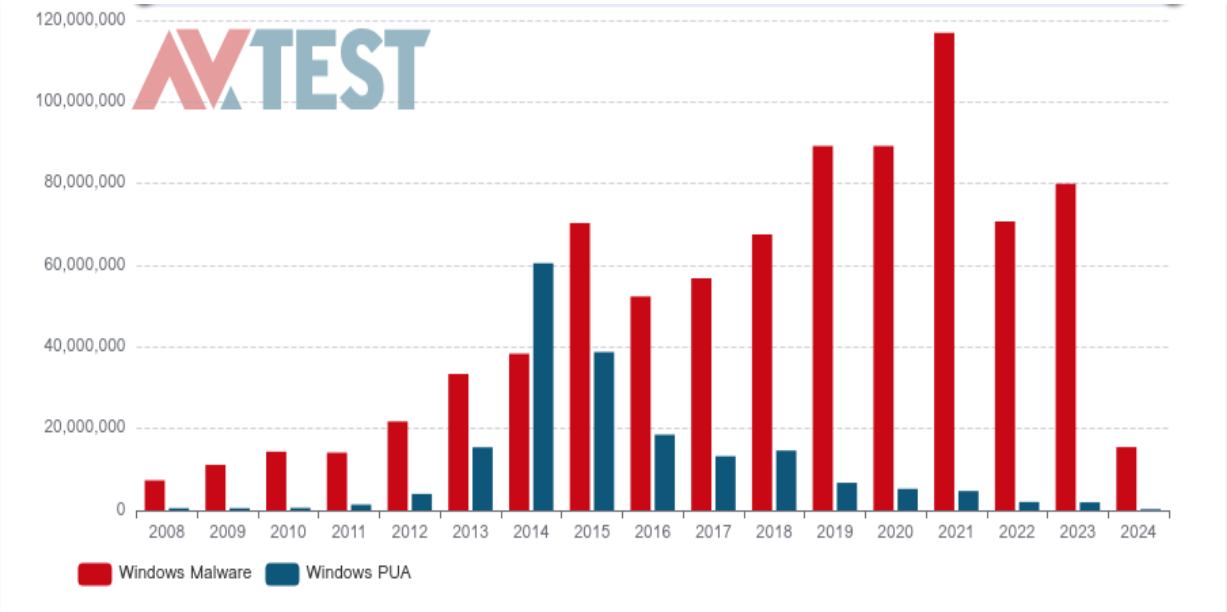
Statista ma'lumotlariga ko'ra, global elektron tijorat savdosi taxminan 5,2 trillion dollarni tashkil etdi. Bundan tashqari, ekspertlar bu ko'rsatkich 2026-yilga kelib 8,1 trillion dollarga yetib, kelgusi yillarda 56 foizga o'sishini bashorat qilmoqda. Biroq, bunday tez o'sish muqarrar ravishda turli qiyinchiliklarni keltirib chiqaradi va elektron tijorat xavfsizligini ta'minlash ulardan biridir.

Statistik ma'lumotlar shuni ko'rsatadiki, savdogarlar har yili kiberhujumlarning yuqori sur'atlariga duch kelishmoqda. LexisNexis'ning 2023-yilgi kiberjinoyatlar hisobotiga ko'ra, 2022-yilda kompyuter va mobil qurilmalarga hujumlar sezilarli darajada oshdi. Moliyaviy xizmatlar sektorida hujumlar yiliga 31% ga, elektron tijorat sektorida esa 29% ga ko'paygan. Umuman olganda, kompyuter va mobil kanallardagi raqamli to'lovlarga hujumlar 27% ga oshgan. Digital Identity Network'da kuzatilgan barcha tranzaksiyalarning 77% mobil tranzaksiyalarni tashkil etgan, mobil ilovalar esa bu trafikning 82% ini tashkil qilgan.

Zararli dasturlarning miqdori har yili o'sib bormoqda va zararli dasturlarga asoslangan hujumlarning intensivligi ham shunga munosib ravishda ko'tarilmoqda. Germaniyada joylashgan AV-TEST tadqiqot instituti har kuni 450000 ta yangi zararli dasturlarni aniqlaydi.

2023-yilda global miqyosda zararli dastur hujumlari soni taxminan 6 milliard bo'lgani, bu avvalgi yillarga nisbatan sezilarli o'sishni anglatadi. Bu kiber tahdidlarning davom etayotgan va rivojlanayotgan tabiati bilan bog'liq.

Ransomware hujumlari ham 2023-yilda keskin ko‘paydi, 2022-yilga nisbatan 68% o‘sish kuzatildi. Bu o‘sish natijasida jami 4,475 ransomware hujumi sodir bo‘ldi, bu yangi rekorddir. LockBit eng faol ransomware guruhi bo‘lib, bu hujumlarning katta qismiga javobgar bo‘ldi. O‘tkan yilda tarqatilgan xizmatni rad etish (DDoS) hujumlari ham katta tahdidbo‘lib qolmoqda. Microsoft kuniga o‘rtacha 1,500 DDoS hujumini qaytarishga muvaffaq bo‘ldi, bu katta tashkilotlarga qarshi kiber tahdidlarning doimiyligini ko‘rsatadi (Malwarebytes) (2-rasm).



2-rasm. Windows zararli dasturlari va PUA ni ishlab chiqish[1]

Sog‘liqni saqlash, ta’lim va moliya kabi muhim sektorlar asosiy nishon bo‘lib qolmoqda. Masalan, sog‘liqni saqlash tashkilotlari katta miqdordagi buzilishlarga duch kelishdi, ransomware hujumlari esa sezilarli ulushni tashkil etdi. Ta’lim sektorihujumlar sonining 70% oshishini ko‘rsatdi, bu uning zaifligini ta’kidlaydi.

2023-yilda zararli reklama yana kuchayib, kiberjinoyatchilar soxta reklamalar orqali zararli dasturlarni tarqatishdi. Bu usul, foydalanuvchilarni zararli dasturlarni yuklab olishga aldash uchun mashhur brendlarni taqlid qilishda ishlatilgan (Malwarebytes). Misol uchun yurtimizda ham so‘nggi yillarda kuzatilgan ko‘plab yolg‘on fake xabarlar, ko‘plab insonlarning pullarini yo‘qtishiga sabab bo‘ldi

Cl0p va ALPHV kabi ransomware guruhlari tomonidan nol-kun zaifliklaridan foydalanish ko‘paydi, bu ularga katta miqyosda murakkab hujumlar qilish imkonini berdi. Ushbu tendentsiya bunday eksploitlarga qarshi kuchli xavfsizlik choralari zarurligini ta’kidlaydi.

Xodimlar elektron tijorat korxonasining eng qimmatli aktivlaridan biri bo‘lib qolsa-da, ularning har biri jinoyatchilar uchun potentsial kirish nuqtasi bo‘lishi

[1] Malware Statistics & Trends Report | AV-TEST

mumkin. Hujumchilar xodimni manipulyatsiya qilish va qimmatli korporativ yoki mijozlar ma’lumotlariga kirish uchun ijtimoiy muhandislik usullaridan (masalan, qo‘rqituvchi dastur, bahona yoki o‘lja) foydalanishi mumkin.2023-yilda CS Hub o‘rtasida o‘tkazilgan bozor hisobotiga ko‘ra, korxonalarning 78 foizi ijtimoiy muhandislik va fishing hujumlarini elektron tijorat xavfsizligiga tahdidlar deb biladi.Shu bilan birga, 2023-yilgi Global kiberxavfsizlik xabardorligi bo‘yicha trening tadqiqotiga ko‘ra, korxonalarning deyarli 32 foizi xavfsizlik bo‘yicha o‘quv dasturlarida ijtimoiy muhandislikni qamrab olmaydi.

Ijtimoiy muhandislik va fishing hujumlari korxonalarga katta zarar yetkazishi mumkin. 2023-yilda phishing hujumlari dunyo bo‘ylab ko‘plab data buzilishlariga sabab bo‘ldi, va bu hujumlar eng ko‘p zarar keltiruvchi kiber tahdidlar qatoriga kiradi. Statistika shuni ko‘rsatadiki, ijtimoiy muhandislik texnikalari orqali amalga oshirilgan data buzilishlarining o‘rtacha narxi 4,5 million dollarni tashkil qiladi.

Korxonalar ijtimoiy muhandislik va phishing hujumlaridan himoyalanish uchun xodimlarni muntazam ravishda o‘qitishlari va bu tahdidlarga qarshi kurashish strategiyalarini ishlab chiqishlari lozim. Shu bilan birga, ko‘p korxonalar hali ham bu borada yetarli darajada chora ko‘rmagan, bu esa ularning kiberxavfsizligini xavfostiga qo‘yadi. Moliyaviy firibgarlik ko‘pincha eng nozik hujum turi hisoblanadi, chunki u savdogarlarning moliyaviy aktivlarini o‘g‘irlashga qaratilgan. Eng oddiy stsenariyda tajovuzkor raqamli do‘konda ruxsatsiz xarid qilish uchun o‘g‘irlangan kredit karta ma’lumotlaridan foydalanadi. Haqiqiy karta egasi so‘ng to‘lovni qaytarish so‘rovini yuboradi, bu esa savdogarni sotishdan tushgan daromadni yo‘qotishiga olib keladi (jo‘natilgan mahsulotlardan tashqari).

Statista ma’lumotlariga ko‘ra, elektron tijorat korxonalari 2023-yilda onlayn to‘lovlarni firibgarlik tufayli 48 milliard dollar yo‘qotgan. 2024-yil oxiriga kelib bu ko‘rsatkich 55 milliard dollargacha oshishi kutilmoqda[5].

Onlayn to‘lovlarni qabul qiladigan har qanday biznes e-skimming (yokionlayn skimming) qurboni bo‘lishi mumkin va aftidan, elektron tijorat korxonalari bundan mustasno emas. Misol uchun, jionyatchilar mijozning kredit karta ma’lumotlarini qo‘lga kiritish va pulni o‘g‘irlash yoki ruxsatsiz xarid qilish uchun to‘lov kartalarini qayta ishlash yoki elektron tijorat saytlariga zararli skimming kodini kiritishi mumkin.

Onlayn skimming eng keng tarqalgan tahdid bo‘lmasa-da, uni e’tiborsiz qoldirmaslik kerak. Federal qidiruv byurosining ta’kidlashicha , skimming hujumlari iste’molchilar va moliyaviy tashkilotlarga yiliga 1 milliard dollardan ko‘proq zarar keltiradi.

Avtomatlashtirilgan zararli botlar elektron tijorat biznesiga zarar yetkazishi mumkin bo‘lgan yana bir tahdiddir. Buzg‘unchilar mijozlar hisoblarini egallash, kredit karta ma’lumotlarini o‘g‘irlash yoki savdogarning narxlari va tarkibini o‘chirish uchun elektron tijorat saytlariga botlarni kiritishlari mumkin (agar raqobatchi bot hujumini boshlagan bo‘lsa).

Afsuski, elektron tijorat sanoati bot hujumlari uchun birinchi raqamli maqsaddir. Imperva tomonidan e-tijorat 2022-yilgi xavfsizlik holati hisobotiga ko‘ra, elektron tijorat saytlariga qilingan barcha hujumlarning 62 foizi avtomatlashtirilgan skriptlar va botlardan foydalanishni nazarda tutadi, boshqa sohalarda esa 38 foiz.

Impervaning hisobotida ta’kidlanishicha, API trafiki elektron tijorat veb-saytlaridagi barcha trafikning qariyb 42 foizini tashkil qiladi. APIlarning 12 foizi muhim mijozlar ma’lumotlari (kredit karta raqamlari, hisob ma’lumotlari va boshqalar) bilan bog‘liq so‘nggi nuqtalarga ulanganligini hisobga olsak, korxonalarushbu kiber tahdidga alohida e’tibor qaratishlari kerak.

Birinchidan, korxonalar mavjud savdo infratuzilmasini uning kuchli va zaif tomonlarini aniqlash uchun baholashlari kerak. Ushbu ma’lumot savdogarga o‘zining noyob ehtiyojlari va talablariga moslashtirilgan yanada samarali kiberxavfsizlik strategiyasini ishlab chiqish imkonini beradi.

Bu korxonaga o‘z tizimlari va ilovalarini turli nuqtai nazardan tahlil qilishga yordam beradi:

Uskuna va dasturiy ta’minotning ishlashi;

Korporativ kiberxavfsizlik siyosati;

Xavfsizlik boshqaruvi va nazorati;

Tarmoq xavfsizligi va zaiflik muammolari.

Infratuzilma paydo bo‘ladigan tahdidlarga dosh berishga tayyorligini ta’minlash uchun yiliga kamida bir marta audit o‘tkazish tavsiya qilinadi. Bundan tashqari, korxonalar bu yerda kiberxavfsizlik bo‘yicha mutaxassislarni jalb qilishlari kerak; maslahatchilar tegishli soha tajribasiga ega bo‘lishi kerak, chunki elektron tijorat sanoati noyob elektron tijorat xavfsizligi tahdidlariga ega.

Rolga asoslangan kirishni boshqarish (RBAC) xavfsizlik modeli bo‘lib, u korporativ ma’lumotlar va resurslarga kirishni cheklash uchun foydalanuvchi rollarini taqsimlashni nazarda tutadi. Ushbu yondashuvda kirish darajasi pastroq bo‘lgan foydalanuvchilar (masalan, quyi darajadagi menejerlar yoki mijozlar) faqat ba’zi tizimlar va ma’lumotlarga kirish huquqiga ega. RBACni qabul qilishning asosiy maqsadi hujum yuzasini va muvaffaqiyatli hujumning mumkin bo‘lgan zararini kamaytirishdir. Xodimlar faqat ish uchun zarur bo‘lgan resurslarga ega bo‘lganligi sababli, ular muhim ma’lumotlarni tajovuzkorlar bilan baham ko‘ra olmaydi, bu esa ijtimoiy muhandislik xavflarini sezilarli darajada kamaytiradi.

Doimiy monitoring tizim xavfsizligini ta’minlashning kalitidir. Biroq, bu vazifa qo‘lda yondashuv bilan murakkab va samarasiz bo‘lishi mumkin. Yaxshiyamki, korxonalar sun’iy intellekt (AI) va mashinani o‘rganish (ML) kabi innovatsion texnologiyalar yordamida bu muammoni hal qilishlari mumkin. AI va MLga asoslangan tizimlar korporativ IT infratuzilmalari bilan bog‘liq trafik va ma’lumotlarni avtomatik ravishda tahlil qilishi mumkin. Shunday qilib, ular har qanday onlayn tahdidni, hatto real vaqt rejimida ham tezda aniqlashlari mumkin, buesa korporativ xavfsizlik bo‘yicha mutaxassislarga tezkor harakat qilishda yordam beradi va shu bilan yuzaga kelishi mumkin bo‘lgan zararni kamaytiradi.

Boshqa narsalar qatorida, savdogarlarga eng qimmatli ma’lumotlarni yo‘qotish yoki buzish holatlarida tezda tiklash uchun ularni zaxiralash tavsiyaqilinadi. Ko‘pgina ma’lumotlarni zaxiralash strategiyalari mavjud bo‘lsa-da, bulutlisaqlash rivojlangan moslashuvchanligi va mahalliy xostingga qaraganda arzonligi tufayli afzal variantga aylanishi mumkin.

Kiberjinoyatlar oqibatida keltirilgan iqtisodiy zararlar statistikasi:

2025-yilga kelib kiberjinoyatlar yetkazgan zararning umumiy qiymati 10.5 trillion dollarga yetishi kutilmoqda.

Har bir tashkilot o‘rtacha ma’lumotlar buzilishida $1.3 million yo‘qotadi.

Tashkilotning ma’lumotlar buzilishini aniqlash va kuchaytirishning o‘rtacha narxi 1,58 million dollarni tashkil qiladi.

2023-yilda ma’lumotlar buzilishining global o‘rtacha narxi 4.45 million dollarni tashkil etdi, bu uch yil ichida 15 foizga oshgan.

Ma’lumotlar buzilishining aholi jon boshiga o‘rtacha narxi 165 dollarni tashkil etadi, bu 2022-yildan bir dollarga yuqori.

To‘lov dasturini buzishning o‘rtacha umumiy qiymati 5.13 million dollarni tashkil etadi, bu 2022-yilga nisbatan 13 foizga yuqori.

2022-yilda AQShning kibersug‘urta mukofotlari 50 foizga oshib, sug‘urtachilar tomonidan yozilgan polislardan yig‘ilgan mukofotlar miqdori 7.2 milliard dollarga yetdi.

Sun’iy intellekt va avtomatlashtirish xavfsizligi vositalaridan keng foydalanadigan kompaniyalarda ma’lumotlar buzilishi bo‘lmagan kompaniyalarga qaraganda 108 marta tezroq sodir bo‘ladi.

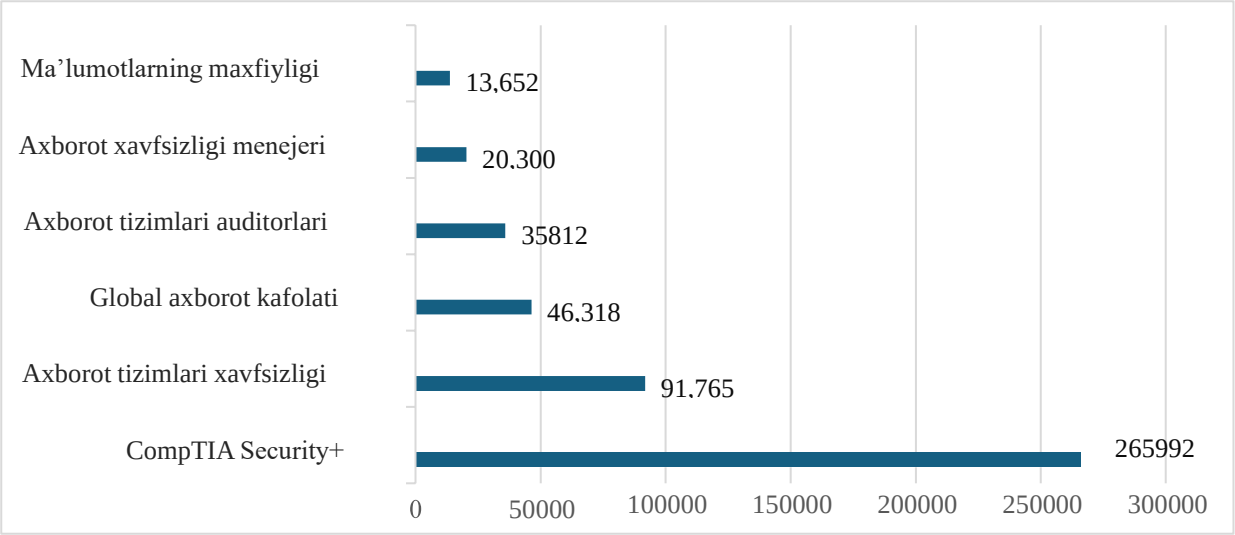
Ishonchsiz yondashuvga ega bo‘lgan tashkilotlar o‘rtacha qoidabuzarlik bo‘lmagan tashkilotlarga qaraganda 1.76 million dollarga arzonroq bo‘lgan.

Har yili shifoxonalar qoidabuzarlikdan keyingi ikki yil ichida reklama uchun64 foizga ko‘proq mablag‘ sarflaydi.

Fishing hujumning eng qimmat vektori bo‘lib, 2023-yilda har bir kompaniya uchun 4.9 million dollarga tushadi.

2023-yilda Qo‘shma Shtatlar ma’lumotlar buzilishining o‘rtacha umumiy qiymati eng yuqori bo‘lgan davlat bo‘lib, 9.48 million dollarni tashkil etadi. Yaqin Sharq 8,07 million dollar bilan ikkinchi o‘rinda.

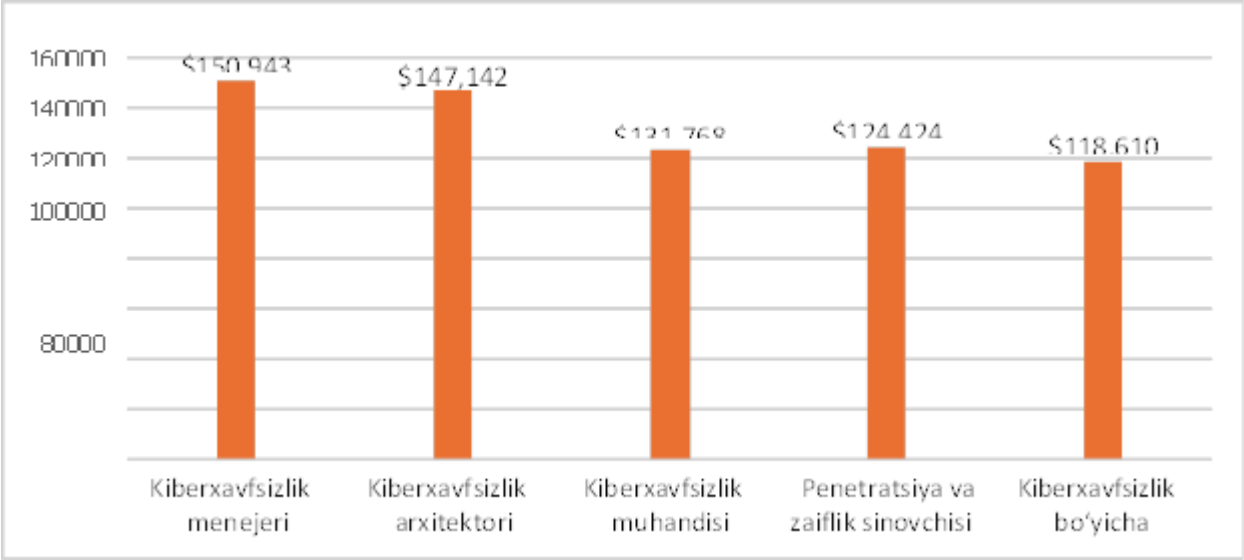
- 2022-yilda kiberxavfsizlik sanoatiga sarflangan mablag‘ 71.1 milliard dollarga yetdi, bu besh yil ichida ikki baravar oshdi.
- Yirik korxonalar kiberxavfsizlik uchun har yili to‘liq vaqtli xodim uchun taxminan 2700 dollar sarflaydi.
- Kichikroq kompaniyalarda (500 nafar yoki undan kam xodim) ma’lumotlar buzilishining o‘rtacha umumiy qiymati 2022-yildagi 2.92 million dollardan 2022-yilda 3,31 million dollargacha oshgan.
- Ma’lumotlarning buzilishi kompaniyalarning 57% uchun biznes takliflari narxining oshishiga olib keldi.
- Kanadada ma’lumotlar buzilishining o‘rtacha umumiy qiymati 9 foizga, 5.64 million dollardan 5.13 million dollargacha kamaydi(3-rasm).



3-rasm. 2024-yil yanvar holatiga ko‘ra eng ko‘p talab qilinadigan kiberxavfsizlik sertifikatlar[1]

2023-yilda ma’lumotlar buzilishi bo‘yicha tekshiruv hisobotida ta’kidlanishicha[7], tahdid qiluvchilarning 97 foizi moliyaviy motivatsiyaga ega(4-rasm).

4-rasm



4-rasm. 2024-yil yanvar oyi holatiga ko‘ra kiberxavfsizlik bo‘yicha eng ko‘p maosh oladigan ishlar [2]

Kiberxavfsizlik bo‘yicha ishlar va martaba istiqbollari: 2023-yilda kiberxavfsizlik bo‘yicha ishchi kuchi tafovuti 4 millionga yetdi. 2022-yilda axborot xavfsizligi

[1] https://csec.uz/uz/news/maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2023-yil-hisoboti/
[2] "O‘zbekiston Respublikasi kiberxavfsizligi - 2023 yil hisoboti" (csec.uz)

bo‘yicha tahlilchilarning o‘rtacha ish haqi 112000 dollarni yoki soatiga 53,85 dollarni tashkil etdi.

AQShda 2022-yil sentabrdan 2023-yil avgustigacha kiberxavfsizlik sohasida572 mingga yaqin ish o‘rni ochildi, bu 2010-yilga nisbatan 74 foizga ko‘pdir.

2022-yil sentabrdan 2023-yil avgustigacha AQShda taxminan 1.18 million kiberxavfsizlik mutaxassisi ishlagan, bu 2010-yildan buyon 59 foizga o‘sgan.

Kiberhujumlardan himoya qilish va ularning elektron tijoratga ta’sirini minimallashtirish uchun kompaniyalar kiberxavfsizlikka sarmoya kiritishlari, xodimlarni xavfsizlik qoidalariga o‘rgatishlari, ma’lumotlarni shifrlashdan foydalanishlari, dasturiy ta’minotni muntazam yangilab turishlari va onlayn muhitda yangi tahdidlarni kuzatishlari kerak.

XULOSA VA TAVSIYALAR

Maqolada elektron tijoratning rivojlanishi va bu sohadagi kiberxavfsizlik tahdidlari chuqur tahlil qilindi. Maqolaning asosiy maqsadi O‘zbekiston sharoitida elektron tijorat platformalarining kiberxavfsizlik darajasini aniqlash, mavjud xavfsizlik choralarining samaradorligini baholash va kiberxavfsizlikni mustahkamlash bo‘yicha tavsiyalar berish edi. Elektron tijoratda kiberxavfsizlik tushunchasi, uning asosiy xususiyatlari va tahdidlar tahlil qilindi. Kiberhujumlarning turli shakllari, ularning elektron tijoratga ta’siri va xalqaro tajribalar misolida muhim xulosalar chiqarildi. Aholining kiberxavfsizlik madaniyatini oshirish, xavfsizlik choralarini kuchaytirish zaruriyati ta’kidlandi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Shaislamova, M., & Kamoliddinov, A. (2023). **Elektron tijoratni rivojlantirishning xorijiy tajribasi**. Interpretation and Researches, 1(7). Извлечено от https://interpretationandresearches.uz/index.php/iar/article/view/223

2. Shaislamova, M., & Kamoliddinov, A. (2023). **ELEKTRON TIJORATNI RIVOJLANTIRISHNING XORIJIY TAJRIBASI**. Interpretation and researches, 1(7).

3. Шаисламова, М. Р., & Ибрагимова, С. А. (2013). **Повышение конкурентоспособности предприятия в условиях глобализации**.

4. Shaislamova, M. R. (2019). **Human Capital Enhancement**. ББК 65 М 34, 378.

5. Shaislamova, M. (2021). **Organization of innovative activities in telecommunications enterprises**. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), 1434-1440.