



ELEKTRON TIJORATDA XAVFSIZLIK MASALALARI

Akbar Qurbonov¹

¹Denov tadbirkorlik va pedagogika institut
“Raqamli iqtisodiyot” kafedrası
O’qituvchi

Ziyodullo Bahodirov²

²Denov tadbirkorlik va pedagogika institut
“Bugalteriya hisobi va audit” yo’nalishi
talabasi

<https://doi.org/10.5281/zenodo.7181387>

Annotatsiya

Bugungi kunda rivojlanib kelayotgan eng zamonaviy soxalardan biri elektron tijoratdir. E-commerce internet orqali savdo-sotiq va xizmat ko’rsatish amaliyotlarini tashkil etishdir. Dunyoning savdo aylanmasini bir muncha qismini elektron tijorat tashkil etadi.

O’zbekiston Respublikasida amalga oshirilayotgan ishlar jumladan O’zbekiston Respublikasida “Elektron tijorat” rivojlanishida yuzaga keladigan bir qancha muammolar ya’ni “Online muhitda xavfsizlik masalalari” haqida yechimlar, O’zbekiston Respublikasi raqamlashtirish asriga ishonch bilan qadam qo’ydi va bunga hukumat tomonidan qaratilayotgan e’tibor asos bo’ladi. Doimiy tarzda amalga oshirilayotgan internet tezligi va sifatini oshirish, zamonaviy AKT qurilmalarini takomillashtirish bilan birgalikda, kiberxavfsizlik sohasiga ham e’tibor qaratmoqda. Rivojlanib kelayotgan mamlakatimizda ayni shu masalani yoritish yuzasidan yechimlar taklif etilgan.

Kalit so’zlar : tranzaksiya, WTO, PayPal, kiberjinoyat, Phishing, Trojan, PaySafe, FBI, Kiberxavfsizlik

Elektron tijoratning ahamiyati ortib bormoqda. Elektron tijoratning afzalliklari biznesmenlar uchun geografik jihatdan to’siqlar yo’qliligi, haridorlar uchun mahsulotlarga buyurtma berishda vaqtdan yutishidir. Ilk marotaba elektrton tijorat AQSHda 1960-yillarda qo’llanadi. American Airlines aviakompaniyasi avia parvozlar uchun joylarni band qilishning avtomatlashgan tizimini, yarim avtomatik biznes tadqiqot muhitini yaratdi.

Internetda ma’lumot o’g’irlash oson emas, lekin ma’lumotni shaxsan o’g’irlashdan ko’ra oson va tezroqdir. Internet odamlarni uzoqdan va deyarli yashirin ravishda talan-taroj qilish imkonini beradi. Internetda yashirin bo’lish online haridorlar va xakkerlarga buyurtmalarni birdek berishga imkon beradi va malumotlarni elektrton pochta orqali qo’lga kiritib o’g’irlash, yoki oddiygina





dasturiy ta'minot viruslari va xakkerlar hujumi yordamida elektron tijorat saytlarini o'chirib qo'yishlari mumkin.

Internet ochiq va juda zaif tarmoqdir. Internetgacha bo'lgan tarmoqlar ichida internet eng zaif tarmoq deb tan olinadi.

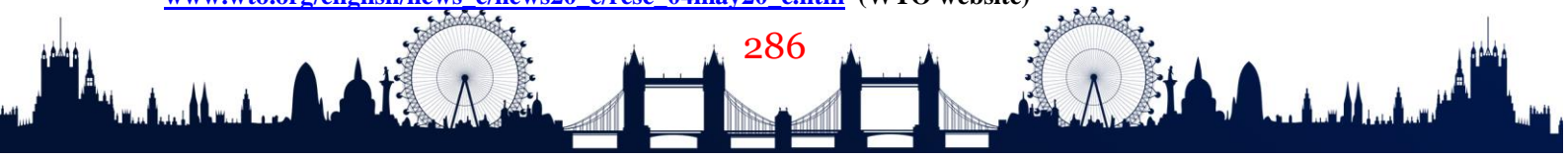
Elektron tijoratda Internet xavfsizligi juda muhim katigoriya hisoblanadi. Ponemon universiteti tadqiqotchilari 2016-yil AQSH korporatsiyalari o'rtasida ma'lumotlarni buzishga qancha mablag' sarflanganini hisoblashdi. Bu 4 millon dollarni tashkil etadi^[1]. Kiberjinoyat biznes tashkilotlar va xaridorlar uchun muhim muammo bo'lib kelyapti. Bot tarmoqlar, DDoS hujumlar, Troyan, Ransomware, Data theft kiber jinoyat turlari bugungi kunda keng tarqalgan. Kiber hujumlar ogirlashib, xavfli tus olib, xususiy va davlat sektorini bir xilda nishonga olmoqda

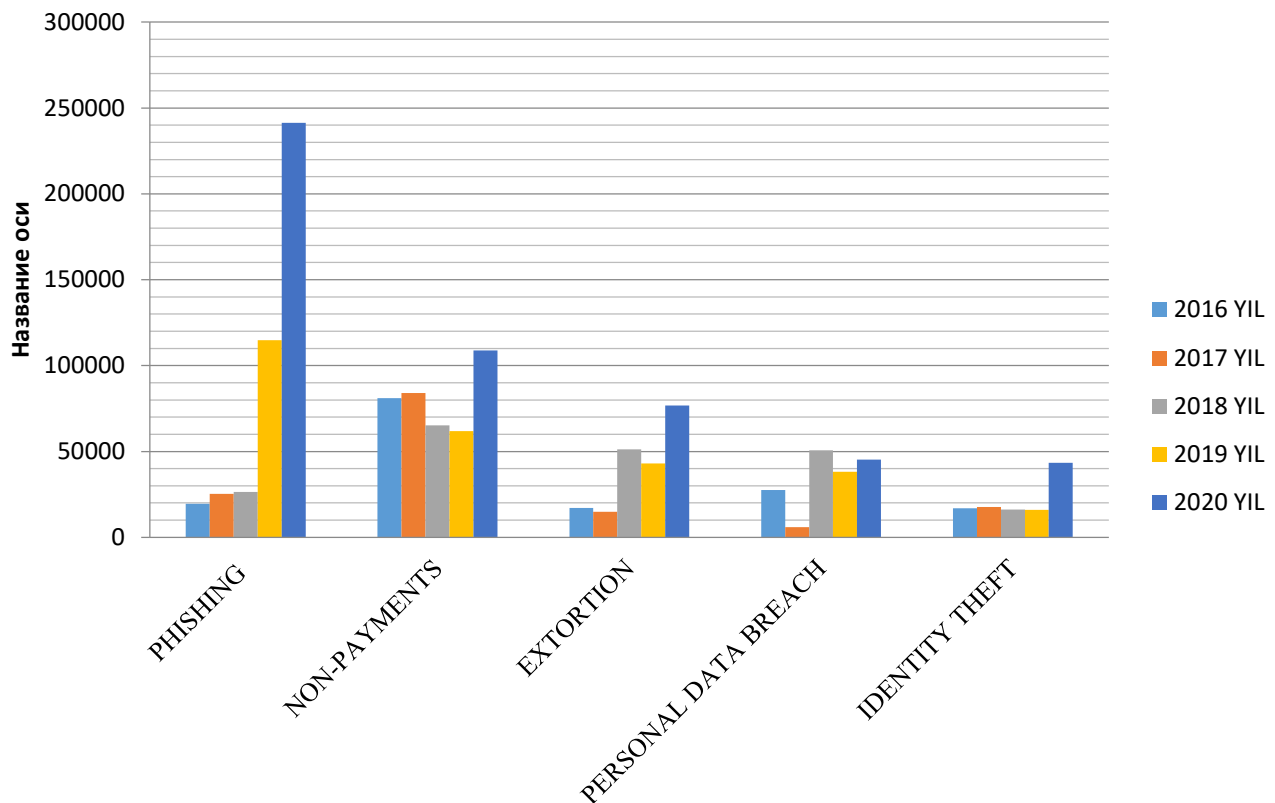
Kiber jinoyat global maydonda eng tez o'sib borayotgan jinoyat turi sanaladi. COVID-19 pandemiyasi kiber tahdidlarning yanada ko'payishiga zamin yaratdi. AQSH federal qidituv byurosi ma'lumotlariga ko'ra, global pandemiya davrida kiber jinoyatlar soni 400 %ga oshgan^[2]. Jahon savdo tashkiloti (World Trade Organization) kotibiyati COVID-19 pandemiyasining elektron tijoratga, shu jumladan transchegaraviy savdoga qanday ta'sir qilgani haqida yangi ma'lumotlarni e'lon qildi. Istemolchilar blakirovka va ijtimoiy masofani cheklash choralariga moslashib borayotganliklari sababli elektron tijorattan foydalanishning ko'payishi va va bir necha muammolarga, masalan, mamlakatlar aro, mamlakat ichida raqamli tengsizlik va kiber jinoyotlarni kelib chiqishini oldini olishga qaratilgan choralarni kuchaytirish kerakligini qayd etgan^[3].

¹ "E-commerce" 2017 Kenneth C.Laudon, Carol Guercio Traver

² www.fbi.gov/news/pressel/press-releases

³ www.wto.org/english/news_e/news20_e/rese_04may20_e.htm (WTO website)





IC3 Complaint statistikasi

Kiber Jinoyatchilik turlarini taqqoslash bo'yicha statistika so'ngi besh yillik natijalar^[4]

O'zbekiston Respublikasida elektron tijorat dastlab 2004-yilda "Elektron tijorat to'grisida" gi qonuni O'zbekiston Respublikasi Birinchi Prizidenti I.A.Karimov tomonidan qabul qilingan.Yangi tahrirdagi qonunlarda Xavfsizlik masalalari haqida ham yoritilgan. "To'lovlar va to'lov tizimlari to'grisida" O'zbekiston Respublikasi qonuni 11-bob 53-moddasi xavfsizlik masalalarini qonuniylashtirilgan[5]. Bugungi kunda O'zbekistonda kiberxavfsizlik masalalari bo'yicha "Kiberxavfsizlik markazi" DUK ish faoliyatini olib bormoqda. Ma'lumki ushbu tashkilot "Axborot xavfsizligini ta'minlash markazi" davlat muassasasi nomi bilan O'zbekiston Respublikasi Prizidentining "O'zbekiston Respublikasining Milliy axborot-kommunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to'g'risida"gi PQ-1989-son qarori bilan 2013-yil 27-iyunda tashkil topib, bugungi kunda O'zbekiston Respublikasi

⁴ IC3 Complaint Statistics "Internet crime Report" 2020

⁵ <https://lex.uz/docs/-4575786>





Prizidentning “O‘zbekiston Respublikasining Milliy axborot-kommunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to‘g‘risida”gi 2018-yil 21-noyabrdagi PQ-4024-son qaroriga muvofiq “Kiberxavfsizlik markazi” sifatida ish faoliyatini olib bormoqda.

Markazning asosiy vazifalari quyidagilardan iborat:

Axborot xavfsizligiga hozirgi vaqtdagi tahdidlar to‘g‘risidagi ma‘lumotlarni yig‘ish, tahlil qilish va to‘plash, davlat organlari va tashkilotlari axborot tizimlari, resurslari va ma‘lumotlar bazalariga noqonuniy kirib olish holatlarining oldini olishni ta‘minlaydigan samarali tashkiliy va dasturiy-texnik yechimlarni tezkor qabul qilish bo‘yicha tavsiyalar va takliflar ishlab chiqish;

Qonun buzuvchilarni, axborotlar makonidagi ruxsatsiz yoxud buzuvchi harakatlarni amalga oshirishda foydalaniladigan metodlar va vositalarni tahlil qilish, identifikatsiyalashda telekommunikatsiyalar tarmoqlarining operatorlari va provayderlari, huquqni muhofaza qilish organlari bilan hamkorlik qilish;

Axborotlashtirish obyektlarida (davlat sirlari bundan mustasno) apparat vositalari va dasturiy mahsulotlarni, axborot-kommunikatsiya texnologiyalari, telekommunikatsiya jihozlari va boshqa texnik vositalarni attestatsiya, ekspertiza va sertifikatdan o‘tkazish;

Davlat organlari va tashkilotlari axborot tizimlari va resurslari axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishda ko‘maklashish;

Davlat axborot tizimlari va resurslari, shuningdek, Internet tarmog‘i milliy segmentining axborot xavfsizligini ta‘minlash sohasidagi normativ-huquqiy bazani takomillashtirish bo‘yicha takliflar ishlab chiqish;

Internetning milliy foydalanuvchilarini Internet tarmog‘i milliy segmentida axborot xavfsizligiga paydo bo‘layotgan tahdidlar to‘g‘risida o‘z vaqtida xabardor qilish, shuningdek, axborotlarni himoya qilish bo‘yicha maslahat xizmatlari ko‘rsatish.

Bu tashkilot asosan hukumat saytlarini ekspirtiza qiladi ularga hizmat ko‘rsatadi, 2021-yilda davlat organlari veb-saytlarini tekshiruvdan o‘tkazish jadvali 1-choragiga ko‘ra top 10 ta kiber xavfsizlik taminlangan tashkilotlar jadvali





No	Tashkilot nomi	berilgan ball			
1	O'zbekiston Respublikasi Markaziy banki	96,6			
2	O'zbekiston Respublikasi adliya vazirligi	95,9			
3	Namangan viloyat hokimligi	91,3			
4	O'zbekiston Respublikasi bojxona qomitasi	89			
5	"O'z sanoat qurilish materiallari" uyushmasi	89			
6	ATIB "IpotekaBank"	88,5			
7	Farg'ona viloyati Hokimligi	87,1			
8	Novoiy konmetallurgiya	85			
9	O'z.Res Davlat soliq qo'mitasi kadast agent	82,9			

2-jadval 2021-yil 1-chorak holati

Ushbu jadvaldan ko'rinadiki elektron tijoratda xususiy korxonalar qayd etilmadan bundan xulosa qilib aytganda O'zbekistonda faoliyat yuritadigan xususiy korxonalar kiberxavfsizligi qoniqarli darajada emas bu esa elektron tijoratda xavfsizlik masalasi yaxshi emasligini anglatadi.

Taklifim shundan iboratki "Kiberxavfsizlik markazi" DUK kabi xususiy korxonalar tashkil etish

Ya'ni ushbu korxonalar to'lov tizimlari, elektron tijorat saytlari xavfsizligini ta'minlash uchun xizmat qilishi ;

Jahon tajribasida bunga misol Paysafe Holdings UK Limited misol bo'la oladi. Bu korxonalar Skrill Limited 2011-yilgi elektron pul va to'lov vositalarini chiqarish uchun "Elektron pul qoidalari" ga muvofiq moliyaviy hatti-harakatlar bo'yicha vakolatli organ tomonidan vakolatga ega.

Kiberhujumlarni oldini olish uchun milliy domenni doimiy tekshiruvlarni amalga oshirish;

Elektron tijorat xavfsizligi bilan shug'ullanuvchi tashkilotlarga bir qator maslahatlar:

1. Doimiy ravishda dasturiy taminotni yangilash, xususiy korxonalar dasturiy taminotidagi kamchiliklarni bartaraf etish va bu haqida foydalanuvchilarni ogohlantirish.
2. Dasturiy ta'minotni yoki xavfsizlik vositalarini avtomatik yangilash tizimini joriy etish

Foydalanuvchilarga maslahat:

1. Doimiy ravishda to'lov tizimlaridan kelgan smslarni nazorat qiling
 2. Qurilmangizdagi "Mening qurilmamni top" funktsiyasini doimiy yoqib qo'yish
- Agar siz mobil qurilmangizni o'g'irlatsangiz yoki yo'qotsangiz ma'lumotlaringizni masofadan tozalab tashlash yoki bloklashga yordam beradi.

Foydalanilgan adabiyotlar:

1. "E-commerce" 2017 Kenneth C.Laudon, Carol Guercio Traver





2. www.wto.org/english
3. <https://lex.uz>
4. www.fbi.gov/news/pressel/press-releases
5. IC3 Complaint Statistics “Internet crime Report” 2020
6. O‘zbekiston Respublika Kiberxavfsizlik markazi hisoboti 2021-yil 14-aprel
7. O‘zbekiston Respublika Kiberxavfsizlik markazi hisoboti 2020-yil

