VIRTUAL OLAMDA IJTIMOIY MUHANDISLIK ORQALI SODIR ETILADIGAN HUQUQBUZARLIKLARNI OLDINI OLISH CHORALARI

Isaqov Abror Faxriddinovich
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i o‘rinbosari
aisaqov921@gmail.com
Yusupov Djavohir O‘tkirovich
Ichki ishlar vazirligi Akademiyasi kursanti
javohiry721@gmail.com

Annotation

This article analyzes the issue of measures to prevent crimes committed through social engineering in the virtual world from the perspective of international experience and legislative documents of the Republic of Uzbekistan. The main types of social engineering - phishing, fake profiles, malware and vishing - are examined in detail, and their distribution trends in Uzbekistan and the world are illustrated with examples. The article studies successful cybersecurity strategies of countries such as the USA, the European Union, and Singapore, and discusses their adaptability to local conditions.

Key words: Social engineering, Phishing, Pretexting, Deepfake, Quid pro quo, Cybersecurity, Networks

Аннотация

В данной статье анализируется вопрос мер по предотвращению преступлений, совершаемых посредством социальной инженерии в виртуальном мире, с точки зрения международного опыта и законодательства Республики Узбекистан. Подробно рассмотрены основные виды социальной инженерии – такие методы, как фишинг, фейковые профили, вредоносные программы и вишинг, а также на примерах описаны тенденции их распространения в Узбекистане и мире. В статье рассматриваются успешные стратегии кибербезопасности таких стран, как США, Европейский Союз и Сингапур, и обсуждается их адаптируемость к местным условиям.

Ключевые слова: Социальная инженерия, Фишинг, Претекстинг, Дипфейк, Услуга за услугу, Кибербезопасность, Сети

Annotatsiya

Ushbu maqola virtual olamda ijtimoiy muhandislik (social engineering) orqali sodir etiladigan huquqbuzarliklarni oldini olish choralari masalasini xalqaro tajriba va O‘zbekiston Respublikasining qonunchilik hujjatlari nuqtai nazaridan tahlil qiladi. Ijtimoiy muhandislikning asosiy turlari — phishing, soxta profillar, zararli dasturlar va vishing kabi usullar batafsil ko‘rib chiqilib, ularning O‘zbekistonda va dunyoda

tarqalish tendensiyalari misollar bilan tasvirlanadi. Maqolada AQSh, Yevropa Ittifoqi, Singapur kabi davlatlarning kiberxavfsizlik sohasidagi muvaffaqiyatli strategiyalari o‘rganilib, ularning mahalliy sharoitlarga moslashuvchanligi muhokama qilinadi.

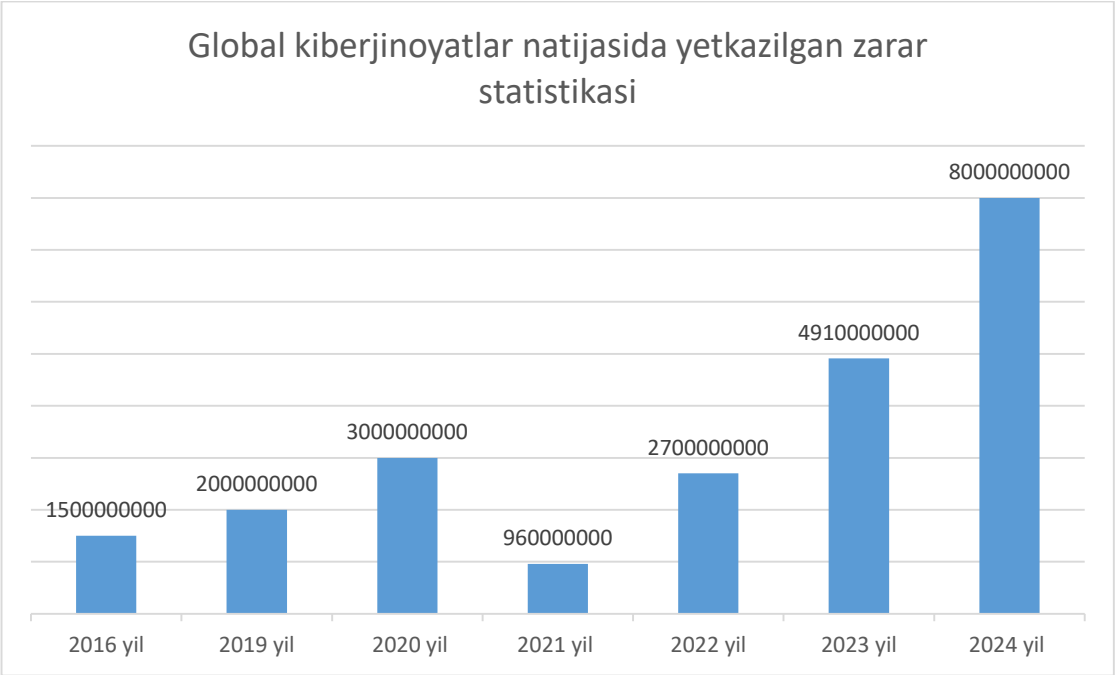
Kalit so‘zlar: Ijtimoiy muhandislik, fishing, pretexting, Deepfake, Quid pro quo, Kiberxavfsizlik, Tarmoqlar

Zamonaviy dunyoda internetning keng tarqalishi insoniyat uchun ulkan imkoniyatlar ochdi. 2025-yilga kelib, dunyoda internet foydalanuvchilarining soni 5,5 milliarddan oshdi (Statista, 2025), O‘zbekistonda esa bu ko‘rsatkich 28 milliondan ortiqni tashkil etdi (O‘zbekiston Respublikasi Raqamli Texnologiyalar Vazirligi, 2025). Biroq, raqamli makonning rivojlanishi bilan kiberjinoyatlar, xususan ijtimoiy muhandislik (social engineering) orqali sodir etiladigan huquqbuzarliklar ham ko‘payib bormoqda. Ijtimoiy muhandislik odamlarning psixologik zaifliklaridan foydalanib, ularni aldash, shaxsiy ma’lumotlarni olish yoki noqonuniy harakatlarga undashga qaratilgan usul sifatida ta’riflanadi. Bu xavf nafaqat shaxsiy foydalanuvchilarga, balki tashkilotlar va davlatlar darajasida ham jiddiy tahdid solmoqda. Masalan, 2024-yilda AQShda ijtimoiy muhandislik hujumlari natijasida korxonalar 2,7 milliard dollar zarar ko‘rgan (FBI Internet Crime Report, 2024). Yevropa Ittifoqida phishing hujumlari soni 2023-yildan 2025-yilgacha 35% ga oshgan (Europol, 2025). O‘zbekistonda ham Telegram va Instagram kabi platformalarda soxta “ish takliflari” yoki “lotereya yutug‘i” shaklidagi aldov holatlari ko‘paymoqda, ammo bu borada aniq statistika hali to‘liq shakllanmagan. Ushbu maqola virtual olamdagi ijtimoiy muhandislik huquqbuzarliklarining oldini olish choralari, xalqaro tajribalar va O‘zbekiston Respublikasining amaldagi qonunchilik hujjatlari asosida tahlil qiladi. Maqsad — global miqyosda sinovdan o‘tgan strategiyalarni mahalliy sharoitlarga moslashtirish va samarali yechimlar taklif etishdir.

Ijtimoiy muhandislik – bu odamlarning psixologik zaifliklaridan foydalanish orqali ulardan ma’lumot olish yoki ularni ma’lum bir harakatga undash san’ati bo‘lib, virtual olamda uning ko‘rinishlari ancha murakkab va xilma-xil tusga kirgan. Internetning keng tarqalishi, ijtimoiy tarmoqlarning ommalashuvi va sun’iy intellekt texnologiyalarining rivojlanishi bilan ijtimoiy muhandislik yangi darajaga ko‘tarildi. Virtual olamda bu jarayon nafaqat shaxsiy ma’lumotlarni o‘g‘irlash, balki kengroq miqyosda – siyosiy manipulyatsiya, iqtisodiy zararni keltirish va hatto global xavfsizlikka tahdid solish uchun ham qo‘llanilmoqda. Virtual olamda ijtimoiy muhandislikning eng keng tarqalgan usullaridan biri – **“fishing” (phishing)** hujumlari. Bu usulda tajovuzkorlar foydalanuvchilarga ishonchli manba (masalan, bank, davlat idorasi yoki mashhur kompaniya) nomidan soxta xabarlar yuboradi. Xabarda odatda shoshilinch muammo haqida ogohlantiriladi: “Hisobingiz bloklandi, darhol

ma’lumotlarni yangilang!” yoki “Sizga katta yutuq kelib tushdi, havolaga kiring!” kabi iboralar ishlatiladi. Masalan, 2023-yilda PayPal foydalanuvchilariga yuborilgan soxta xatlar orqali minglab odamlarning hisob ma’lumotlari o‘g‘irlangani xabar qilingan edi. Bunday hujumlarning muvaffaqiyati foydalanuvchilarning shoshilinchlik hissi va e’tiborsizligiga bog‘liq. Yana bir keng tarqalgan usul – **“pretexting” (bahona yaratish)**. Bu yerda tajovuzkor foydalanuvchi bilan ishonchli munosabat o‘rnatish uchun o‘zini boshqa shaxs sifatida ko‘rsatadi. Masalan, IT-xodim sifatida qo‘ng‘iroq qilib, “Tizimni yangilash uchun parolingizni ayting” deb so‘rashi mumkin. Virtual olamda bu usul ko‘pincha ijtimoiy tarmoqlar orqali amalga oshiriladi: soxta profil yaratib, odamning do‘sti yoki hamkasbi sifatida murojaat qilinadi. Ijtimoiy tarmoqlar ijtimoiy muhandislik uchun eng qulay platformalardan biridir. Facebook, Instagram, Twitter (X) va LinkedIn kabi tarmoqlarda foydalanuvchilar o‘z hayotlari haqida ko‘p ma’lumotlar – tug‘ilgan sanasi, ish joyi, oila a’zolari, sayohatlari haqida postlar joylashtiradi. Tajovuzkorlar ushbu ma’lumotlarni tahlil qilib, shaxsga moslashtirilgan hujumlarni rejalashtiradi. Masalan, agar bir foydalanuvchi yaqinda sayohatdan qaytganini yozsa, tajovuzkor undan “aeroportdagi yo‘qotilgan yukingiz topildi, ma’lumotlaringizni shu havolada tasdiqlang” degan xabar yuborishi mumkin. Bu usulning samaradorligi shundaki, u foydalanuvchining shaxsiy tajribasiga moslashtirilgan. Bundan tashqari, ijtimoiy tarmoqlarda **“klonlash”** deb ataladigan usul ham mashhur. Bu yerda tajovuzkor mavjud foydalanuvchining profilini nusxalaydi va uning do‘stlariga xabar yuborib, yordam so‘raydi: “Pulim tugab qoldi, zudlik bilan 100 dollar yuboring”. Ko‘pincha odamlar bunday xabarni do‘stidan kelgan deb o‘ylab, shubhalanmasdan pul o‘tkazadi. Sun’iy intellektning rivojlanishi ijtimoiy muhandislikni yanada xavfli darajaga olib chiqdi. **“Deepfake”** texnologiyasi yordamida tajovuzkorlar real odamlarning ovozini yoki tasvirini soxtalashtirib, ishonchli manipulyatsiyalar qilmoqda. Masalan, 2022-yilda bir kompaniya bosh direktori sifatida soxta video qo‘ng‘iroq orqali xodimlardan katta miqdorda pul o‘tkazish so‘ralgan holat qayd etilgan. Deepfake’lar nafaqat shaxsiy darajada, balki jamoatchilik fikrini manipulyatsiya qilish uchun ham ishlatilmoqda – masalan, soxta siyosiy bayonotlar tarqatish orqali. Yana bir tendensiya – **“smishing” (SMS orqali fishing)** va **“vishing” (ovozli fishing)** kabi usullarning ko‘payishi. Smishingda foydalanuvchilarga SMS orqali zararli havolalar yuboriladi, vishingda esa avtomatlashtirilgan qo‘ng‘iroqlar orqali ma’lumot so‘raladi. Masalan, “Soliq idorasidanmiz, qarzingizni tekshirish uchun shu raqamga javob bering” degan qo‘ng‘iroqlar ko‘p odamlarni aldagan. Bu usullarning oqibatlari shaxsiy darajadan tortib global miqyosgacha bo‘lishi mumkin. Shaxsiy darajada odamlar moliyaviy yo‘qotishlarga duch keladi, kompaniyalar esa maxfiy ma’lumotlarining oshkor bo‘lishi tufayli katta zarar ko‘radi. Masalan, 2021-yilda bir xalqaro korporatsiya ijtimoiy muhandislik hujumi tufayli 60 million dollardan ortiq yo‘qotgan. Global miqyosda esa

bunday hujumlar saylovlarga aralashish, dezinformatsiya tarqatish va kiber-urushlarning bir qismi sifatida qo‘llanilmoqda. “**Quid pro quo”** usulida tajovuzkorlar foydalanuvchilarga biror xizmat yoki yordam evaziga ma'lumotlarini taqdim etishni taklif qiladilar. Masalan, texnik yordam taklif qilib, buning evaziga foydalanuvchidan tizimga kirish ma'lumotlarini so'rash odatiy holat. Bu usul ko'pincha kichik bizneslar yoki shaxsiy foydalanuvchilarga qarshi qo'llaniladi, chunki ular ko'pincha yordamga muhtoj bo'lishadi.



Ijtimoiy muhandislik huquqbuzarliklari shaxslar va tashkilotlar uchun katta xavf tug'diradi. Shaxslar moliyaviy yo‘qotishlar, shaxsiy ma’lumotlarning o‘g‘irlanishi va shaxsiy hayotining buzilishi kabi oqibatlarga duch keladi. Tashkilotlar uchun esa mijozlar ma’lumotlarining yo'qolishi, obro'ning tushishi va huquqiy javobgarlik xavfi mavjud. Ushbu huquqbuzarliklarning barchasi inson psixologiyasiga asoslangan bo'lib, foydalanuvchilarning ishonchini suiiste’mol qilish orqali amalga oshiriladi. Shuning uchun, texnik choralardan tashqari, huquqiy va ta'lim choralari ham muhim ahamiyatga ega. Misol uchun, 2016-yilda Bangladesh Bankiga qaratilgan hujumda ijtimoiy muhandislik orqali 1 milliard AQSh dollari miqdorida mablag‘ o‘g‘irlashga urinish bo‘lgan, bu esa ushbu muammoning global miqyosda qanchalik jiddiy ekanligini ko'rsatadi (Reuters, 2016).

2019-yilda qabul qilingan **“Shaxsiy ma'lumotlar to‘g‘risida”gi qonun** shaxsiy ma’lumotlarni himoya qilishning huquqiy asoslarini belgilaydi (O'zbekiston Respublikasi qonuni, 2019). Ushbu qonunga ko‘ra, shaxsiy ma’lumotlar faqat shaxsning roziligi bilan to‘planishi, saqlanishi va qayta ishlanishi mumkin. Qonunda

shaxsiy ma’lumotlarni himoya qilish mexanizmlari, jumladan, ma’lumotlarni himoya qilish bo‘yicha huquqiy, tashkiliy va texnik choralar ko‘rish talablari belgilangan. Ushbu qonun ijtimoiy muhandislik hujumlari orqali shaxsiy ma’lumotlarni o‘g‘irlashga qarshi kurashishda muhim ahamiyatga ega. Masalan, agar tashkilot shaxsiy ma’lumotlarni himoya qilish bo‘yicha choralar ko‘rmasa, huquqiy javobgarlikka tortiladi.

Ammo qonunda ijtimoiy muhandislikning o‘ziga xos xususiyatlari, masalan, phishing yoki pretexting kabi taktikalar aniq ko'rsatilmagan. Bu esa qonunning samaradorligini cheklaydi. Misol uchun, agar foydalanuvchi phishing hujumi orqali o'z ma'lumotlarini oshkor qilsa, tashkilotning javobgarligi aniq belgilanmagan. Shu sababli, qonunchilikni yanada aniqroq qilish va ijtimoiy muhandislikka qarshi maxsus choralarni kiritish zarur.

O'zbekiston Respublikasining **Jinoyat kodeksi**da kiberjinoyatlarga qarshi kurashishga qaratilgan bir qator moddalar mavjud (O'zbekiston Respublikasi Jinoyat kodeksi, 1994):

- **278^3-modda**: Kompyuter tizimlariga ruxsatsiz kirish – bu moddada kompyuter tizimlariga ruxsatsiz kirish uchun jarima yoki 2 yilgacha axloq tuzatish ishlari jazosi belgilanadi;
- **278^4-modda**: Kompyuter malumotlarini o‘g‘irlash – bu moddada ma'lumotlarni o'g'irlash uchun 2 yilgacha ozodlikdan mahrum qilish nazarda tutilgan;
- **278^6-modda**: Zararli dasturlarni tarqatish – bu moddada zararli dasturlarni yaratish yoki tarqatish uchun 2 yilgacha ozodlikdan mahrum qilish jazosi mavjud.

Ushbu moddalarda kiberjinoyatlar uchun jazo choralari belgilangan bo‘lib, ular umumiy ma’noda ijtimoiy muhandislik hujumlarini ham qamrab olishi mumkin. Biroq, ushbu moddalarda ijtimoiy muhandislik taktikalariga alohida e’tibor qaratilmagan. Masalan, phishing orqali ma’lumot o‘g‘irlash texnik jihatdan “ruxsatsiz kirish” sifatida baholanishi mumkin bo'lsa-da, bu jarayonda inson omili asosiy rol o'ynaydi, lekin qonunda bu aniq aks ettirilmagan. Shuning uchun, qonunchilikni yanada takomillashtirish va ijtimoiy muhandislikning o'ziga xos xususiyatlarini hisobga olgan holda yangi normalarni kiritish zarur.

“Axborot xavfsizligi to'g'risida”gi qonun axborot tizimlarini himoya qilish, axborot xavfsizligini ta’minlash va kiberhujumlarga qarshi kurashishga qaratilgan (O’zbekiston Respublikasi qonuni, 2003). Ushbu qonunda axborot tizimlarini himoya qilish bo‘yicha davlat siyosati, axborot xavfsizligini ta’minlash choralari va javobgarlik choralari belgilangan. Masalan, qonunga ko'ra, davlat organlari va tashkilotlar axborot tizimlarining xavfsizligini ta’minlash uchun choralar ko'rishlari shart. Ushbu qonun kiberxavfsizlik sohasida umumiy asoslarni yaratadi va davlat organlarining mas’uliyatini belgilaydi.

Biroq, ijtimoiy muhandislik hujumlari ko‘pincha texnik zaifliklardan ko‘ra inson omiliga asoslanganligi sababli, ushbu qonunda ham ijtimoiy muhandislikka qarshi maxsus choralar yetarli emas. Masalan, foydalanuvchilarni o‘qitish yoki phishing hujumlarini aniqlash bo’yicha talablar qonunda aniq ko‘rsatilmagan. Shu sababli, qonunchilikni inson omilini hisobga olgan holda yanada takomillashtirish zarur.

O‘zbekiston qonunchiligida ijtimoiy muhandislik huquqbuzarliklariga qarshi kurashish uchun umumiy asoslar mavjud bo‘lsa-da, quyidagi bo‘shliqlar mavjud:

- Ijtimoiy muhandislikning aniq ta’rifi va turlari qonunda ko‘rsatilmagan, bu esa huquqiy choralar qo‘llashda qiyinchiliklar tug‘diradi;
- Tashkilotlar va shaxslar uchun ijtimoiy muhandislikka qarshi maxsus profilaktika choralari talab qilinmagan, bu esa oldini olish ishlarini qiyinlashtiradi;
- Huquq-tartibot organlarining ijtimoiy muhandislik hujumlarini tergov qilish bo‘yicha maxsus tajribasi yetarli emas, bu esa jinoyatchilarni jazolashni qiyinlashtiradi.

Ushbu bo‘shliqlarni bartaraf etish uchun qonunchilikni xalqaro tajribaga moslashtirish va zamonaviy kiberxavfsizlik standartlariga mos yangilash zarur. Xalqaro tajribadan foydalanish orqali O'zbekiston qonunchiligi yanada samarali bo'lishi mumkin.

Xalqaro tajribada ijtimoiy muhandislik huquqbuzarliklariga qarshi kurashish uchun bir qator samarali huquqiy, texnik va ta'lim choralari qo‘llanilmoqda. Ushbu tajribalarni O'zbekiston qonunchiligi va amaliyotiga tatbiq etish orqali huquqbuzarliklarni oldini olish samaradorligini oshirish mumkin. Quyida bir nechta davlat tajribasi tahlil qilinadi.

Estoniya tajribasi

Estoniya kiberxavfsizlik sohasida dunyoda yetakchi davlatlardan biri sifatida tan olingan. Estoniyaning **“Kiberxavfsizlik to‘g‘risida”gi qonuni** muhim infratuzilmani himoya qilish, davlat va xususiy sektor o‘rtasida hamkorlikni kuchaytirish va kiberhujumlarga qarshi kurashishga qaratilgan (Estonian Information System Authority, 2023). Bundan tashqari, Estoniyada kiberxavfsizlik bo‘yicha milliy strategiya ishlab chiqilgan bo‘lib, unda ijtimoiy muhandislik hujumlariga qarshi kurashish choralari ham o‘z aksini topgan.

Estoniya tajribasining asosiy jihatlari quyidagicha:

Davlat-xususiy hamkorlik: Kiberxavfsizlikni ta’minlash uchun davlat organlari va xususiy kompaniyalar o‘rtasida yaqin hamkorlik yo‘lga qo‘yilgan. Bu hamkorlik kiberhujumlarga qarshi tezkor javob berish va tajriba almashish imkonini beradi.

Ta’lim choralari: Davlat xodimlari va xususiy sektor vakillari uchun muntazam ravishda kiberxavfsizlik bo‘yicha treninglar o‘tkaziladi, bu esa ijtimoiy muhandislik hujumlarini aniqlash va ularga qarshi kurashish qobiliyatini oshiradi.

Masalan, Estoniyada xodimlar uchun phishing hujumlarini aniqlash bo'yicha maxsus simulyatsiyalar o‘tkaziladi.

Texnologik infratuzilma: Estoniyada elektron hukumat tizimlari (e-Government) yuqori darajada himoyalangan bo‘lib, ko‘p bosqichli autentifikatsiya va shifrlash texnologiyalari qo‘llaniladi. Bu ijtimoiy muhandislik orqali ruxsatsiz kirishni qiyinlashtiradi.

Estoniya tajribasi O'zbekiston uchun foydali bo‘lishi mumkin, ayniqsa davlat-xususiy hamkorlikni rivojlantirish va elektron hukumat tizimlarini himoya qilishda.

Singapur tajribasi

Singapurda **“Kiberxavfsizlik to‘g‘risida”gi qonun** kiberhujumlar haqida hisobot berishni majburiy qiladi va kiberxavfsizlik xizmatlari ko‘rsatuvchi provayderlar uchun litsenziyalash tizimini joriy etadi (Cybersecurity Agency of Singapore, 2023). Singapurda ijtimoiy muhandislik hujumlariga qarshi kurashish uchun texnik choralarga katta e’tibor qaratiladi.

Singapur tajribasining asosiy jihatlari:

- **Texnik himoya**: Ko‘p bosqichli autentifikatsiya (MFA) tizimlari va shifrlash texnologiyalari keng qo‘llaniladi. Masalan, Singapur banklari va davlat tashkilotlari MFA tizimlarini majburiy qilib belgilagan.
- **Ma'rifiy kampaniyalar**: Hukumat aholi o'rtasida kiberxavfsizlik bo‘yicha keng qamrovli ma'rifiy kampaniyalar o'tkazadi, bu esa foydalanuvchilarning ijtimoiy muhandislik taktikalarini tanib olish qobiliyatini oshiradi. Masalan, "Cyber Safe Singapore" kampaniyasi orqali aholiga phishingdan himoyalanish bo‘yicha maslahatlar beriladi.
- **Huquqiy majburiyatlar**: Tashkilotlar kiberxavfsizlik choralarini ko‘rishga majbur bo'lib, aks holda jarimaga tortiladi. Bu tashkilotlarni xavfsizlikka ko‘proq e’tibor qaratishga undaydi.

Singapur tajribasi O‘zbekiston uchun texnik choralarni joriy etish va aholini kiberxavfsizlik bo‘yicha o‘qitishda foydali bo'lishi mumkin.

Yevropa Ittifoqi tajribasi

Yevropa Ittifoqida **“Umumiy ma’lumotlarni himoya qilish reglamenti” (GDPR)** shaxsiy ma’lumotlarni himoya qilishning qat’iy standartlarini belgilaydi (European Union, 2016). GDPRga ko‘ra, tashkilotlar shaxsiy ma’lumotlarni himoya qilish bo‘yicha qat’iy choralarni ko‘rishlari shart, aks holda katta jarimalarga tortiladilar.

GDPRning asosiy jihatlari:

- **Ma‘lumotlar himoyasi**: Tashkilotlar shaxsiy ma’lumotlarni himoya qilish uchun texnik va tashkiliy choralar ko‘rishlari shart. Masalan, ma’lumotlar bazalarini shifrlash va xodimlarni o‘qitish majburiy hisoblanadi.

- **Hisobot berish**: Ma’lumotlar buzilishi holatlari haqida 72 soat ichida xabar berish majburiy. Bu kiberhujumlarga tezkor javob berish imkonini beradi.
- **Foydalanuvchi huquqlari**: Shaxslar o‘z ma’lumotlari ustidan ko‘proq nazoratga ega bo‘lib, ularni o‘chirish yoki o‘tkazish huquqiga ega. Bu ijtimoiy muhandislik orqali ma‘lumotlarni o‘g‘irlashni qiyinlashtiradi.

Ushbu reglament ijtimoiy muhandislik hujumlari orqali ma‘lumotlarni o‘g‘irlashga qarshi kurashishda samarali vosita hisoblanadi, chunki tashkilotlar ma‘lumotlarni himoya qilish uchun texnik va tashkiliy choralarni kuchaytirishga majbur bo'ladilar. O‘zbekiston GDPR tajribasidan shaxsiy ma’lumotlarni himoya qilish bo‘yicha qat’iy standartlarni joriy etishda foydalanishi mumkin. Xalqaro tajriba shuni ko‘rsatadiki, ijtimoiy muhandislikka qarshi kurashish uchun faqat huquqiy choralarga tayanish yetarli emas. Texnik yechimlar, ta’lim va davlat-xususiy hamkorlik birgalikda qo‘llanilganda samarali natija beradi. O'zbekiston ushbu tajribalarni o‘z sharoitlariga moslashtirib, kiberxavfsizlikni yanada mustahkamlashi mumkin. Masalan, Estoniyaning davlat-xususiy hamkorlik modeli, Singapurning texnik choralarga e’tibori va GDPRning shaxsiy ma’lumotlarni himoya qilish bo‘yicha qat‘iy talablari O'zbekiston uchun muhim saboqlar bo‘la oladi.

Respublikamizda virtual olamda ijtimoiy muhandislik orqali sodir etiladigan huquqbuzarliklarni oldini olish uchun huquqiy, texnik va ta'lim choralari majmuasini qo'llash zarur. Texnik jihatdan, Respublikamizda ijtimoiy muhandislik hujumlariga qarshi kurashish uchun zamonaviy kiberxavfsizlik vositalarini joriy etish zarur. Quyidagi texnik yechimlar samarali bo‘lishi mumkin:

Ko'p bosqichli autentifikatsiya (MFA)

Foydalanuvchilardan tizimga kirish uchun bir nechta tasdiqlash usullaridan foydalanish talab etiladi (masalan, parol + SMS kod). Bu phishing hujumlari orqali olingan login/parollar yordamida tizimga kirishni qiyinlashtiradi. Masalan, O‘zbekiston banklari va elektron hukumat xizmatlari MFA tizimlarini majburiy qilib joriy etishi mumkin.

Shifrlash texnologiyalari

Maxfiy ma’lumotlarni shifrlash orqali, hatto ma’lumotlar o‘g‘irlansa ham, tajovuzkorlar ularni o‘qiy olmasligi ta’minlanadi. Masalan, bank tizimlari va elektron hukumat xizmatlarida shifrlash majburiy qilinishi mumkin. Bu ijtimoiy muhandislik orqali ma'lumotlar o'g'irlangan taqdirda ham zarar miqdorini kamaytiradi.

Zararli dasturlarga qarshi dasturlar

Foydalanuvchilarning qurilmalariga zararli dasturlarni aniqlash va bloklashga qodir dasturlarni o'rnatish. Bu baiting hujumlari orqali tarqatiladigan viruslarga qarshi samarali. Masalan, antivirus dasturlari davlat organlari va xususiy tashkilotlarda majburiy qilinishi mumkin.

Axborot xavfsizligi monitoring Tashkilotlar ichida axborot xavfsizligini doimiy ravishda monitoring qilish va shubhali faoliyatni aniqlash tizimlarini joriy etish. Masalan, phishing elektron xatlarini avtomatik aniqlash uchun AI-ga asoslangan tizimlar qo‘llanilishi mumkin. Bu tashkilotlarga kiberhujumlarga tezkor javob berish imkonini beradi.

Ta’lim va ma’rifiy choralarning kuchaytirilishi

Ijtimoiy muhandislik hujumlariga qarshi kurashishda eng muhim omillardan biri foydalanuvchilarning kiberxavfsizlik bo‘yicha bilim va ko‘nikmalarini oshirishdir. O‘zbekistonda quyidagi ta’lim choralari qo‘llanilishi mumkin:

Maktab va universitetlarda kiberxavfsizlik darslari

Yosh avlodni kiberxavfsizlik bo'yicha asosiy bilimlar bilan ta’minlash uchun ta'lim dasturlariga kiberxavfsizlik bo’yicha maxsus darslar kiritilishi kerak. Masalan:

Phishing hujumlarini qanday aniqlash;

Xavfsiz parollarni yaratish qoidalari;

Internetda shaxsiy ma’lumotlarni himoya qilish usullari.

Bu darslar yoshlarni kiberxavfsizlik bo‘yicha ongli qilishga yordam beradi va kelajakda ularni ijtimoiy muhandislik hujumlaridan himoyalaydi.

Tashkilotlarda muntazam treninglar

Davlat va xususiy sektor tashkilotlari xodimlar uchun ijtimoiy muhandislik hujumlarini aniqlash va ularga qarshi kurashish bo'yicha muntazam treninglar o‘tkazishlari shart. Masalan, xodimlarga soxta elektron xatlarni haqiqiydan ajratish o‘rgatilishi mumkin. Treninglar real hayotdagi misollar asosida o‘tkazilishi va simulyatsiyalarni o'z ichiga olishi kerak.

Ommaviy axborot vositalari orqali ma’rifiy kampaniyalar Televidenie, radio va ijtimoiy tarmoqlar orqali keng ommani kiberxavfsizlik bo‘yicha ogohlantirish va ularga asosiy himoya choralari haqida ma‘lumot berish. Masalan, “Phishingdan ehtiyot bo‘ling!” kabi kampaniyalar o‘tkazilishi mumkin. Ushbu kampaniyalar aholining kiberxavfsizlik bo‘yicha bilimlarini oshirishga xizmat qiladi va ularni ijtimoiy muhandislikdan himoyalaydi.

Davlat-xususiy hamkorlik

Ijtimoiy muhandislikka qarshi kurashishda davlat organlari va xususiy sektor o‘rtasida hamkorlikni kuchaytirish zarur. Masalan:

- Kiberxavfsizlik bo‘yicha milliy markaz tashkil etish – bu markaz kiberhujumlarga qarshi muvofiqlashtirish va tezkor javob berish vazifasini bajaradi;
- Xususiy kompaniyalar bilan tajriba almashish platformalarini yaratish – bu platformalar orqali kiberxavfsizlik bo‘yicha eng yaxshi amaliyotlar almashiladi;
- Kiberhujumlarga qarshi birgalikda javob berish mexanizmlarini ishlab chiqish – bu mexanizmlar kiberhujumlarning oldini olish va zararini kamaytirishga xizmat qiladi.

Virtual olamda ijtimoiy muhandislik orqali sodir etiladigan huquqbuzarliklar zamonaviy raqamli dunyoda jiddiy xavf-xatarlardan hisoblanadi. O‘zbekiston Respublikasida ushbu huquqbuzarliklarni oldini olish uchun qonunchilik asoslari mavjud, ammo ularni yanada takomillashtirish va xalqaro tajribadan foydalanish zarur. Huquqiy, texnik va ta’lim choralari majmuasini qo‘llash orqali O‘zbekiston ushbu huquqbuzarliklarga qarshi samarali kurash olib borishi mumkin. Ayniqsa, qonunchilikni ijtimoiy muhandislikning o‘ziga xos xususiyatlarini hisobga olgan holda takomillashtirish, zamonaviy texnik vositalarni joriy etish va foydalanuvchilarning kiberxavfsizlik bo‘yicha bilimlarini oshirish muhim ahamiyatga ega. Masalan, Jinoyat kodeksiga ijtimoiy muhandislikka qarshi maxsus moddalar kiritish, tashkilotlar uchun majburiy texnik standartlarni joriy etish va maktablarda kiberxavfsizlik darslarini yo'lga qo‘yish kabi choralardan boshlash mumkin. Xalqaro tajribaga tayangan holda, Estoniya va Singapur kabi davlatlarning davlat-xususiy hamkorlik va ta'lim sohasidagi yondashuvlari O‘zbekiston uchun foydali bo'lishi mumkin. Faqat shu yo‘l bilan O‘zbekiston virtual olamdagi huquqbuzarliklarga qarshi ishonchli himoyani ta’minlay oladi. Ushbu maqolada keltirilgan tavsiyalar amalda qo'llanilsa, O‘zbekiston nafaqat ijtimoiy muhandislik hujumlaridan himoyalanish, balki umumiy kiberxavfsizlik darajasini oshirishda ham muhim yutuqlarga erishadi. Kiberxavfsizlikni ta’minlash nafaqat davlat organlari, balki xususiy sektor va har bir fuqaroning mas’uliyatidir. Shu sababli, ushbu sohada umumiy harakat va hamkorlik zarur.

Foydanilgan adabiyotlar:

1. **O‘zbekiston Respublikasi qonuni**. (2019). “Shaxsiy ma’lumotlar to‘g‘risida”gi qonun. O‘zbekiston Respublikasi Oliy Majlisi tomonidan qabul qilingan, 2-oktyabr, 2019-yil, № ZRU-571.
2. **O‘zbekiston Respublikasi Jinoyat kodeksi**. (1994). O‘zbekiston Respublikasi Oliy Majlisi tomonidan qabul qilingan, 22-sentyabr, 1994-yil, № 2012-XII (keyingi o‘zgartirishlar bilan).
3. **O'zbekiston Respublikasi qonuni**. (2003). “Axborot xavfsizligi to'g'risida”gi qonun. O‘zbekiston Respublikasi Oliy Majlisi tomonidan qabul qilingan, 11-dekabr, 2003-yil, № 560-II
4. **Verizon**. (2023). “2023 Data Breach Investigations Report.” Verizon Business. https://www.verizon.com/business/resources/reports/dbir/
5. **Reuters**. (2016). “Bangladesh Bank Heist: How Hackers Stole $1 Billion.” Reuters, 10-mart, 2016-yil. https://www.reuters.com/article/us-cyber-heist-bangladesh-idUSKCN0WC0TJ
6. **Estonian Information System Authority**. (2023). “Cybersecurity in Estonia: Legislation and Strategy.” https://www.ria.ee/en/cybersecurity.html
7. **Cybersecurity Agency of Singapore**. (2023). “Cybersecurity Act and Initiatives.” https://www.csa.gov.sg/legislation/cybersecurity-act

8. **European Union**. (2016). "General Data Protection Regulation (GDPR)." Regulation (EU) 2016/679 of the European Parliament and of the Council, 27-aprel, 2016-yil. https://eur-lex.europa.eu/eli/reg/2016/679/oj
9. **National Institute of Standards and Technology (NIST)**. (2020). "Special Publication 800-63B: Digital Identity Guidelines." U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
10. **ENISA (European Union Agency for Cybersecurity)**. (2022). "Threat Landscape 2022." https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
11. **Cybersecurity Agency of Singapore**. (2023). "Cybersecurity Act and Initiatives." https://www.csa.gov.sg/legislation/cybersecurity-act
12. **BM Security**. (2022). "Cost of a Data Breach Report 2022." https://www.ibm.com/security/data-breach
13. **United Kingdom National Cyber Security Centre (NCSC)**. (2023). "Introduction to Social Engineering." https://www.ncsc.gov.uk/guidance/introduction-social-engineering
14. **World Economic Forum**. (2023). "Global Cybersecurity Outlook 2023." https://www.weforum.org/reports/global-cybersecurity-outlook-2023/
15. **Interpol**. (2022). "Cybercrime: Social Engineering Threats." https://www.interpol.int/Crimes/Cybercrime/Social-engineering-threats