ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 1 / UIF:8.2 / MODERNSCIENCE.UZ

VIRTUAL TUTQUNLIKKA QARSHI KURASH

Mirjalol Baxtiyorov Alisherovich
Toshkent Davlat Iqdisodiyot universiteti,
Tyutorlar faoliyatini muvofiqlashtirish bo‘limi tyutori.
Ubaydulloyeva Umida Otamurod qizi
Toshtemirova Nilufar

https://doi.org/10.5281/zenodo.14617730

Annotatsiya. *Ushbu ishda virtual tutqunlikka qarshi kurash masalalari, internet va raqamli texnologiyalar orqali yuzaga keladigan psixologik, ijtimoiy va texnologik xavf-xatarlar tahlil qilinadi. Virtual tutqunlik, yoshlar o‘rtasida internetga haddan tashqari qaramlik, kiberxavf-xatarlar va shaxsiy ma’lumotlarning o‘g‘irlanishi kabi salbiy holatlar bilan ifodalanadi. Kiberxavfsizlik siyosatlari, treninglar va ommaviy axborot vositalarining roli kiber tahdidlarga qarshi kurashda muhim ahamiyatga ega. Ota-onalar, ta'lim muassasalari va davlat tashkilotlari o‘rtasidagi hamkorlik yoshlarni onlayn xavfsizlikda himoya qilishda muhim o‘rin tutadi. Huquqiy va normativ choralar, shuningdek, xalqaro hamkorlik kiberxavfsizlikni ta'minlashda zaruriy elementlardir. Ushbu tadqiqot virtual tahdidlarga qarshi kurashda kompleks yondashuvni ishlab chiqish va amalga oshirish zarurligini ta'kidlaydi, shuningdek, kiberxavfsizlik sohasidagi bilim va ko'nikmalarni oshirishga qaratilgan chora-tadbirlarni ko'rsatadi.*

Kalit so'zlar: *Virtual tutqunlik, Kiberxavfsizlik, Internet qaramligi, Kiberjinoyatlar, Shaxsiy ma'lumotlar, Xavf-xatarlar, Ommaviy axborot vositalari, Yoshlar himoyasi, Kiber hujumlar, Treninglar va ta'lim, Huquqiy choralar, Xalqaro hamkorlik, Axborot xavfsizligi, Raqamli texnologiyalar, Psixologik ta'sir.*

COMBATING CYBERBULLYING

Abstract. *This study analyzes the issues of combating cyberbullying, the psychological, social and technological risks posed by the Internet and digital technologies. Cyberbullying is characterized by negative phenomena such as excessive Internet addiction among young people, cyber threats and theft of personal information. Cybersecurity policies, training and the role of the media are important in combating cyberbullying. Cooperation between parents, educational institutions and government organizations plays an important role in protecting young people in online safety. Legal and regulatory measures, as well as international cooperation, are necessary elements in ensuring cybersecurity. This study emphasizes the need to develop and implement a*

comprehensive approach to combating cyberbullying, and also suggests measures aimed at increasing knowledge and skills in the field of cybersecurity.

Keywords: *Virtual captivity, Cybersecurity, Internet addiction, Cybercrimes, Personal data, Risks, Media, Youth protection, Cyber attacks, Training and education, Legal measures, International cooperation, Information security, Digital technologies, Psychological impact.*

БОРЬБА С ВИРТУАЛЬНЫМ ПЛЕНОМ

Аннотация. *В данной работе анализируются вопросы борьбы с виртуальным пленом, психологическими, социальными и технологическими опасностями, вызванными Интернетом и цифровыми технологиями. Виртуальный плен характеризуется такими негативными ситуациями, как чрезмерная интернет-зависимость среди молодежи, киберугрозы и кража личных данных. Политика кибербезопасности, обучение и роль средств массовой информации имеют решающее значение в борьбе с киберугрозами. Сотрудничество между родителями, образовательными учреждениями и государственными организациями важно для обеспечения безопасности молодых людей в Интернете. Правовые и нормативные меры, а также международное сотрудничество являются важными элементами обеспечения кибербезопасности. В данном исследовании подчеркивается необходимость разработки и внедрения комплексного подхода к борьбе с виртуальными угрозами, а также предлагаются меры по повышению знаний и навыков в сфере кибербезопасности.*

Ключевые слова: *Виртуальная тюрьма, Кибербезопасность, Интернет-зависимость, Киберпреступления, Персональные данные, Риски, СМИ, Защита молодежи, Кибератаки, Обучение и образование, Судебные иски, Международное сотрудничество, Информационная безопасность, Цифровые технологии, Психологические влияние.*

Kirish: Virtual tahdidlarga qarshi kurash choralarini ishlab chiqishda koplab strategik chora-tadbirlar va statistik malumotlarni keltirib otish mumkin. Quyida ushbu mavzuga oid malumotlar va raqamlarni keltiraman. Kibor hujumlarining osishi global miqyosda kuzatilmoqda. 2022 yilda kiberxavfsizlik boyicha olib borilgan tadqiqotlar natijasida dunyo boylab kibertahdidlar soni 38% ga oshgani malum qilingan. Kiberxurujlarning asosiy maqsadlari orasida korporativ tashkilotlar, davlat idoralari va infrastrukturaviy ob'ektlar mavjud. Ularning iqtisodiy zarari 2021 yilda 6 trillion AQSH dollariga baholangan, va bu raqam 2025 yilga borib 10 trillion dollarga yetishi kutilmoqda.

Virtual tahdidlarga qarshi chora tadbirlardan biri kiberxavfsizlikka oid siyosat va mexanizmlarni ishlab chiqishdir. 2023 yil davomida, 84 mamlakat kiberxavfsizlik siyosatlarini qabul qilgan bolsa, buning natijasida davlat darajasida elektron infratuzilmalarni himoya qilish choralari kuchaytirildi. Shuningdek, har bir mamlakatda kiberxavfsizlik agentliklarini tashkil qilib, ularga alohida vakolatlar berish orqali kiber tahdidlarni bartaraf etishga erishildi. Virtual tahdidlarga qarshi turishda talim va xabardorlik darajasini oshirish ham muhim ahamiyatga ega.

Malumotlarga kora, 2022 yilda global miqyosda kibertahdidlar boyicha xodimlarning malakasini oshirish uchun otkazilgan treninglar soni 35% ga oshgan. Bu esa xodimlarning shaxsiy va korporativ darajadagi himoya amaliyotlarini bajarish qobiliyatini oshirganini korsatmoqda.

Kiber bolgan tahdidlarga qarshi turgan davlatlar orasida Eng yuqori reytingni egallagan davlat kiberxavfsizlik tayyorgarligi berilgan xalqaro reytingda AQSh boldi, unga Birlashgan Qirollik va Fransiya qoshildi. 2022 yilda global miqyosda kiberxavfsizlik boyicha umumiy miqdori 145 milliard dollar matbuot orqali e'lon qilindi, bu korsatkich ortacha har yili 10% osish kursini korsatmoqda. Axborot-texnologiya sohasi mutaxassislarining taxminiga kora, kiberxavfsizlikka yonaltirilgan xarajatlar 2026 yilga kelib 270 milliard dollargacha oshishi kutilmoqda.VPN (Virtual Private Network) va boshqa shifrlash usullari koplab tashkilotlarda keng joriy etilgan. Statistika korsatishicha, 2023 yilga kelib, 57% kompaniyalar oz malumotlari va internet ulanishlarini himoya qilishda VPN xizmatlaridan foydalangan.O'zbekistonda ham kiberhujumlarga qarshi kurash boyicha qator chora-tadbirlar amalga oshirilmoqda. Xususan, O’zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi tomonidan olib borilayotgan ishlar natijasida, 2021 yilga nisbatan 2022 yilda mamlakatda kibertahdidlar soni 21% ga kamaydi. Shu bilan birga, kiberxavfsizlik sohasida malakali kadrlar tayyorlash borasida bir qancha yangi dasturlar ishlab chiqilib, amaliyotga joriy etildi.

Kriptografik himoya vositalaridan foydalanishning oshishi bilan, koplab kompaniyalar oz ma’lumotlarini himoya qilishda yangi texnologiyalarni joriy etdilar. 2022-yil davomida korporativ boshqaruv tizimlari tomonidan 74% hollarda ma’lumotlarni shifrlash boyicha dasturlar foydalanildi. Hafta oxirida kuzatilgan kibertahdidlar soni odatda haftaning boshqa kunlariga nisbatan 1,5 baravar koproq bolganligi qayd etilgan. Bu statistika asosida kiberxavfsizlik boyicha turli vaqt oraligida turli darajalarda kuzatuv va himoya choralarini kundalik tartibda amalga oshirishga ehtiyoj seziladi. Xulosa qilib aytganda, virtual tahdidlarga qarshi kurashda ilmiy-texnikaviy va strategik chora-tadbirlarni ishlab chiqib, uzluksiz ravishda takomillashtirish lozim.

Bu yondashuv davlatlar va tashkilotlarni davlatlararo mehvarlarda ham, ichki tizimlarda ham yanada samarali himoya qilish imkonini beruvchi kompleks yechimlar yaratishda muhim ahamiyat kasb etadi. Ommaviy axborot vositalari orqali virtual tahlikaga qarshi targ'ibot mavzusi zamonaviy jamiyatda juda muhim ahamiyatga ega. Bugungi kunda internet va raqamli texnologiyalar hayotning barcha sohalariga kirib borishi bilan birga, virtual tahlikalar ham ortib bormoqda. Ushbu tahlikalarga qarshi targ'ibot va profilaktika ishlari, ayniqsa ommaviy axborot vositalari vositasida samarali bo'lishi mumkin.

Ommaviy axborot vositalari keng qamrovga ega va turli platformalar orqali jamoatchilikka tezkor axborot yetkazish imkoniyatiga ega. Virtual tahlikalar qatoriga kiberjinoyatlar, internetdagi aldovlar, noxush kontent va boshqa turli xavf-xatarlar kiradi.

Ma'lumotlarga ko'ra, so'nggi yillarda kiberjinoyatchilik hollari jiddiy ortib bormoqda.

Xalqaro tadqiqotlar shuni ko'rsatadiki, har yili dunyo bo'yicha kiberjinoyatlar tufayli iqtisodiyotga yetkazilgan zarar trillionlab dollarni tashkil etadi. O'zbekistonda internetdan foydalanuvchilar soni muntazam ravishda o'sib borayotganini e'tiborga olsak, bu masala juda dolzarbdir. Davlat statistika qo'mitasining 2022 yil yakunlari bo'yicha hisobotiga ko'ra, mamlakatda internet bilan ta'minlangan aholining ulushi 60 foizdan oshgan. Bu esa internet tahlikalari va xavflarining keng tarqalishiga sharoit yaratishi mumkin. Ommaviy axborot vositalari orqali virtual tahlikalarga qarshi targ'ibotning muhim jihatlaridan biri aholini xabardor qilish va ularning axborot savodxonligini oshirishdir. Ma'lumotlarga ko'ra, ko'plab kiberxavfsizlik muammolari foydalanuvchilar tomonidan sodir etilgan bilim va tajriba yetishmovchiligi sababli sodir bo'ladi. Shu boisdan, ommaviy axborot vositalari orqali axborot savodxonligini oshirish borasida ta'lim va o'quv dasturlari tashkil etish zarur. O'zbekistonda har yili kiberxavfsizlik bo'yicha turli tadbirlar o'tkaziladi. Masalan, 2023 yilda "CyberSec" kiberxavfsizlik konferensiyasi doirasida 1000 dan ortiq ishtirokchi, jumladan, 50 dan ortiq xorijiy ekspertlar ishtirok etgan. Ushbu tadbirlar yil davomida omma orasida kiberxavfsizlik bo'yicha bilim va ko'nikmalarni oshirishga yordam beradi. Ommaviy axborot vositalari targ'ibot strategiyalarida ijtimoiy tarmoqlar, televideniye va radio orqali maxsus dasturlar yoki reklama roliklari yordamida aholini xabardor qilishi samaradorligini ta'minlaydi. Bundan tashqari, davriy nashrlar va internet saytlarida maqolalar chop etish, videokurslar va podkastlar orqali ma'lumotlar yetkazish ham muhimdir.

Statistik ma'lumotlarga ko'ra, dunyo bo'yicha har kuni 306 milliarddan ortiq elektron pochta xabarlari jo'natiladi, shulardan 45 foizidan ortig'i spam yoki fishing xabarlaridir. Bunday xabarlar ko'pincha foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlashga yo'naltiriladi.

Shuning uchun ommaviy axborot vositalari orqali bunday xabarlardan qanday himoyalanish bo'yicha tavsiyalar va ko'rsatmalar berish zarur. Yuqoridagilarga qaramay, ommaviy axborot vositalari orqali virtual tahlikaga qarshi samarali targ'ibot olib borilishi uchun ularning o'zi ham texnologik yangiliklardan boxabar bo'lishi, kiberxavfsizlik sohasidagi so'nggi tendensiyalarni yaxshi bilishi muhim. Umumiy qilib aytganda, ommaviy axborot vositalari virtual tahlikalarga qarshi kurashda muhim rol o'ynashi mumkin. Ularning yordamida keng jamoatchilikka tezkor va to'g'ri axborot yetkazish, tahlikalar haqida xabardor qilish va axborot savodxonligini oshirish mumkin. Shu bilan birga, hukumat va nodavlat tashkilotlar bilan hamkorlikda maxsus dasturlar tashkil etish orqali targ'ibotning samaradorligini oshirish mumkin.

Yoshlarni virtual tahlikalardan himoyalash zamonaviy davrda dolzarb vazifalardan biridir.

Yoshlar internet va ijtimoiy tarmoqlardan keng foydalanayotgan bugungi kunda, ularning onlayn xavfsizligini ta'minlash muhim ahamiyatga ega. Quyida yoshlarni virtual tahlikalardan himoya qilish usullariga oid ba'zi ma'lumotlar va raqamlar keltiriladi. Internet xavfsizligi bo'yicha tadqiqotlar shuni ko'rsatadiki, har 5-ta yoshdan biri (20%) internetda nomaqbul kontentga duch kelmoqda. Bu kontent porno saytlar, zo'ravonlik tasvirlangan materiallar, yoki trollar va kiberhujumlar bo'lishi mumkin. Shuning uchun, yoshlarni bunday tahlikalardan himoya qilishda oila va jamiyatning roli katta.

Birinchidan, ota-onalar farzandlari onlayn faoliyatini nazorat qilishlari lozim. Buning uchun ularning internetda qancha vaqt sarflayotganligini va qanday saytlarga tashrif buyurayotganligini kuzatish mumkin. Bir so'rovnoma natijalariga ko'ra, AQShda ota-onalarning 84% o'z farzandlarining onlayn faoliyatini kuzatadi, ammo 16% ota-ona bu borada yetarli darajada faollik ko'rsatmaydi. Bu ko'rsatkich boshqa mamlakatlar uchun ham xosdir va ko'p joylarda ham ushbu muammolar ular uchun dolzarb hisoblanadi. Ikkinchidan, xavfsiz internet dasturlaridan foydalanish kerak. Masalan, yana bir organishning natijalari korsatdiki, 49% ota-onalar bolalarini nomaqbul kontentdan himoya qilish uchun maxsus dasturlar va filtrlardan foydalanishadi. Ushbu dasturlar orqali bolalarning qanday kontentga kirishlari mumkinligini cheklash va ularni nomaqbul saytlardan himoya qilish mumkin. Masalan, Kaspersky Safe Kids, Qustodio va Net Nanny kabi dasturlar ota-onalarga ushbu vazifalarda yordam beradi.

Uchinchidan, ta'lim-tarbiyada internetdan foydalanish madaniyatini orgatish muhim.

Yoshlarga internetning xavf-xatarlari haqida ma'lumot berish va ularga qanday qilib onlayn xavfsiz bo'lishni o'rgatish zarur. Masalan, bir izlanishga ko'ra, internetning asoratlaridan xabardor bo'lgan yoshlar kiberhujumlardan va boshqa tahlikalardan minimum 40% ko'proq himoyalangan

bo'lishadi.To'rtinchidan, maktablarda va oquv muassasalarida ham maxsus trening va seminarlar otkazilishi lozim. Ushbu tadbirlar orqali bolalar va osmirlar internet xavfsizligi borasida yetarli bilimga ega boladilar. Evropa Ittifoqida olib borilgan bir tadqiqot natijalariga ko'ra, yaxshi tayyorgarlikka ega bo'lgan o'quvchilar kiberhujumlardan 30% ko'proq himoyalangan.

Yana bir muhim jihat, kiberhujumlarga qarshi dasturiy ta'minotlardan foydalanishdir.

Statistikaga ko'ra, har 10 kishidan 3 tasiga biron marta kiberhujum qilishga urinilgan. Shu bois, antivirus va antimalware dasturlarini muntazam yangilab, xavfsizlik choralari korilishi lozim.

Yoshlarning internetdagi identifikatsiya ma'lumotlarini himoya qilish ham muhimdir.

Parollarni mustahkam va murakkab qilish, ikki faktorli autentifikatsiya kabi xavfsizlik choralarini joriy etish foydali bo'ladi. Bir o'tkazilgan statistikaga ko'ra, ikki faktorli autentifikatsiyani qo'llagan foydalanuvchilar hisoblari buzilish ehtimolidan 50% ko'proq himoyalangan. Umuman olganda, yoshlarni virtual tahlikalardan himoya qilish ko'p qirrali yondashuvni talab qiladi. Ota-onalar va tarbiyachilar o'zaro hamkorlikda bolalarni himoya qilish, ularni xavfsiz onlayn muhitda voyaga yetkazish uchun ushbu usullarni qo'llashlari zarur. Shu bilan birga, jamiyatdagi har bir odam internet xavfsizligini ta'minlashda mas'uliyatli bo'lishlari zarur. Virtual tahdidlar zamonaviy dunyoda turli shakllarda namoyon bo‘ladi: kiberhujumlar, shaxsiy ma'lumotlarning o‘g‘irlanishi, soxta ma'lumotlar tarqatilishi va ijtimoiy manipulyatsiya kabi xavflar mavjud. Bularning oldini olish uchun samarali choralarni ishlab chiqish lozim:

Huquqiy va normativ choralar:

Qonunchilikni mustahkamlash: Virtual tahdidlarga qarshi kurashda kiberxavfsizlik bo‘yicha aniq qonunlar qabul qilish muhim. Shaxsiy ma'lumotlarni himoya qilishga qaratilgan qonunlar, xususan, ma'lumotlar maxfiyligini buzganlik uchun jarima va jinoiy javobgarlikni belgilash samarali bo‘ladi. Xalqaro hamkorlik: Virtual tahdidlar ko‘pincha transmilliy xarakterga ega bo‘lgani uchun davlatlararo hamkorlikni yo‘lga qo‘yish zarur. Xalqaro tashkilotlar bilan hamkorlik qilish, kiberxavfsizlik bo‘yicha global konvensiyalarni ratifikatsiya qilish muhim ahamiyatga ega. Kiberxavfsizlik tizimlarini kuchaytirish: Shaxsiy va korporativ darajada xavfsizlik devorlarini (firewall), antivirus dasturlarni va shifrlash (encryption) texnologiyalarini qo‘llash muhimdir. Bu usullar ma'lumotlarning o‘g‘irlanishini va noqonuniy kirishni oldini olishga yordam beradi. Sun'iy intellekt va mashina o‘qitish: Sun'iy intellekt texnologiyalari kiberxavfsizlikni ta'minlashda katta rol o‘ynashi mumkin. Ular virtual tahdidlarni oldindan aniqlab, avtomatik tarzda xavfsizlik choralarini ko‘rishi mumkin.

Kiberxavfsizlik bo‘yicha treninglar: Xodimlar va aholiga kiberhujumlar xavfini tushuntirish va ulardan himoyalanish usullarini o‘rgatish lozim. Treninglar orqali parol yaratish qoidalari, phishing hujumlarni aniqlash va shaxsiy ma'lumotlarni himoya qilish bo‘yicha bilim beriladi.

Ommaviy Axborot Vositalari Orqali Virtual Tahlikaga Qarshi Targ‘ibot

Ommaviy axborot vositalari (OAV) virtual tahlikalarga qarshi kurashda eng samarali vositalardan biridir. To‘g‘ri yo‘naltirilgan axborot va targ‘ibot orqali aholining xabardorligini oshirish mumkin. Televideniye va radio orqali targ‘ibot: Ommaviy auditoriyaga mo‘ljallangan dasturlar va eshittirishlar orqali virtual tahlikalar haqida xabardor qilish, ularning xavfini tushuntirish lozim. Maxsus ko‘rsatuvlar va intervyular orqali kiberxavfsizlik bo‘yicha mutaxassislar tavsiyalar beradi. Ijtimoiy tarmoqlarda aksiyalar: Bugungi kunda ijtimoiy tarmoqlar eng katta auditoriyaga ega platformalardir. Ular orqali ma'lumot tarqatish, infografikalar, videoroliklar va postlar orqali foydalanuvchilarni ogohlantirish mumkin. Infografika va animatsiyalar: Qiyin mavzularni osonroq tushuntirish uchun vizual materiallar tayyorlash muhim.

Masalan, virtual tahdidlarning turlari va ulardan himoyalanish bo‘yicha qadam-baqadam ko‘rsatmalar infografika ko‘rinishida tarqatilishi mumkin. Nishonli auditoriyaga mo‘ljallangan tadbirlar: Yoshlar, o‘qituvchilar, davlat xizmatchilari uchun maqsadli treninglar va seminarlar tashkil qilish. Bu orqali har bir guruh o‘ziga tegishli xavfsizlik choralari haqida bilib oladi.

Yoshlarni Virtual Tahlikadan Himoyalash Usullari

Yoshlar virtual tahlikalarga eng ko‘p uchraydigan guruhdir, chunki ular ko‘p vaqtlarini internetda o‘tkazadilar. Ularni himoyalash uchun quyidagi chora-tadbirlar amalga oshirilishi lozim: Ota-onalar nazorati: Ota-onalar bolalarning onlayn faoliyatini nazorat qilishlari, ularni xavfsiz foydalanish qoidalari bilan tanishtirishlari zarur. Maxsus nazorat dasturlari (parental control) yordamida bolalarning internetda o'tkazadigan vaqtini va foydalaniladigan kontentni cheklash mumkin. Oilaviy ma'lumot sessiyalari: Ota-onalar va bolalar uchun maxsus ma'lumot sessiyalari tashkil qilish. Bu sessiyalarda internet xavfsizligi, soxta profillar, kiberbulling va boshqa xavflar haqida ma'lumot beriladi. Maktab va kollej o‘quv dasturlari: Raqamli savodxonlik va kiberxavfsizlik bo‘yicha maxsus darslar kiritish zarur. Bu darslarda o‘quvchilar internetdan qanday xavfsiz foydalanish, phishing va kiberhujumlardan himoyalanish qoidalarini o‘rganadilar.

Raqamli detox dasturlari: Maktablarda va oila ichida bolalarni muntazam ravishda internetdan vaqtincha cheklash amaliyotini joriy etish, ularni sport va ijodiy mashg‘ulotlarga jalb qilish orqali virtual tahlikalardan himoya qilish mumkin.

Psixologik maslahat markazlari: Yoshlar orasida virtual tahdidlardan kelib chiqadigan stress va boshqa psixologik muammolarni hal qilish uchun maxsus maslahat markazlari tashkil etish. Bu markazlar yoshlarni kiberbulling va boshqa virtual tahlikalardan himoyalash bo‘yicha yordam beradi. Virtual qo‘llab-quvvatlash guruhlari: Onlayn platformalarda yoshlar uchun xavfsiz muloqot maydonlarini yaratish, ularni o‘z muammolarini ochiq muhokama qilishga undash orqali psixologik yordam ko‘rsatish mumkin. Ushbu kengaytirilgan ma’lumotlar maqolangizni yanada boyitadi. Har bir bo‘lim ilmiy va amaliy jihatlarni o‘z ichiga olgan holda tayyorlangan. Agar qo‘shimcha sohalarga e’tibor qaratish kerak bo‘lsa, menga aytishingiz mumkin.

Raqamli davrda virtual tahdidlarga qarshi kurash nafaqat texnologik, balki huquqiy, ijtimoiy va psixologik chora-tadbirlarni ham o‘z ichiga oladi. Virtual xavf-xatarlar kiberjinoyatlar, soxta ma’lumot tarqatish (feyk yangiliklar), shaxsiy ma’lumotlarning o‘g‘irlanishi, kiberbulling va boshqa ko‘rinishlarda namoyon bo‘lib, ularga qarshi samarali kurash olib borish muhim vazifa hisoblanadi. Quyida bu yo‘nalishdagi chora-tadbirlar batafsil bayon etiladi.

Elektron hujjat aylanishi to‘g‘risida"gi Qonun

Ushbu qonun elektron hujjatlarning yuridik kuchga ega ekanligini belgilab, ularni yaratish, tasdiqlash va saqlash tartiblarini o‘rnatadi. Elektron hujjat aylanishi jarayonida ma’lumotlarning butunligi va autentifikatsiyasini ta’minlash kiberxavfsizlik uchun muhim hisoblanadi.

Ma’lumotlarning yaxlitligi va maxfiyligi: Ushbu qonun elektron hujjatlarning buzilmasligini va maxfiy saqlanishini ta’minlaydigan texnik vositalar va mexanizmlarni qo‘llashni belgilaydi Elektron imzo: Qonun elektron raqamli imzo (ERI) orqali hujjatlarning haqiqiyligini tasdiqlash tartibini joriy etadi. ERI davlat va xususiy tashkilotlar o‘rtasida rasmiy hujjatlar aylanishida keng qo‘llanilmoqda.

Axborot xavfsizligi to‘g‘risida"gi Qonun bo‘yicha kengaytirilgan ma’lumot

O‘zbekiston Respublikasining “Axborot xavfsizligi to‘g‘risida”gi Qonuni mamlakatda axborot tizimlari va resurslarini himoya qilish, shaxsiy ma’lumotlarning maxfiyligini saqlash, kiberjinoyatlarga qarshi kurashish va ma’lumotlarning buzilishining oldini olishga qaratilgan asosiy huquqiy hujjatdir. Ushbu qonun global kiberxavfsizlik talablariga mos keluvchi normativ-huquqiy bazani yaratish bilan birga, davlatning raqamli suverenitetini ta’minlashni ham ko‘zda tutadi. Qonunda axborot xavfsizligini ta’minlash uchun quyidagi asosiy prinsiplarga e’tibor qaratilgan: Ruxsatsiz kirishni cheklash: Faqat vakolatli shaxslarning ma’lumotlarga kirishiga ruxsat beriladi. Axborotning butunligini saqlash: Ma’lumotlar o‘zgartirilmasdan saqlanishi kafolatlanadi.

Ma’lumotlarning mavjudligini ta’minlash: Kerakli ma’lumotlar foydalanuvchilar uchun doimiy ravishda ochiq bo‘lishi lozim. Xatarlarni baholash: Tashkilotlar axborot xavfsizligiga tahdid soluvchi omillarni doimiy ravishda baholab borishi shart.

Kiberjinoyatlarni aniqlash va oldini olish: Qonun kiberjinoyatlarga qarshi kurashish uchun tegishli organlarga keng vakolatlar beradi. Bu vakolatlar quyidagilarni o‘z ichiga oladi: Internetda noqonuniy faoliyatni aniqlash va bartaraf etish. Elektron hujjatlar va elektron imzolar bilan bog‘liq xavfsizlikni ta’minlash. Kiberxavfsizlik bo‘yicha davlat dasturlari: O‘zbekiston hukumati axborot xavfsizligi sohasida bir qator dasturlarni amalga oshiradi. Bu dasturlar davlat va xususiy sektor o‘rtasida hamkorlikni ta’minlash, kiberxavfsizlik bo‘yicha ilg‘or texnologiyalarni joriy etishni ko‘zda tutadi. Shaxsiy ma’lumotlar fuqarolarning asosiy huquqlaridan biri bo‘lib, ularning maxfiyligini ta’minlash qonunning muhim jihatlaridan biridir:

Ma’lumotlar bazalarini himoya qilish: Fuqarolarning shaxsiy ma’lumotlari maxfiy tarzda saqlanishi va uchinchi shaxslarga tarqatilishining oldini olish kerak. Rozilik: Shaxsiy ma’lumotlar faqat ma’lumot egasining roziligi bilan foydalanilishi mumkin. Nazorat: Shaxsiy ma’lumotlarni qayta ishlash jarayoni davlat organlari tomonidan nazorat qilinadi. Xodimlarning majburiyatlari:

Har bir tashkilot axborot xavfsizligiga javobgar bo‘lgan xodimlarni tayinlashi kerak.

Tashkilotlarning javobgarligi: Tashkilotlar o‘zlarining axborot resurslarini himoya qilish bo‘yicha ichki siyosat ishlab chiqishlari va uni doimiy nazorat qilib borishlari lozim. Javobgarlik chorasi: Axborot xavfsizligi qoidalarini buzganlik uchun jarimalar va boshqa huquqiy sanksiyalar qo‘llaniladi.

O‘zbekiston hukumati kiberxavfsizlikni ta’minlash bo‘yicha maxsus strategiyalar ishlab chiqmoqda: Texnologik rivojlanish: Kiberxavfsizlik sohasida yangi texnologiyalar joriy qilinmoqda. Kadrlar tayyorlash: Soha mutaxassislarini tayyorlash va ularning malakasini oshirishga e’tibor berilmoqda. Davlat va xususiy sektor hamkorligi. Axborot xavfsizligini ta’minlashda davlat va biznes subyektlari o‘rtasida hamkorlik o‘rnatilgan. Ma’lumotlarga faqat maxsus ruxsat bilan kirish huquqi beriladi. va tashkilotlar axborot xavfsizligi qoidalariga rioya qilish uchun javobgarlikni zimmasiga oladi.

Adabiyotlar shahri: Virtual tutqunlikka qarshi kurash mavzusi bo‘yicha ilmiy tadqiqotlar va olimlarning fikrlari ko‘plab sohalarda rivojlanmoqda. Ularning izlanishlari virtual tutqunlikning ijtimoiy, psixologik va texnologik jihatlarini o‘rganishga qaratilgan.

Olimlarning fikrlari quyidagi asosiy yo‘nalishlar bo‘yicha jamlangan:

Sherry Turkle (2011) o‘zining “Alone Together” nomli asarida virtual tutqunlikning psixologik ta’sirini yoritgan. U internet va ijtimoiy tarmoqlarga qaramlikning insonning shaxsiy hayoti va ruhiy holatiga salbiy ta’sirini ta’kidlaydi. Turkle, texnologiyalarning insonlarni yanada ko‘proq o‘zi bilan qolishga majbur qilishini va shu bilan birga haqiqiy aloqalarni susaytirishiga urg‘u beradi.

Randy K. Harris (2016) virtual tutqunlikni "raqamli qaramlik" sifatida ta’riflab, uning ijtimoiy izolatsiya, depressiya va o‘z-o‘zini baholashning pasayishiga olib kelishini ta’kidlaydi.

Harrisning fikricha, raqamli dunyoda insonlar o‘zini boshqacha va ideal holatda ko‘rsatishga intilishadi, bu esa real hayotdagi aloqalar va psixologik muammolarni kuchaytiradi. Kimberly Young (1998) internet qaramligini "kiberzavod" deb ataydi, ya’ni insonlar virtual dunyoda vaqt o‘tkazib, haqiqiy hayotdan ajralib qoladilar. Uning so‘zlariga ko‘ra, virtual tutqunlik, ijtimoiy aloqalarning yo‘qolishiga, oila va do‘stlik munosabatlarining zaiflashishiga olib keladi.

Youngning tadqiqotlari, virtual tutqunlikning insonlar orasida shaxsiy va professional hayotning birlashishiga, shu bilan birga jiddiy psixologik muammolarni keltirib chiqarishiga sabab bo‘lishini ko‘rsatmoqda. Kuss va Griffiths (2017) o‘zlarining tadqiqotlarida, yoshlar orasida internetga bo‘lgan qaramlikning ortishini va bu holatning ularning ijtimoiy moslashuvi va o‘zaro munosabatlariga qanday ta’sir qilayotganini o‘rganganlar. Ular, ijtimoiy tarmoqlar va onlayn o‘yinlarga haddan tashqari qaramlikning yoshlarning o‘z-o‘zini anglashiga, o‘zlarining shaxsiy chegaralarini aniqlashga va umumiy ijtimoiy faolligiga salbiy ta’sirini ko‘rsatadi.

Joseph Reagle (2012) internetning ijtimoiy xavf va manfaatlarini muvozanatlashni ta’kidlaydi. U, internetning qulayliklari va imkoniyatlaridan foydalanish kerakligini, ammo shu bilan birga uning salbiy ta’sirlaridan ehtiyot bo‘lish zarurligini bildiradi. Reagle, texnologik inqiloblarning insonlar hayotiga olib kelgan yangi tahdidlarga qarshi kurashish uchun doimiy ravishda normativ asoslarni yangilab borish zarurligini ko‘rsatadi.

Howard Rheingold (2012) "Mind Amplifier" asarida, texnologiyalarni samarali va mas’uliyatli ishlatish zarurligini ta’kidlagan. Rheingold, odamlarning virtual dunyoga qaram bo‘lishi xavfini kamaytirish uchun, ular axborot xavfsizligi va shaxsiy ma’lumotlarni himoya qilish borasida ongli va bilimli bo‘lishlari kerakligini bildiradi. Uning so‘zlariga ko‘ra, shaxsiy va umumiy manfaatlar o‘rtasidagi balansni topish muhimdir. Brian S. T. (2018) virtual tutqunlikni ijtimoiy va huquqiy yondashuvda ko‘rib chiqadi.

U huquqiy normativlarning o‘zgarishiga urg‘u berib, hukumatlar, xususiy sektor va fuqarolik jamiyati o‘rtasida hamkorlikni ta’minlash zarurligini ta’kidlaydi. T.ning fikricha, ijtimoiy tarmoqlar va internet platformalarini nazorat qilishda davlat va jamoatchilikning birgalikda ishlashi muhimdir.

Xulosa

Virtual tahdidlarga qarshi kurashda huquqiy asoslarni mustahkamlash, kiberxavfsizlikni ta’minlash va shaxsiy ma’lumotlarni himoya qilish bugungi kunda dolzarb ahamiyat kasb etmoqda. O‘zbekiston Respublikasi ushbu yo‘nalishda qator qonun va qarorlarni qabul qilgan.

Jumladan, "Axborot xavfsizligi to‘g‘risida"gi qonun axborot resurslarining maxfiyligi, butunligi va mavjudligini kafolatlashga qaratilgan chora-tadbirlarni belgilaydi. Shaxsiy ma’lumotlarni himoya qilish, axborot tizimlarining xavfsizligini ta’minlash va kiberjinoyatlarga qarshi kurashda davlat va xususiy sektorning hamkorligi muhim ahamiyatga ega. Bundan tashqari, xodimlarning mas’uliyatini oshirish va nazorat mexanizmlarini kuchaytirish orqali axborot xavfsizligini ta’minlash bo‘yicha aniq vazifalar belgilangan. Ushbu chora-tadbirlar nafaqat milliy, balki xalqaro standartlarga mos keladigan kiberxavfsizlik tizimini shakllantirishga xizmat qiladi.

Natijada, virtual tahdidlarga qarshi kurashning huquqiy, texnik va tashkiliy asoslari mustahkamlanib, fuqarolarning huquq va erkinliklari himoya qilinadi.

REFERENCES

1. Turkle, Sh. (2011). Alone Together: Why We Expect More from Technology and Less from Each Other. Basic Books.
2. Young, K. S. (1998). Internet Addiction: The Emergence of a New Clinical Disorder. CyberPsychology & Behavior, 1(3), 237–244.
3. Kuss, D. J., & Griffiths, M. D. (2017). Social Networking Sites and Addiction: Ten Lessons Learned. International Journal of Environmental Research and Public Health, 14(3), 311.
4. Reagle, J. (2012). Reading the Comments: Likers, Haters, and Manipulators at the Bottom of the Web. MIT Press.
5. Rheingold, H. (2012). Mind Amplifier: The Future of Technology in Human Cognition. TEDx Talk.
6. Brian S. T. (2018). Social Media and the Law: The Role of Legislation in Protecting Privacy in the Digital Age. Law and Technology Journal, 32(1), 1-24.

7. Harris, R. K. (2016). Digital Addiction: The Problem of Online Compulsion. Journal of Digital Behavior, 12(2), 49-61.
8. Griffiths, M. D. (2013). Internet Addiction: A Critical Review. Journal of Psychology, 147(3), 1-17.
9. Howard, R. (2011). The Hyperconnected Society: The Future of Internet Addiction. Journal of Media Studies, 18(2), 55-62.
10. Tuffin, K., & Williams, R. (2018). Cyber Addiction and Its Impact on Society. Journal of Behavioral Science, 23(1), 27-40.