Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Cybersecurity, digital law and digital hygiene – an alternative solution to cybersecurity

Javlon ZOILBOEV[1]

Tashkent State University of law

ARTICLE INFO

Article history:
Received May 2021
Received in revised form
28 May 2022
Accepted 20 June 2022
Available online
25 July 2022

Keywords:
cybersecurity,
cybercrime,
digital law,
digital hygiene,
digital world,
digital court,
legal system,
legal policy.

ABSTRACT

Today, each of us uses modern smart devices that are connected wirelessly with the internet for our reading, work and other chores. Through phone, computer, smart watches, tablet and other gadgets, we find the necessary information to search the World Internet network. Also now new concepts have appeared and become popular in the legal system. This is the so-called "digital Law" and "digital hygiene". This article examines the origins, development, and current challenges and shortcomings of cybersecurity, digital law and digital hygiene, as well as the obstacles that exist in the world community. The first part analyzes the emergence of concepts and the penetration into the politics of states, the second part describes the current threats and circumstances, the problems are highlighted, the third part provides examples of solutions to the problems and important proposals and conceptions, doctrines that will be needed in the future. At the end of the article, the author explains his views, conclusions. Besides that the author used a new style in writing the article, in which each part analyzes the issues that are new, but a logical continuation of the subject studied in the previous part.

DOI: https://doi.org/10.47689/2181-1415-vol3-iss6/S-pp12-24

Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim

Kalit so'zlar:
kiberxavfsizlik,
kiberjinoyat,
raqamli huquq,

ANNOTATSIYA

Bugun har birimiz o'qishda, ishda va boshqa yumush-larimizni bajarishimiz uchun internet bilan simsiz va simli bog'langan holda zamonaviy aqlli qurilmalardan foydalanamiz.

[1] Teacher, Tashkent State University of law. E-mail: j.zoilboyev@tsul.uz.

raqamli gigiyena,
raqamli dunyo,
raqamli sud,
huquqiy tizim,
huquqiy siyosat.

Telefon, kompyuter, aqlli soatlar, planshet va boshqa gadjetlar orqali kerakli ma’lumotlarni jahon internet tarmog‘i orqali izlab topmoqdamiz. Shuningdek, huquq tizimida yangi tushunchalar paydo bo‘lib, ommlashmoqda. Bu, so‘zsiz, “raqamli huquq” va “raqamli gigiyena” hisoblanadi. Mazkur maqolada kiberxavf-sizlik, raqamli huquq va raqamli gigiyenaning kelib chiqishi, rivojlanishi va jahon ommasida hozirgi kunda mavjud muammo va kamchiliklar, to‘siqlar tahlil qilinadi. Birinchi qismda tushunchalarning vujudga kelishi hamda davlatlar siyosatiga kirib kelishi tahlil qilinsa, ikkinchi qismda hozirgi mavjud tahdidlar va holatlar bayon etiladi, muammolar yoritib beriladi, uchinchi qismda esa muammolarning yechimlari misollar bilan keltirilib, kelgusida kerak bo‘ladigan muhim taklif va konsep-siyalar, doktrinalar beriladi. Maqolaning so‘ngida esa muallif o‘z qarashlari, xulosalarini bayon etadi. Bundan tashqari, muallif maqolani yozishda yangicha uslub qo‘llagan bo‘lib, unda har bir qismda yangi, ammo oldingi qismda tadqiq qilingan mavzuning mantiqiy davomi bo‘lgan masalalarni tahlil qiladi.

Кибербезопасность, цифровое право и цифровая гигиена: альтернативное решение для борьбы с киберпреступностью

Ключевые слова:
кибербезопасность,
киберпреступность,
цифровое право,
цифровая гигиена,
цифровой мир,
цифровой суд,
правовая система,
правовая политика.

АННОТАЦИЯ

Сегодня каждый из нас для учебы, работы и других занятий используем современные интеллектуальные устройства, которые соединяются с интернетом по беспроводной и проводной связи. Через телефоны, компьютеры, умные часы, планшеты и другие гаджеты мы ищем нужную нам информацию во всемирной паутине. Также сейчас в правоведении появляются и становятся популярными новые понятия. Это буквально «цифровое право» и «цифровая гигиена». В этой статье будут рассмотрены проблемы и недостатки кибербезопасности, цифрового права и цифровой гигиены, а также проблемы и препятствия, с которыми сталкиваются мировые СМИ в настоящее время. В первой части анализируется возникновение концепций и их внедрение в политику государств, во второй части излагаются текущие угрозы и ситуации, освещаются проблемы, а в третьей части приводятся важные предложения и концепции, доктрины, необходимые в будущем, с примерами решений проблем. В конце статьи автор излагает свои взгляды, выводы. Также в статье будет приведен список использованной литературы. Также автор применил новую методику написания статьи, в которой в каждой части анализируются вопросы, являющиеся новым, но логическим продолжением исследуемой в предыдущей части темы.

Zamonaviy dunyoda har bir mezon turli darajada qimmatliklarga egaligi bilan ajralib turadi. Siz kompyuteringiz bilan internet tarmog‘i orqali qandaydir tadqiqot olib bormoqchimisiz? O‘zingizga bir savolni berishingiz kerak: bu muhit qanchalik xavfsiz va men o‘zimni qanday himoya qila olishim kerak? ***Steve Morgan***ning tadqiqotiga ko‘ra, “Agar alohida bir davlat deb qaraladigan bo‘lsa, kiberhujumlar va kiberjinoyatchilik 2021-yilda butun dunyo bo‘ylab 6 trillion AQSh dollariga teng miqdorda moddiy zarar yetkazganligini ta’kidlash joizdir. Bunda esa birgina kiberjinoyatchilikning ko‘lami butun AQSh va Xitoydan keyin dunyodagi uchinchi yirik iqtisodiyotga aylanadi”. Ko‘rinib turibdiki, jinoyatchilikning yangi va navqiron ko‘rinishi allaqachon jamiyat va davlatlar ildiziga chirmashib bo‘lgan. Shuningdek, kiberhujumlar va kiberjinoyatchilikning zararli ta’siri nafaqat iqtisodiyotga pasayish olib keladi, balki demografik o‘zgarishlar, inqirozlar, davlatlarning kiberxavfsizlikka haddan ortiq miqdorda byudjet mablag‘larining ajratishi kabi va buning natijasida ijtimoiy himoyaga muhtoj qatlamning moddiy ko‘maklarsiz qolib ketishiga olib keladigan misli his etilmagan salbiy yemirilishlar, tahdidlarni keltirib chiqaradi.

Bundan ham tahlikali jihati shundan iboratki, statistik ma’lumotlar evolyutsiyasiga ko‘ra, kiberjinoyatchilikning zararini baholash tarixiy ko‘rsatkichlarga asoslanadi, shu jumladan, so‘nggi yillardagi o‘sish, buyurtmachi davlatlar va uyushgan jinoiy guruhlar tomonidan homiylik qilingan xakerlik faoliyatining keskinortishi, yaqin kelgusi yillarda ro‘y berishi mumkin bo‘lgan hujumlar va ularning natijasida yuzaga keladigan zararlarning ko‘lami hozirgiga qaraganda bir necha barobar yirikroq bo‘lishini taxmin qilish qiyin emas. Buning sababi esa bu ko‘rinishdagi ijtimoiy xavfli qilmishlar o‘z ichiga ikki ko‘rinishdagi:

1. Mmoddiy:

– ma’lumotlarga zarar yetkazish yoxud ularning yo‘q qilinishi;

– moddiy-moliyaviy boylikning yo‘qotilishi;

– intellektual mulkning nobud bo‘lishi;

– firibgarlik;

– sud-tergov ma’lumotlarining yo‘qotilishi;

2. Ma’naviy-ruhiy:

– shaxsiy va moliyaviy ma’lumotlarning o‘g‘irlanishi;

– tadbirkorlikning va tashabbuskorlikning yo‘qotilishi;

– samaradorlik va mahsuldorlikning kamayishi;

– hujum natijasida olingan ma’lumotlarning yo‘qotilishi, shuningdek, uning oshkor etilishi natijasida shaxsga va uning obro‘siga zarar yetkazilishini qamrab oladi.

KIBERXAVFSIZLIK.

Nazariy-huquqiy tahlil.

Bugunga kelib, hayotning har bir jabhasi raqamlashmoqda, tug‘ilishdan tortib vafot etishgacha raqamli boshqaruv asosida hayot kechirmoqdamiz. Aholi demografiyasining o‘sishi hamda pasayishi, jinoyatchilik miqdorining harakatlanishi, valyuta qimmatliklarining harakatlari, onlayn savdo, shuningdek, masofaviy ta’lim, masofaviy boshqaruv kabilar shular jumlasidandir. Mazkur vositalar asosidagi hayot tarzi bizga beqiyos qulayliklar bermoqda, biroq bugun shaxsning qadrsizlanishi, shaxsiy ma’lumotlarning dunyo bo‘ylab tarqalib ketishi, firibgarlik qurboniga aylanishi har qachongidan osonlashmoqda. Buning tub sababi ham aynan raqamli dunyodir. 1995-yilda nashr etilgan M. Ethan Katshning “Raqamli dunyoda huquq” nomli kitobining kirish

qismida William Gates tomonidan bir jumla aytiladi: “Kelajakda barcha narsa raqamli bo‘ladi” **(Katsh, 1995).** Oradan 27 yil muddat o‘tdi hamki, mazkur fikrning tasdig‘ini ko‘rmoqdamiz. Yuqorida aytilganidek, har bir soha va hayotning har bir jabhasi raqamlashmoqda. www.datareportal.com sayti tomonidan taqdim etilgan ma’lumotlarga qaraganda, bugungi kunda dunyo bo‘ylab jami 5 milliard kishi internetdan foydalanmoqda – bu dunyo aholisining 63 foiziga teng demakdir. Xuddi shunday ma’lumot www.statista.com sayti tomonidan ham taqdim etilgan. Joseph Johnson ning tahlillariga ko‘ra, “2022-yil aprel oyida dunyo aholisining umumiy sonidan 4,65 milliard kishi ijtimoiy tarmoq foydalanuvchilari sanalishadi”. Internet foydalanuvchilari ham o‘sishda davom etmoqda, so‘nggi ma’lumotlar shuni ko‘rsatadiki, dunyodagi internet bilan bog‘langan aholi soni

2022-yil aprel oyigacha bo‘lgan 200 oy ichida deyarli 12 millionga o‘sdi. Bu esa aholining kundan kunga jahon intenet tarmog‘i bilan bog‘lanib borayotganligini anglatadi. Bu kabi statistik ma’lumotlar ijobiyligi sababli ham rivojlanish sari turtki bo‘la oladi. Biroq masalaning dolzarbligi aynan yuqoridagi ijobiy jihatlarda emasligini unutmaslik kerak.

Amaliy-nazariy tahlil.

Kiberhujumlar, kiberjinoyat, hakerliklarning zararli ta’siri raqamli dunyoda shaxsiy hayot xavfsizligini, shaxsiy ma’lumotlar daxlsizligi haqidagi qarashlarni tubdan o‘zgartirib yubordi. Hozirda biz tomonimizdan “yangi sanoat inqilobi” deb nomlanayotgan jarayon yangi jamiyatni, yangi muhitni taqdim etganligi bilan bir tomondan ijobiy ahamiyat kasb etsa, ikkinchi tomondan real xavfni ham keltirib chiqarmoqda. Misli ko‘rilmagan rivojlanishga qaramay, internet bizga qo‘rquvning yangicha ko‘rinishlarini, xavfning yangicha shakllarini olib keldi. Majir Yar va Kevin F.Steinmetzlarning fikriga ko‘ra, “Kibermakon, kompyuterlashtirilgan o‘zaro aloqalar va almashinuvlar sohasi jinoyatchilar va deviant faoliyat uchun juda ko‘p yangi imkoniyatlarni taqdim etadi **(Yar, Majid, and Kevin F. Steinmetz., 2019)**. Shuningdek, aksariyat manbalarda “kiberjinoyat” tushunchasi “kiberhujumlar”, “kompyuterda sodir etilgan jinoyatlar” yoki “kompyuter jinoyatlari” kabi nomlar bilan atalishi, Gudmen va Benner tomonidan XXI asrning boshidayoq ilgari surilgan edi **(Goodman, Brenner, 2002)**. Biroq mazkur tushunchalar bir xil ma’no-mazmun anglatmasligini aytib o‘tish joiz. Misol uchun, “kiberjinoyatchilik” atamasi kompyuter bilan bog‘liq jinoyatlarga qaraganda torroq tushunchani ifodalashi bilan ajralib turadi. Sababi, u faqatgina kompyuter tarmog‘ini o‘z ichiga olib, u bilan sodir etiladigan jinoiy qilmishlarni qamrab oladi. Kompyuterlar bilan bog‘liq jinoyatlar esa hatto tarmoq bilan hech qanday aloqasi bo‘lmagan, faqat shaxsiy kompyuter tizimlariga ta’sir qiladigan jinoyatlarni ham qamrab oladi **(Gercke, 2012)**. Kiberjinoyatchilik transmilliy jinoyatchilikning rivojlanayotgan shaklidir. Birlashgan Millatlar Tashkilotining Jinoyatchilikning oldini olish va huquqbuzarlarni profilaktika qilish bo‘yicha 10-Kongressida tegishli seminar doirasida raqamli texnologiyalar orqali sodir etiladigan jinoyatlar uchun ikkita asosiy ta’rif ishlab chiqilgan edi. Tor ma’noda, kiberjinoyatchilik (kompyuter jinoyati) bu kompyuter tizimlari xavfsizligining buzib kirilishi va aynan kompyuterlar tomonidan ma’lumotlarning g‘arazli maqsadlarda qayta ishlanib foydalanilishi tushuniladi. Kiberjinoyatchilik, keng ma’noda esa, (kompyuter bilan bog‘liq jinoyatlar) kompyuter tizimi yoki tarmog‘i orqali yoki aynan kompyuterga va raqamli tizimlarga nisbatan sodir etilgan har qanday noqonuniy xatti-harakatlarni, shu jumladan, kompyuter tizimi yoki tarmog‘i orqali noqonuniy egalik qilish va ma’lumotlarni taqdim etish yoki tarqatish kabi

jinoyatlarni qamrab oladi **(Patri, 2009)**. Kibermakonning chegarasiz hududida sodir bo‘ladigan jinoyatning murakkab tabiati uyushgan jinoyatchilik guruhlarining tobora ko‘payib borishi bilan murakkablashadi hamda mazkur omillarning ta’sirida jinoyatchilikning yangicha ko‘rinishi tobora xavflilik kasb etmoqda.

Kiberjinoyatchilar va ularning qurbonlari turli mintaqalarda joylashgan bo‘lishi mumkin va uning ta’siri butun dunyo bo‘ylab jamiyatlar orqali o‘tib, shoshilinch, dinamik va kompleks javob berish zarurligini taqozo etmoqda. Buning uchun esa eng muqobil yechim kiberxavfsizlikni kuchaytirish sifatida maydonga chiqdi. Hozirda barcha davlatlar tomonidan kiberxavfsizlikni rivojlantirishga qaratilgan chora-tadbirlar olib borilmoqda.

Kiberxavfsizlik qanday ta’minlanadi? Xalqaro tajribaning samarali yechimlari.

Kiberxafszlik nima, uni qanday qilib yaratish va ta’minlash mumkin? Kiberxavfsizlik tushunchasi bu raqamli muhitning turli xil tashqi xavflardan himoya, muhofaza etilishini anglatadi. Yanada aniqroq qilib aytganda, kiberxavfsizlik – bu kiber(raqamli) muhitni va tashkilot va foydalanuvchi aktivlarini himoya qilish uchun ishlatilishi mumkin bo‘lgan vositalar, siyosat, xavfsizlik tushunchalari, xavfsizlik kafolatlari, ko‘rsatmalar, xatarlarni boshqarish yondashuvlari, harakatlar, treninglar, eng yaxshi amaliyotlar, ishonch va texnologiyalar to‘plami. Unga tashkilot va foydalanuvchi aktivlariga ulangan hisoblash moslamalari, xodimlar, infratuzilma, dasturlar, xizmatlar, telekommunikatsiya tizimlari va kibermuhitda uzatiladigan va/yoki saqlanadigan ma’lumotlarning yig‘indisi kiradi. Kiberxavfsizlik tashkilot va foydalanuvchi aktivlarining xavfsizlik xususiyatlariga erishish va texnik xizmat ko‘rsatishni ta’minlashga intiladi.

Kiberxavfsizlik axborot texnologiyalarining doimiy rivojlanishida muhim rol o‘ynaydi. Internet xizmatlari kiberxavfsizlikni kuchaytirish va muhim axborot infratuzilmalarini himoya qilish har bir mamlakat xavfsizligi va iqtisodiy farovonligi uchun juda muhimdir. Internetni xavfsizroq qilish (va internet foydalanuvchilarini himoya qilish), yangi xizmatlarni rivojlantirish davlat siyosatining ajralmas qismiga aylandi **(Kellermann, 2014)**. Kiberjinoyatchilikni to‘xtatish milliy kiberxavfsizlik va muhim axborot infratuzilmasini himoya qilish strategiyasining ajralmas qismidir. Xususan, bunga AKTni jinoiy yoki boshqa maqsadlarda suiiste’mol qilishga qarshi tegishli qonunchilikni qabul qilish va milliy tanqidiy infratuzilmalar yaxlitligiga ta’sir ko‘rsatishga qaratilgan tadbirlar kiradi. Milliy darajada bu davlat organlari, xususiy sektor va fuqarolarning oldini olish, tayyorlash, javob berish va hodisalardan qutulish bilan bog‘liq muvofiqlashtirilgan harakatlarni talab qiladigan umumiy mas’uliyatdir. Mintaqaviy va xalqaro miqyosda bu tegishli sheriklar bilan hamkorlik va muvofiqlashtirishni talab qiladi. Kiberxavfsizlik uchun milliy asos va strategiyani shakllantirish hamda amalga oshirish keng qamrovli yondashuvni talab qiladi. Kiberxavfsizlik strategiyalari, masalan, kiberjinoyatchilik qurboniga aylanishining oldini olish uchun texnik himoya tizimlarini ishlab chiqish yoki foydalanuvchilarni o‘qitish kiberjinoyatchilik xavfini kamaytirishga yordam beradi. Kiberxavfsizlik strategiyasini ishlab chiqish va qo‘llab-quvvatlash kiberjinoyatchilikka qarshi kurashda muhim element hisoblanadi. Dunyoda mavjud analitik tashkilotlar hamda ishonchli statistik ba’za ma’lumotlari shuni ko‘rsatmoqdaki, hozirda davlatlar raqamli ma’lumotlarning xavfsizligini, ularning ishonchli himoya qilinishini ta’minlash uchun har yili davlat byudjeti xarajatlarini oshirib bormoqdalar. Misol uchun, bu ko‘rsatkich 2021-yilda Amerika Qo‘shma Shtatlari davlat byudjeti uchun qariyb 11 milliard dollarga tushganini alohida ta’kidlash joizdir. Quyida 10 ta davlat byudjetining qancha qismi kiberxavfslzilikni ta’minlashga ajratilayotganligi keltirilgan.

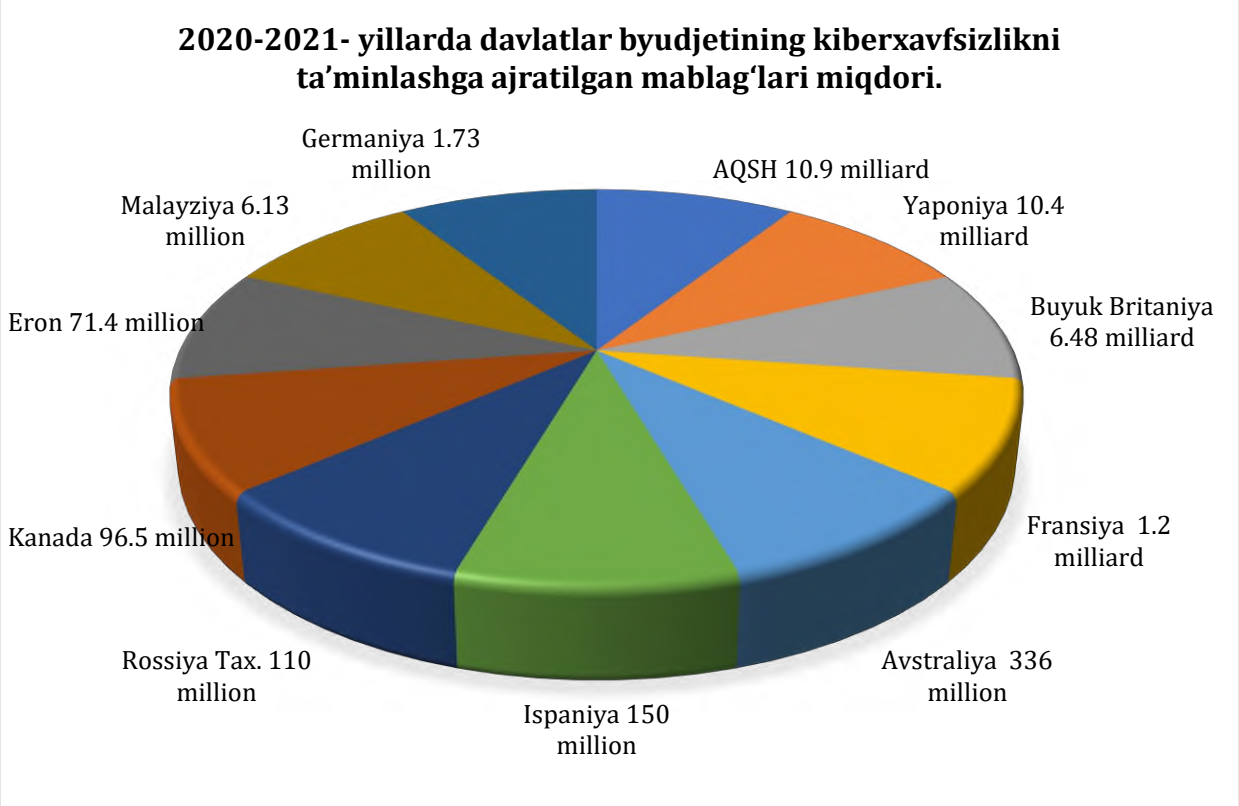
1-jadval.

2020-2022-yillarda davlatlar byudjetining kiberxavfsizlikni ta'minlashga ajratilgan mablag'lari miqdori.

№	Davlatlar	Kiberxavfsizlik uchun sarflanayotgan mablag' miqdori(AQSh dollarida)	Yil
1.	AQSh	10.9 milliard	2021
2.	Yaponiya	10.4 milliard	2020
3.	Buyuk Britaniya	6.48 milliard	2021
4.	Fransiya	1.2 milliard	2021
5.	Avstraliya	336 million	2021
6.	Ispaniya	150 million	2021
7.	Rossiya	Tax. 110 million	2021
8.	Kanada	96.5 million	2022
9.	Eron	71.4 million	2021
10.	Malayziya	6.13 million	2021
11.	Germaniya	1.73 million	2021

Ko'rinib turibdiki, 3 davlatda AQSh, Yaponiya hamda Buyuk Britaniyada kiberxavfsizlikni ta'minlash masalasi hamda unga ajratilayotgan mablag' miqdori yuqori.

Yuqorida aks ettirilgan jadvaldagi ma'lumotlar diagrammaga joylanganida, qaysi davlat tomonidan qanday miqdorda moliyaviy mablag'lar ajratilayotgan kiberxavfsizlik sohasi aks etganligini ko'rishimiz mumkin



Mazkur diagrammada aks etgan raqamlar faqatgina 2020–2021-yillarda qayd etilgan natijalar sanaladi. Undan tashqari, davlatlar tomonidan ikki yillik, uch yillik strategiyalar, rejalar ishlab chiqilgan bo‘lib, mazkur strategiyalarni amalga oshirish uchun moliyaviy mablag‘larni ajratish ko‘lami oshib bormoqda. Qo‘shimcha qilib aytganda, hozir faqat davlat tomonidan emas, balki xususiy subyektlar, investorlar, shuningdek, tadbirkorlik subyektlari ham o‘z bizneslarining xavfsizligini ta’minlashga doir bir qator chora-tadbirlarni amalga oshirmoqdalar. Raqamli transformatsiya tashabbuslarini har qachongidan ham tezroq amalga oshirish zarurati bilan qo‘llab-quvvatlangan korxonalar so‘nggi bir yil ichida mavjud mahsulotlarni yangilash va bulutga asoslangan yangi mahsulotlarni ishlab chiqish orqali onlayn xizmatlardan foydalanishni ikki barobarga oshirdi.

Bugunga kelib, xususiy sektor vakillari ham kiberxavfsizlik uchun chora-tadbirlar miqdori hamda ko‘lamini yanada oshirib bormoqdalar. Shu bilan birga, unga ajratilayotgan moddiy mablag‘larning miqdori ham yildan yilga oshib bormoqda. Misol uchun, quyidagi jadvaldan ham buni ko‘rishimiz mumkin bo‘ladi.

2-jadval.

Axborot xavfsizligi va xatarlarni boshqarish segmenti bo‘yicha oxirgi foydalanuvchi xarajatlari, 2020–2021 (million AQSh dollari).

№	Segment sohasi	2020	2021	O‘sish(%da)
1.	Dastur xavfsizligi	3.333	3.738	12.2
2.	Bulutli xavfsizlik	595	841	41.2
3.	Ma’lumotlar xavfsizligi	2.981	3.505	17.5
4.	Hisobga olish kartalariga kirishni boshqarish	12.036	13.917	15.6
5.	Infratuzilmani muhofaza qilish	20.462	23.903	16.8
6.	Integratsiyalashgan xatarlarni boshqarish	4.859	5.473	12.6
7.	Tarmoq xavfsizligi uskunalari	15.626	17.020	8.9
8.	Boshqa axborot xavfsizligi dasturlari	2.306	2.527	9.6
9.	Xavfsizlik xizmatlari	65.070	72.497	11.4
10.	Iste’molchilar xavfsizligi dasturi	6.507	6.990	7.4
	Jami	**133.776**	**150.409**	**12.4**

Ma’lum bo‘lmoqdaki, xususiy sektorda ham axborot xavfsizligini, kiberxavfsizlikni ta’minlashga doir jadal choralar ko‘rilmoqda. Eng yuqori moliyaviy ta’minot har ikki yilda ham xavfsizlik xizmatlarini ko‘rsatishga sarflangan. Biroq 2021-yilga kelib, umumiy o‘sish ko‘rsatkichi 12.4 foizni tashkil etganligini ko‘rishimiz mumkin.

Bir qator davlatlar tomonidan kiberxjinoyatchilikning oldini olish hamda unga qarshi kurashish uchun kiberxavfsizlikni mustahkamlash taklif etilayotgan paytda olimlar hamda bir necha mutasaddi tashkilotlar, shuningdek, ilmiy-jamoatchilik vakillari, avvalo, ikkita mezon, va ko‘nikma to‘g‘ri shakllantirilsa, singdirilsa, raqamli dunyoda xavfsiz yashash hamda ish samaradorligi orqali mehnatdan qoniqishga erishish mumkinligini ilgari suradilar. Bular **“raqamli huquq”** hamda **“raqamli gigiyena”**. Tadqiqotimizning kelgusi davomida mazkur tushunchalar haqida so‘z yuritamiz.

RAQAMLI HUQUQ.

“Ma’lumotni raqamlashtirish” **(Eric Hilgendorf, Jochen Feldle, 2018)** ma’lumotni nol va birliklar ketma-ketligi sifatida taqdim etishni anglatadi. Raqamli ma’lumotlarni tahrirlash, saqlash va kompyuterlar o‘rtasida osongina uzatish mumkin. Zamonaviy kompyuterlarning yuqori quvvatini va ularning global internet tarmog‘ini hisobga olgan holda, bu katta hajmdagi ma’lumotlarni real vaqt rejimida qayta ishlash, saqlash va uzatish mumkinligini anglatadi. Bu esa ma’lumotlarni raqamlashtirish demakdir. Demak, “raqamli” tushunchasi axborotning raqam ko‘rinishida ifodalanishi ekan. Bu yo‘l bilan esa, odatda, maxfiylik kasb etuvchi ma’lumotlar shifrlanadi, barchaga ma’lum bo‘lishidan saqlanadi. Endilikda huquq tushunchasiga to‘xtalsak, uzoq yillardan beri shakllanib kelayotgan tushunchalar huquqni anglash va talqin etishga ko‘mak beradi. Qonun nazorat vositasi sifatida **(Waldron J, E.N. Zalta, 2020)** XVIII asrdan beri o‘zining ichki tuzilishini shakllantirib, saqlab kelmoqda. Shuningdek, huquq bu “muayyan mamlakat yoki jamoa o‘z a’zolarining harakatlarini tartibga soluvchi va jazo qo‘llash orqali amalga oshirishi mumkin bo‘lgan qoidalar tizimi” sifatida ham bayon etiladi. Shuningdek, “qonun – bu inson xulq-atvori qoidalarni boshqarishga bo‘ysundirish korxonasi” sanalishini keltirish ham o‘rinlidir **(Austin, 1955)**. Undan tashqari, huquq – bu “xulq-atvorni shakllantirish, nizolarni hal qilish, huquqlarni ta’minlash va erkinliklarni himoya qilish, hatto adolatni ta’minlashga umid qiladigan jarayon” **(Katsh, 1995)** sifatida ta’rif etiladi. Bundan kelib chiqadiki, qonun bu jamiyatda yurish-turish tartibini belgilaydigan, davlat hokimiyati tomonidan ishlab chiqlishi va qo‘riqlanishi bilan alohida xususiyat kasb etadigan ijtimoiy jarayon sanaladi. Shuningdek, huquqni tadqiq etishda turli xil yondashuvlar ham mavjudki, mazkur yondashuvlar hamda qarashlar, huquq oilalari ta’sirida huquq “umumiy huquq” **(Packard, 2010)** va “kontinental huquq” kabi ulkan turlarga ajratiladi. Biroq biz so‘z yuritmoqchi bo‘lgan raqamli huquq esa yuqoridagi ikki oilani birlashtirdi desak, mubolag‘a bo‘lmaydi.

Insoniyat paydo bo‘lib, shaxslar jamoa bo‘lib yashay boshlaganidan buyon jamaiyat a’zolari o‘zlari tomonidan amalga oshiriladigan ayrim xatti-harakatlarni qoida tariqasida belgilab qo‘yganlar. Vaqtlar o‘tishi, zamonaviy texnika vositalarining hayotimizga kirib kelishi bilan, endilikda huquqning amalga oshirilishi hamda qo‘llanadigan sohalari ham o‘zgarib, kengayib bormoqda. Xususan, bugungi raqamli dunyoda “raqamli huquq” tushunchasi hayotimizga kirib keldi va ayni damda “kiberjinoyatlar”ga, onlayn huquqbuzarliklarga qarshi eng muqobil yechim sifatida “raqamli huquq”ni rivojlantirish raqamli kurash maydoniga chiqmoqda. Raqamli huquq o‘zi nima? Umumiy huquqdan qanday farqli jihatlari mavjud? Raqamli huquq bu axloqiy yoki axloqiy bo‘lmagan xatti-harakatlar uchun elektron javobgarlikni ifoda etuvchi zamonaviy tushuncha sifatida maydonga chiqmoqda. Shu bilan birga, raqamli huquq harakatlar va harakatlar uchun elektron javobgarlik sifatida belgilanadi. Buni boshqacha qilib ta’riflaydigan bo‘lsak, raqamli huquq internetdan foydalanish davomida ruxsat berilgan va foydalanish taqiqlangan amallarni anglatadi. Shuningdek, internetdan foydalanishning axloq mezoniga ko‘ra ikki turi farqlanib, axloqiy foydalanish jamiyatning qonunlariga mos keladigan internetdagi barcha ishlarni qamrab oladi. Axloqiy bo‘lmagan foydalanish jamiyatning qonunlariga mos kelmaydigan internetdagi barcha harakatlarni qamrab oladi. Avval ta’kidlanganidek, kiberxavfsizlik axborot texnologiyalari va internet xizmatlarining doimiy rivojlanishida muhim rol o‘ynaydi. Internetni xavfsizroq qilish (internet foydalanuvchilarini himoya qilish) hamda yangi xizmatlarni rivojlantirish hukumat siyosatining ajralmas qismiga aylanmoqda. Kiberxavfsizlik strategiyalari,

masalan, kiberjinoyatchilik qurboniga aylanishning oldini olish uchun texnik himoya tizimlarini ishlab chiqish yoki foydalanuvchilarni o‘qitish – kiberjinoyatchilik xavfini kamaytirishga yordam beradi. Aynan raqamli huquq ham ana shunday vositalardan eng muhimi hisoblanadi. Davlatning va xalqaro tashkilotlarning asosiy xatti-harakatlari konstitutsiyalar, qonunlar, xalqaro shartnomalar, qonunosti hujjatlarida aks etgan bo‘lsa, raqamli huquq ham huquqning bu manbalarini inkor etmagan holda mazkur huquqlarning zamonaviy texnika-texnologiyalar hamda internet jahon ommaviy tarmog‘ida amalga oshiriladigan ko‘rinishidir.

Iqtisodiy hamkorlik va taraqqiyot tashkiloti **(OECD)**, Osiyo-Tinch Okeani Iqtisodiy Hamkorlik Forumi **(APEC)** va Afrika Ittifoqi **(AU)** kabi xalqaro iqtisodiy tashkilotlar shaxsiy ma’lumotlarning transchegaraviy uzatilishi bilan bog‘liq maxfiyligi bo‘yicha o‘z ko‘rsatmalarini ishlab chiqdilar. Ushbu ko‘rsatmalar xalqaro savdoni rivojlantirish uchun xalqaro maxfiylik va ma’lumotlarni himoya qilish standartini yaratishga yordam beradi, lekin mazkur normalar ba’zi ishtirokchi mamlakatlarning ichki qonunlariga qaraganda zaifligi bilan ajralib turadi. Mazkur standartlarning eng asosiylaridan biri bu Yevropa Ittifoqi tomonidan 2016-yilda qabul qilingan “Shaxsiy ma’lumotlarni himoya qilishning umumiy qoidalari” hisoblanadi. Oddiy ijtimoiy munosabatlarda shaxsning shaxsiy huquqlari Konstitutsiya, qonunlar, qonunosti hujjatlari hamda xalqaro shartnomalarda nazarda tutilgan qoidalar bilan kundalik moddiy hayotda ro‘y beradigan ijtimoiy munosabatlarni tartibga soladi. Raqamli huquqda esa, xuddi shuningdek, Konstitutsiya, qonunlar, qonunosti hujjatlari hamda xalqaro shartnomalarda internetda amalga oshiriladigan xatti-harakatlarni amalga oshirish va boshqarish qonun-qoidalari, tartib-qoidalari belgilab beriladi. Misol uchun, O‘zbekiston Respublikasi Jinoyat kodeksining 97-moddasida “qasddan odam o‘ldirish” shaxsga qarshi jinoyat sanalsa, shaxsga doir ma’lumotlarni uning ruxsatisiz oshkor qilish, shuningdek, diniy materiallarni tayyorlash, saqlash va tarqatish ham jinoyat sanalishi belgilab qo‘yilgan. Mazkur normalar moddiy huquq normalari sanaladi. Raqamli huquq esa huquqning yangi bir sohasi sifatida zamonaviy texnika-texnologiyalar bilan bog‘liq ijtimoiy munosabatlarni tartibga solishga qaratilgan huquqiy normalar yig‘indisidir. Qoida tariqasida shuni aytish joizki, raqamli huquq bu – raqamli texnologiyalar vositasida yuzaga keladigan ijtimoiy munosabatlarni tartibga solishga qaratilgan, internet tarmog‘i foydalanuvchilarining o‘z xatti-harakatlari uchun javobgarlik darajasini belgilab beruvchi xulq-atvor qoidalalari yig‘indisi. Raqamli huquqqa misol sifatida dunyo aholisining qariyb 2 milliard 936 million aholisi tomonidan foydalanilayotgan Facebook ijtimoiy tarmog‘ining raqamli huquqiy me’yorlarini ko‘rib chiqamiz. https://transparency.fb.com saytining ma’lumotlariga ko‘ra, Facebook ijtimoiy tarmog‘idan foydalanuvchilar quyidagi sohalardagi huquqiy me’yorlarga amal qilishlari kerak bo‘ladi:

– haqiqiylik;
– xavfsizlik;
– maxfiylik;
– qadr-qimmat.

Haqiqiylik.

Facebook unda ko‘rilgan kontent haqiqiy ekanligiga ishonch hosil qilishni istaydi va shuni ta’minlashga harakat qiladi. Shuningdek, haqiqiylik ma’lumot almashish uchun yaxshi muhit yaratilganligini inobatga olib, Facebookdan foydalanadigan foydalanuvchilar kim ekanligi yoki ular nima qilayotgani haqida ma’lumotni buzish Facebook tomonidan qo‘llab-quvvatlanmaydi.

Xavfsizlik.

Facebook xavfsiz tarmoq bo‘lib, foydalanuvchilarning jismoniy xavfsizligiga zarar yetkazishi mumkin bo‘lgan kontent olib tashlanadi. Odamlarga tahdid soladigan, boshqalarni qo‘rqitishi, kamsitishi, haqorat qilishi mumkin bo‘lgan har qanday ma’lumot tarmoqdan o‘chiriladi.

Maxfiylik.

Facebook foydalanuvchilarning shaxsi hamda ma’lumotlarning maxfiyligini ta’minlaydi. Maxfiylik foydalanuvchilarga Facebookda qachon va qanday ma’lumotlarni ulashish hamda qaysi ma’lumotlarni ulashmaslik haqida mustaqil qaror qabul qilishni yaratib beradi.

Qadr-qimmat.

Facebookdan foydalanayotgan har bir foydalanuvchining qadr-qimmat va huquq erkinliklarida bir xillik kafolatlanadi. Shuningdek, har bir foydalanuvchi boshqalarning ham qadr-qimmatlarini hurmat qilishlarini ta’minlash choralarini ko‘radi.

Yuqorida keltirib o‘tilganlar Facebook ijtimoiy tarmog‘ining foydalanuvchi shartlari hisoblanadi. Undan tashqari, har bir foydalanuvchi amal qilishi kerak bo‘lgan muhim raqamli qoidalar ham mavjud. Xususan, foydalanuvchilar quyidagi mazmundagi materiallarni post sifatida qo‘yishlari taqiqlanadi:

– zo‘ravonlik va zo‘ravonlikni targ‘ib etuvchi materiallar;

– shafqatsizlik va diniy kamsitishlarni targ‘ib etuvchi materiallar;

– millatlararo ig‘volar tarqatuvchi, insoniyatga xavf tug‘diruvchi kontentlar.

Xulosa qilish mumkin bo‘ladiki, raqamli huquq bu moddiy huquqning zamonaviy texnologiyalarga tatbiq etiladigan ko‘rinishidir. Bunda esa asosiy e’tibor raqamli texnologiyalar orqali sodir etiladigan har qanday jinoyat yoki boshqa ijtimoiy xavfli qilmish uchun xuddi an’anaviy huquqda bo‘lgani kabi javobgarlik belgilanishiga qaratilishi darkor. Xususan, ommaviy axborot vositalari, ijtimoiy tarmoqlar orqali kishining sha’ni,qadr-qimmatiga yetkazilgan har qanday zarar qat’iy jazolanishi kerak. Undan tashqari, mualliflik huquqining har qanday ko‘rinishi muhofaza etilishi maqsadga muvofiq bo‘ladi.

RAQAMLI GIGIYENA NIMA VA U KIBERJINOYATCHILIKNING OLDINI OLA OLADIMI?

Gigiyena atamasini eshitishimiz bilan ko‘z oldimizga har kuni tongda turib, yuz-qo‘limizni yuvishimiz, tishlarimizni tozalashimiz, ozoda ust-bosh kiyishimiz kabi harakatlar majmui keladi. Bu amallar kishining sog‘ligi uchun asosiy protektor vazifasini o‘tab beradi. Ayni paytda ishga, o‘qishga yo‘l olishdan oldin esa qo‘limizdagi mobil aloqa vositasi orqali ijtimoiy tarmoqdagi profillarimizga kirib, undagi yangiliklar, bizga yo‘naltirilgan va bizga jo‘natilgan xabarlar bilan tanishib chiqamiz. **Endi bir o‘ylab qarang-a, siz mobil aloqa qurilmangizda va ijtimoiy tarmoqlarda o‘z shaxsiy gigiyenangizga amal qilasizmi?**

Raqamli gigiyena – biz kundalik turmushimizni ularsiz tasavvur qilolmaydigan ijtimoiy tarmoqlar hamda elekton qurilmalar, shuningdek, internet jahon tarmog‘idan xavfsiz foydalanish tartib-qoidalaridir. Ilmiy tomondan qaralganda esa, “raqamli gigiena odamlarni kiberxatarlarni minimallashtirish maqsadida muntazam ravishda raqamli amaliyotlarni bajarishga undovchi vositadir”. Ushbu atama ilk bor 1977-yil oktabr oyida James institutidagi ma’ruzalardan birida Suzan Sontag tomonidan qo‘llangan bo‘lib, harbiy yoki urush harakatlarida ishlatiladigan **“kiberxavfsizlik”**dan farqli o‘laroq, “raqamli xavfsizlik” shaxsning sog‘ligi bilan bog‘liq atamani anglatadi, ya’ni ijtimoiy olamdagi tom ma’nodagi sog‘ligini.

2014-yilda esa Tarmoq madaniyati instituti(INC) olimlari tomonidan **“raqamli gigiyena”** atamasining butun ilmiy-nazariy jihatlari yoritib berildi. Unga koʻra, “Raqamli transkodlash” deb nomlangan matnda Marianne van den Boomen “raqamli amaliyot” tushunchasini *“ijtimoiy ahamiyatga ega boʻlgan raqamli ramziy obyektlarni manipulyatsiya qilish, modifikatsiya qilish va loyihalashni oʻz ichiga olgan kundalik amaliyotlarning ketma-ket toʻplami*” sifatida izohlab berdi.

Demak, **“raqamli gigiyena”**ning kelib chiqishi yaqin oʻtmishga borib taqalar ekan, ijtimoiy tarmoqlardagi xavfsizligimizni ta’minlash uchun biz nimalarga amal qilishimiz kerak?

Birinchidan, “eshitaman va unutaman; koʻraman va eslayman; bajaraman va tushunaman” tamoyiliga (I hear, and forget. I see, and I remember. I do, and I understand) amal qilish koʻnikmasini shakllantirish zarur. Boisi shundan iboratki, har birimiz kundalik hayotimizda ijtimoiy tarmoqlardan foydalamiz. Deylik, sizda Facebook, Instagram yoki oddiygina Telegram messenjeri mavjud va siz ular orqali oʻz faoliyatingizni yuritasiz. Telegram messenjerida sizning shaxsiy ma’lumotlaringiz, fayllaringiz, oilangiz bilan hordiq chiqarishdagi suratlaringizni xavfsiz saqlash uchun siz bir necha bosqichli algoritmni amalga oshirishingiz kerak boʻladi. Bu algoritm **“ikki bosqichli tekshiruv”** deb nomlanadi. Bu himoya tizimini ishga tushirib, shaxsiy ma’lumotlaringiz himoyasini ta’minlashingiz uchun siz, albatta, uni oʻzingiz sinab koʻrishingiz kerak. Shundagina sizning ma’lumotlaringiz xavfsiz saqlanadi, har qanday ikkinchi odamning yordami bilan yaratilgan xavfsizlik tizimi oʻsha yordamchi shaxsning xavfini yuzaga keltiradi. Shunday ekan, “eshitaman va unutaman; koʻraman va eslayman; bajaraman va tushunaman” tamoyiliga amal qilish muhimdir.

Ikkinchidan, shaxsiy ma’lumotlaringizni xavfsiz saqlamaslik oqibatlari bilan yaxshilab tanishib qoʻyishingiz maqsadga muvofiq. Bu esa oʻz-oʻzidan sizda “raqamli gigiyena” nima ekanligi haqidagi tasavvurni va unga rioya qilish koʻnikmasini shakllantiradi.

Kibermuhitdagi xavfsizlik qoidalariga rioya qilmaslik va shaxsiy ma’lumotlarni himoyalamaslik quyidagi oqibatlarni keltirib chiqaradi:

– kompyuter, telefon, umuman olganda, **“gadjet”** ishdan chiqishi;

– boshqa qurilmalardan viruslar osongina oʻtishi va qurilmangizni bir arzmias buyumga aylantirib qoʻyish darajasida zararlashi xavfi yuzaga kelishi;

– qurilmaning qarovsiz qoldirilishi hamda undan ham ogʻir oqibat, unda saqlanayotgan siz uchun juda muhim **fayllarning** yoʻqotilishiga olib kelishi mumkin;

– kerakli ma’lumotlarning tiklanmaydigan darajada zararlanishi yoki yoʻqotilishiga olib kelishi;

– shaxsga doir ma’lumotlarning ochiqlanishi, tarqalishi, oshkor etilishi, buning natijasida esa “shaxsiy daxlsizlik huquqi”ning buzilishiga olib kelishi;

– yosh avlod, ayniqsa, sizning farzandingiz, oʻziga mos boʻlmagan ma’lumotlar bilan zaharlanishi;

– moliyaviy xavfsizlikning buzilishi hamda shaxsning faoliyatiga ta’sir etadigan xavflarning koʻpayishi va boshqalar.

“Raqamli gigiyena” shuni oʻrgatadiki, ma’lumotlar xavfsizligini ta’minlash uchun bir necha bosqichli nazoratni oʻrnatish shart. Xavfni profilaktika qilish uni bartaraf etishdan koʻra yaxshiroqdir.

Quyida eng yaxshi vosita va usullar keltirilgan:

1. Qurilmaning xavfsizlik jihatdan mustahkamligiga ishonch hosil qilish.

2. Doim himoyalangan tizimlardan foydalanish, masalan, himoyalanmagan Wi-Fi xavfsiz emasligini bilish zarur.

3. Kirayotgan saytlarining zararli emasligini saytiga kirishda oldinroq tekshirish.

4. Internetda fayllarni yuklab olayotganda xavfsizlik choralarini ko'rish.

5. Internetda berilgan har qanday "free" dasturlarni yuklab olishdan saqlanish, ular virus manbai bo'lish ehtimolidan xoli emasligini doim yodda tutish.

6. Har qanday holatda ham berilgan tashqi xotira qurilmalarini antivirusga tekshiruvdan o'tkazish.

7. Favqulodda paydo bo'luvchi ekran reklamalari va e'lonlaridan ehtiyot bo'lish kerakligini anglash.

8. Qurilmaning xavfsizligini ta'minlovchi rasmiy ilovalardan foydalanish.

9. Ijtimoiy tarmoqni real hayot sifatida tasavvur qilib, agar biror shubha uyg'otuvchi omil paydo bo'lganda, o'sha omilni tark etish ko'nikmasini shakllantirish.

10. Fayllarni muntazam tozalab turish.

Shunisi muhimki, sizning shaxsiy ma'lumotlaringizga xavf soluvchilar, avvalo, texnika ilmini mukammal egallagan shaxslardir. Shuningdek, ular o'qimishli va aniq harakat qiluvchidirlar. Bunga yaqqol misol qilib esa Skotsmen ismli yosh yigitchani keltirish mumkin. U 2002-yilda **"barcha vaqtlarning eng yirik harbiy xakerlik hujumi"**ni sodir etdi. Bir vaqtning o'zida Skotsmen 97 ta kompyuterlar tizimini buzib kira oldi (Bu tizim AQSh va NATO harbiy kuchlariga tegishli edi).

Umumiy xulosa qilib aytganda, bugungi juda ham tez harakatlanayotgan raqamli dunyoda, avvalo, shaxsning, shuningdek, ma'lumotlarning xavfsizligi amalga oshirilayotgan chora-tadbirlarning ko'lami hamda ta'sir darajasiga har jihatdan bog'liqdir. Yuqorida qayd etilganidek va tahlil qilinganidek, kiberjinoyatchilik jamiyat va davlatning eng xavfli dushmanidan biriga aylanmoqda. Unga qarshi kurashda esa eng samarali tizimlarni joriy etish, amaliyotga kiritish hamda integratsiyani kuchaytirish talab etilmoqda. Yana muhim jihat esa kiberxavfsizlik, raqamli huquq hamda raqamli gigiyenani shakllantirish, kundalik turmushning ajralmas qismiga aylantirish zamon talabi sifatida qayd etilmoqda.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Austin J. (1955). The Province of Jurisprudence Determined. Cambridge: Cambridge University Press.
2. Eric Hilgendorf, Jochen Feldle. (2018). Digitization and the Law. Wurzburg: Nomos.
3. Gercke D.M. (2012). Understanding cybercrime: phenomena, challenges and legal response. Geneva: International Telecommunication Union (ITU).
4. Goodman, Brenner. (2002). The emerging consensus on criminal conduct in cybercrime. International journal of law and information technology, 144.
5. Katsh M.E. (1995). Law in a digital world. London: Oxford University Press.
6. Kellermann. (2014). Technology risk chechlist, Cybercrime and Security. IIB-2.
7. Packard,A. (2010). Digital Media Law. Oxford: WILEY-BLACKWELL.
8. Patri A.K. (2009). Cyber Law. Lucknow.

9. Waldron J, E.N. Zalta. (2020). The Stanford Encyclopedia of Philosophy. Stanford: Stanford University.

10. Yar, Majid, and Kevin F. Steinmetz. (2019). Cybercrime and society. SAGE.

11. Steve Morgan “Cybersecurity Ventures” jamiyatining asoschisi hamda tadqiqotchisi hisoblanib, Cybersecurity Ventures asoschisi, “Cybercrime” jurnalining Bosh muharriri. va “Cybercrime Radio” da Ijrochi prodyuser. kiberjonoyatchgilik hamda kiberxavfsizlik mavzulariga oid qator ilmish ishlar muallifi sanaladi.

12. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybercrime%20costs%20include%20damage%20and,hacked%20data%20and%20systems%2C%20and

13. https://datareportal.com/global-digital-overview.

14. https://www.statista.com/aboutus/our-research-commitment/2210/joseph-johnson)

15. Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

16. Recommendation ITU-T X.1205 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

17. David Braue. Kiberxavfsizlik bo‘yicha qator tanlovlar go‘libi, shuningdek, ilmiy maqolalar yozuvchisi. https://www.linkedin.com/in/davidbraue/. Maqola nomi: Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025. Melburn, Avstraliya. Onlayn havola: https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

18. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. Stamford, Conn. May 17. 2021.

19. Digital Citizenship by Stephanie Miller is licensed under a Creative Commons Attribution NonCommercial-NoDerivs 3.0 Unported License.

20. https://www.oecd.org (Iqtisodiy hamkorlik va taraqqiyot tashkiloti)

21. https://www.apec.org (Osiyo tinch-okeani iqtisodiy hamkorlik tashkiloti)

22. https://au.int

23. General Data Protection Regulation. 2016. Onlayn: https://gdpr-info.eu/

24. O‘zbekiston Respublikasi Jinoyat kodeksining 97, 141-2 hamda 244-3 moddalari. Onlayn: https://lex.uz/docs/-111453

25. Maqolani onlayn o‘qish uchun havola: https://datareportal.com/essential-facebookstats#:~:text=Here’s%20what%20the%20latest%20data,)%3A%202.936%20billion%20(April%202022)&text=Number%20of%20people%20who%20use,)%3A%201.960%20billion%20(April%202022)

26. https://www.youtube.com/watch?v=6WC5ncbR0zQ

27. https://networkcultures.org/blog/2021/05/12/digital-hygiene/

28. Good Digital Hygiene: A guide to staying secure in cyberspace 1st edition © 2015 Ed Gelbstein & bookboon.com ISBN 978-87-403-0577-7. 15-b

29. https://www.androidcentral.com/how-activate-two-factor-authentication-telegram