УДК 378.147.004

Axrarov B.S., *p.f.f.d (PhD)*
“Zamonaviy axborot texnologiyalari” kafedrasi dotsenti
O‘zbekiston Davlat jahon tillari universiteti, Toshkent

KIBERXAVFSIZLIK ASOSLARINI O‘QITISH MASALALARI

Annotatsiya. Kiberxavfsizlik kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va ma'lumotlarni buzg‘unchilarning hujumlaridan himoya qilish usullari va amaliyotlari to‘plamidir. Kiberxavfsizlik asoslarini o‘qitish uchun alohida e’tibor berish kerak bo‘lgan kiberxavfsizlik komponentlari ajratib o‘tilib, ularning mazmun-mohiyati ochib berilgan. “Kiberxavfsizlik asoslari” fani bakalavriatning barcha yo‘nalishlarining o‘quv rejasiga kiritilishi haqida tavsiyalar berilgan.

Kalit so‘zlar: kiberxavfsizlik, kiberjinoyatchilik, kiberhujum, kiberterrorizm, axborot xavfsizligi, ilovalar xavfsizligi, tarmoq xavfsizligi, operatsion xavfsizlik, zarar yetkazuvchi dasturlar, viruslar, troyan dasturlari. josus dasturlar, tovlamachi dasturlar, bakalariat yo‘nalishlari.

Akhrarov B.S., *Doctor of Philosophy in Pedagogical Sciences (PhD)*
Associate Professor of the Department of Modern Information Technologies of the Uzbek State University of World Languages, Tashkent

CYBERSECURITY BASICS TRAINING ISSUES

Abstract: Cybersecurity is a set of methods and practices for protecting computers, servers, mobile devices, electronic systems, networks, and data from attackers. The components of cybersecurity that require special attention when teaching the basics of cybersecurity are highlighted, and their content and essence are explained. It is recommended to include the subject “Fundamentals of Cybersecurity” in the curriculum of all bachelor's degree programs.

Keywords: cybersecurity, cybercrime, cyberattack, cyberterrorism, information security, application security, network security, operational security, malware, viruses, Trojan horses. spyware, ransomware, undergraduate courses.

Jamiyatimiz taraqqiyotining hozirgi bosqichida axborot-kommunikatsiya texnologiyalari muhim o‘rin tutmoqda. Aholi farovonligini yanada oshirish, mamlakatning iqtisodiy barqarorligini mustahkamlashning muhim omili sifatida aloqa, axborotlashtirish va telekommunikatsiya texnologiyalarini rivojlantirish O‘zbekiston hukumati siyosatining ustuvor vazifalari qatoriga kiradi. Mazkur vazifalarning mohiyati, maqsadi va istiqboldagi rivoji O‘zbekiston Respublikasi Prezidenti tomonidan 2020-yil 5-oktabrda qabul qilingan “Raqamli O‘zbekiston-2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmonida ham o‘z ifodasini topdi. Ushbu Farmonga muvofiq, raqamli infratuzilmani, elektron hukumatni, raqamli iqtisodiyotni, raqamli texnologiyalar milliy bozorini rivojlantirishning, axborot texnologiyalari sohasida ta’lim berish va malaka oshirishning ustuvor yo‘nalishlari belgilangan. Strategiyaning maqsadi - iqtisodiyot tarmoqlari, ijtimoiy soha va davlat boshqaruvi tizimining jadal raqamli rivojlanishini ta’minlash, shu jumladan elektron davlat xizmatlarini ko‘rsatish mexanizmlarini yanada takomillashtirishdan iborat [1].

O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyev ta’kidlaganidek, “Iqtisodiyotimizning barqarorligi, barcha sohalarning sifatli va samarali ishlashi, aholi hayotining qulayligi axborot texnologiyalariga bog‘liq. Shuning uchun ushbu soha uchun yanada keng imkoniyatlarni, zarur infratuzilmani yaratish, mutaxassislarni rag‘batlantirish, qobiliyatli yoshlarni tarbiyalash kerak.” [2]. Shu ma’noda oliy ta’lim tizimida axborot madaniyati yuqori darajada shakllangan malakali kadrlarni tayyorlashda ularda kiberxavfsizlik asoslari, shu jumladan, axborot xavfsizligini ta’minlashga oid bilim, malaka va ko‘nikmalarni rivojlantirish dolzarb masalalardan hisoblanadi .

Dunyo miqyosida kiberxavfsizlikni ta’minlash barcha mamlakatlar uchun iqtisodiyotni rivojlantirish, jamiyat farovonligini ta’minlash garovi bo‘lib qolmoqda.

Bozor va iste’molchilar ma’lumotlariga ixtisoslashgan Germaniyaning nufuzli Statista's Market Insights kompaniyasi ma’lumotlariga ko‘ra, 2024 yilda dunyo miqyosida kiberjinoyatlar natijasida ko‘rilgan zarar miqdori 9,22 trillion dollarni tashkil etgan. Ushbu miqdor 2028-yilga kelib 13,82 trillion dollargacha oshishi kutilmoqda [3].

Gartner tadqiqot kompaniyasi (axborot texnologiyalari bozoriga ixtisoslashgan Amerika tadqiqot va konsalting kompaniyasi) ekspertlari kiberxavfsizlik biznes rivojlanishi uchun juda muhimligini e’tirof etganlar. Kompaniya analitiklari 2024-yilning iyun oyidan noyabrigacha turli mamlakatlardagi 456 kompaniya rahbarlari o‘rtasida o‘tkazilgan so‘rovnoma natijalarini tahlil qilib, shunday xulosaga kelishgan. Olingan ma’lumotlarga ko‘ra, respondentlarning 85 foizi kiberxavfsizlik muhimligiga ishonchlari komil bo‘lgan. So‘rovnoma natijalari shuningdek, biznes rahbarlarining 61 foizi kibertahdidlardan xavotirda ekanliklarini ko‘rsatdi. Ushbu holat asosan hozirgi biznes jarayonlarida sun’iy intellektning ortib borayotgan roli, shuningdek, takomillashayotgan texnologiyalarni izlab topish va ularni amaliyotga joriy etish bilan bog‘liq. Qaltisliklar, xavf-xatar chegaralari o‘zgargan sari respondentlar kiberxavfsizlikni o‘z tashkilotlari muvaffaqiyatining muhim omili sifatida e’tirof etganlar [4].

Gartner hisob-kitoblariga ko‘ra, 2025 yilgacha foydalanuvchilarning kiberxavfsizlik bo‘yicha global xarajatlari yiliga 15 foizdan ko‘proq o‘sib, 212 milliard dollarga yetadi.

Ushbu o‘sishning katta qismi sun’iy intellektning o‘sishi va xususan, generativ sun’iy intellekt (GenAI) bilan bog‘liq bo‘lib, ilovalar xavfsizligi, ma’lumotlarni himoya qilish, maxfiylik va tarmoq infratuzilmasi xavfsizligiga investitsiyalarni jalb qiladi. Generativ sun’iy intellekt (GenAI) - trening davomida o‘rganilgan ma’lumotlar asosida yangi ma’lumotlarni yaratish uchun foydalaniladigan neyron tarmoq turi. Bunday neyron tarmoqlar tasvirlar, matnlar, audio va videolar, tushunchalar va boshqa turdagi tarkiblarni yaratishi mumkin.

Gartner prognozlariga ko‘ra, 2027 yilga kelib, kiberhujumlar yoki ma’lumotlar yaxlitligi buzilishining 17 foizi GenAIning qandaydir ko‘rinishini o‘z ichiga oladi. Biroq, yangi texnologiyalarga asoslangan kiberhujumlar ko‘lami ham oshib borishi mumkin [5].

2007-yil 25-dekabrda “Axborotlashtirish va ma’lumotlarni uzatish sohasida qonunga hilof harakatlarni sodir etganlik uchun javobgarlik kuchaytirilganligi munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi O‘RQ-137-son Qonuni 1-moddasiga ko‘ra, O‘zbekiston Respublikasi Jinoyat Kodeksining «***Axborotlashtirish qoidalarini buzish***» nomli 174-moddasi chiqarib tashlandi va uning o‘rniga «***Axborot texnologiyasi sohasidagi jinoyatlar***» nomli 6 moddadan iborat yangi **XX^1 bob** kiritildi. Keyinchalik jahon iqtisodiyoti hamda siyosatiga ta’sir qilib kelayotgan axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashishni kuchaytirish maqsadida O‘zbekiston Respublikasining 2019-yil 3-dekabrdagi O‘RQ-586-sonli Qonuni hamda 2024-yil 19-yanvardagi O‘RQ-899-sonli Qonuniga asosan Jinoyat Kodeksining **XX^1 bobi** 9 moddadan iborat yangi tahrirda qabul qilindi [6].

Qonunchilik palatasi tomonidan 2022-yil 25-fevralida qabul qilingan, hamda 2022-yil 17-martda Senat tomonidan ma’qullangan “Kiberxavfsizlik to‘g‘risida”gi qonun Prezident tomonidan 2022-yil 15-aprelda O‘RQ–764-son bilan tasdiqlandi. Ushbu qonunning asosiy maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat. Qonunda kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilish davlatning kiberxavfsizligini ta’minlashda ustuvor hisoblanishi belgilangan [7].

Hozirgi kunda mamlakatimizda "Kiberxavfsizlik markazi" davlat unitar korxonasi. O‘zbekiston Respublikasi Prezidentining 2019-yil 14-sentabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida"gi PQ-4452-son qaroriga muvofiq faoliyat yuritib kelmoqda.

Kiberxavfsizlik asosan uch turdagi tahdidlarga qarshi kurashadi.

Kiberjinoyatchilik - axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi. Boshqacha qilib aytganda, kiberjinoyat - bu bir yoki bir nechta yovuz niyatli shaxslar tomonidan tizimga hujum qilish, uning faoliyatini buzish yoki moliyaviy foyda olish maqsadida uyushtirilgan harakatdir.

Kiberhujum kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat.

Kiberterrorizm qo‘rquv yoki vahima qo‘zg‘ash uchun elektron tizimlarni beqarorlashtirishga yo‘naltirilgan harakatidir.

Kiberxavfsizlik masalalarini o‘qitishda uning quyidagi komponentlarini hisobga olish muhim:

1. ***Axborot xavfsizligi*** – shaxs, jamiyat va davlat hayotiy manfaatlarining axborot sohasidagi buzg‘unchi ta’sir tahdidlaridan himoyalanganlik holati [6, 10 b.]. Axborot xavsizligida ma’lumotlarni saqlash, uzatish jarayonida ularning ochiqligi, yaxlitligi va maxfiyligini ta’minlash muhimdir.

Axborotga ochiqligini (unda erkin foydalanish imkoniyatini) ta’minlash - belgilangan vaqt oralig‘ida vakolatga ega bo‘lgan axborot foydalanuvchilari va sub’ektlari uchun axborot yoki u bilan bog‘liq servisga murojaat qilib foydalanish imkoniyatini ta’minlashni anglatadi.

Axborotning yaxlitligini ta’minlash- saqlanayotgan axborot vakolatga ega bo‘lmagan sub’ektlar tomonidan o‘zgartirilishidan, ya’ni axborot tuzilishi va ma’nosi qanday berilgan bo‘lsa, shunday saqlashni ta’minlashni anglatadi.

Axborotning maxfiyligini ta’minlash - axborotga vakolati bo‘lmagan sub’ektlar tomonidan murojaat qilib, undan oshkor holda foydalanishdan himoya qilishni anglatadi

2. ***Ilovalar xavfsizligi*** – elektron qurilmalarda o‘rnatilgan dasturlarda kiberjinoyatchilar yashirishi mumkin bo‘lgan tahdidlardan himoya qilish. Zararlangan

ilova buzg‘unchiga himoyalanishi kerak bo‘lgan maxfiy ma'lumotlarga kirishi uchun ruxsat berishi mumkin. Ilovaning xavfsizligi uni ishlab chiqish bosqichida, ochiq manbalarda paydo bo‘lishidan ancha oldin ta’minlanadi.

3. ***Tarmoq xavfsizligi*** - bu kompyuter tarmoqlarini maqsadli hujumlar yoki zarar yetkazuvchi dasturlar kabi turli tahdidlardan himoya qilish jarayoni.

4. ***Operatsion xavfsizlik*** - axborot resurslari bilan ishlash va ularni himoya qilish. Ushbu guruhga, masalan, tarmoqqa kirish ruxsatlarini yoki ma’lumotlarning qayerda va qanday saqlanishi va uzatilishini belgilaydigan qoidalarni boshqarish kiradi.

5. ***Favqulodda vaziyatlarda tiklash va axborot tizimi ishining uzluksizligini ta’minlash*** - xavfsizlik hodisalariga (buzg‘unchilar faoliyati) yoki tizimning buzilishi yoki ma’lumotlar yo‘q qilinishi yoki o‘g‘irlanishiga olib keladigan boshqa hodisalarga munosabat bildirish. Favqulodda vaziyatlarda tiklash - tashkilot hujum oqibatlarini qanday hal qilishini va biznes jarayonlarini tiklashini tavsiflovchi qoidalar to‘plami. Biznesning uzluksizligi - buzg‘unchilar tomonidan uyushtirilgan hujum tufayli tashkilot ma’lum resurslardan foydalanish imkoniyatini yo‘qotgan taqdirda harakat rejasi.

6. ***Xabardorlikni oshirish*** - foydalanuvchilarni o‘qitish. Ushbu yo‘nalish kiberxavfsizlik sohasidagi eng oldindan aytib bo‘lmaydigan omil - inson omilining ta’sirini kamaytirishga yordam beradi. Hatto eng xavfsiz tizim ham kimningdir xatosi yoki mas’uliyatsizligi tufayli xavfsizligining buzilishiga olib kelishi mumkin. Shuning uchun har bir tashkilot xodimlar uchun seminar-treninglar o‘tkazishi va ular asosiy qoidalardan iborat xavfsizlik siyosati haqida ma’lumotlar bilan tanishtirilishi kerak: masalan, ular elektron pochta xatlariga biriktirilgan shubhali fayllarni ochmasliklari yoki shubhali USB qurilmalariga ulanmasliklari kerak.

Ma’lumotlarning sizib chiqishiga (ruxsatsiz tarqalishi) ko‘pincha moliyaviy, davlat yoki chakana savdo tashkilotlari duchor bo‘ladilar. Buzg‘unchilar, shuningdek, shaxsiy ma’lumotlarini o‘g‘irlaydilar. Shaxsiy ma’lumotlarni o‘g'irlash ham jismoniy shaxslarga, ham tashkilotlarga katta zarar keltiradi. Aksariyat hollarda buning sababi

kiberjinoyatchilarning harakatlari bilan bog‘liq. Ayrim tashkilotlar buzg‘unchilarni aniq bir sababga ko‘ra o‘zlariga jalb qiladilar: ular moliyaviy va shaxsiy ma’lumotlari qo‘lga kiritish maqsadida reja asosida ish ko‘radilar. Biroq, har qanday kompaniya buzg‘unchilar nishoniga aylanishi mumkin, chunki kiberjinoyatchilar o‘z manfaatlari yo‘lida mijozlar ma’lumotlarini qo‘lga kiritish maqsadida turli usul va vositalarni qo‘llaydilar: kuzatishlari, josuslik qilishlari yoki kiberhujum uyushtirishlari mumkin.

Qanday qilib buzg‘unchilar kompyuter tizimlari ustidan nazoratni qo‘lga kiritadilar? Ular turli xil vositalar va usullardan foydalanadilar.

Zarar yetkazuvchi dasturiy ta’minot kiberjinoyatchilar tomonidan qo‘llaniladigan eng keng tarqalgan vositadir. Ular foydalanuvchining kompyuteriga va undagi ma’lumotlarga zarar yetkazish yoki ularni o‘chirish maqsadida yaratiladilar. Zarar etkazuvchi dasturlar ko‘pincha foydali fayllar niqobi ostida yoki elektron pochta xatlariga biriktirilgan fayllar orqali tarqatiladilar. Kiberjinoyatchilar ulardan pul ishlash yoki g‘arazli maqsadlardagi hujumlarni amalga oshirish uchun foydalanadilar.

Zarar yetkazuvchi dasturlar turli shakllarda bo‘lishi mumkin, ularning keng tarqalgan turlari quyidagilar:

Viruslar (Viruses)– ular shunday dasturlarki, boshqa dasturlarga joriy etilib, zararlangan fayllarni ishga tushirishni boshqarish maqsadida ularga o‘zlarining zarar yetkazuvchi kodlarini kiritadilar. Kompyuter tizimida tarqalish uchun ular o‘zlarini nusxalarini yaratadilar.

Troyan dasturlari (Trojan programs) - foydali dasturiy ta’minot niqobi ostida yashiringan zarar yetkazuvchi dasturlar. Ular suqilib kirgan kompyuterda foydalanuvchining ruxsatisiz ma’lum amallarni bajarishga kirishadilar, ya’ni ma’lum sharoitlarda diskdagi ma’lumotlarni o‘chiradilar, tizimning “osilib” qolishiga olib keladilar, maxfiy axborotlarni o‘g‘irlaydilar va xokazo. Asosan troyan dasturlari kiberjinoyatchilar tomonidan “foydali” dastur sifatida tarmoq orqali tarqatiladilar va keyin ma’lumotlarni yig‘adilar yoki ularga zarar yetkazadilar.

Josus dasturlar (Spyware) - foydalanuvchining harakatlarini yashirincha kuzatib boruvchi va ma'lumotlarni (masalan, kredit karta ma’lumotlari) to‘playdigan

dasturiy ta’minot. Keyinchalik kiberjinoyatchilar to‘plangan ma’lumotlardan o'z maqsadlari uchun foydalanishlari mumkin.

Tovlamachi dasturlar (Ransomware) – ular tizimdagi fayllar va ma’lumotlarni shifrlaydilar. Kiberjinoyatchilar, foydalanuvchi o‘z ma’lumotlarini yo‘qotishlari mumkinligiga ishora qilib, ularni tiklab berish uchun to‘lov talab qiladilar.

Kiberjinoyatchilar ayniqsa tarmoq serverlariga kiberhujumlar uyushtirib, tarmoq tizimining normal holda ishlashiga to‘sqinlik qilishlari, hattoki yaroqsiz holga kelishiga sababchi bo‘lishlari mumkin. Masalan, ular muhim infratuzilma komponentlariga zarar etkazishlarii va tashkilot faoliyatini sabotaj qilishlari ham mumkin.

Dunyo ta’lim tizimi taraqqiyotida raqamli iqtisodiyotni rivojlantirish, unda joriy etilayotgan axborot tizimlaridan kiberxavfsizlikni ta’minlagan holda samarali foydalanish hamda axborot madaniyati shakllangan kadrlarni tayyorlash masalalari tobora muhim ahamiyat kasb etmoqda. Rivojlangan mamlakatlar ta’lim tizimida sohalardagi axborot tizimlaridan foydalanuvchi bo‘lajak kadrlarga kiberxavfsizlikni ta’minlash masalalari o‘qitilmoqda. Hozirgi paytda mamlakatimiz oliy ta’lim tizimida kiberxavfsizlik asoslariga oid maxsus kurslar umumkasbiy fanlar sifatida axborot xavfsizligi va turdosh yo‘nalishlarda ta’lim olayotgan talabalarga o‘qitilishi yo‘lga qo‘yilgan. Nomutaxassislik yo‘nalishlari bo‘yicha ushbu kurs mavzulari qisman “Axborot texnologiyalari” fani tarkibida o‘qitilmoqda.

Axborot-kommunikatsiya tizimlarining keng qo‘lamdagi foydalanuvchilari bo‘lgan nomutaxassislik yo‘nalishlari (shu jumladan filologiya va tillarni o‘qitish, xalqaro jurnalistila, sotsiologiya va shu kabi boshqa yo‘nalishlar) uchun kiberxavfsizlik masalalari “Axborot texnologiyalari”, “Axborot texnologiyalarini sohada qo‘llash” fanlari tarkibida o‘qitilishi, ya’ni, ushbu fanlar o‘quv dasturlarida kiberxavfsizlik asoslariga oid mavzular uchun soatlar taqsimoti turlichaligi, amaliy mashg‘ulotlari uchun ajratilgan soatlarning tanqisligi talabalar tomonidan zarur bilimlarni o‘zlashtirish imkonini cheklaydi. Shu bilan birga nomutaxassisliklari yo‘nalishlari xususiyatlari va ta’lim oluvchi talabalarning psixofiziologik

xususiyatlarini hisobga olgan holda o‘quv materiallarini yaratish zarurati muammo bo‘lib qolmoqda. Ayniqsa, bugungi kunda sohalarda joriy etilayotgan axborot tizimlari va texnologiyalari tashkil etuvchilariga nisbatan bo‘ladigan tahdidlar, ulardagi zaifliklar kutilayotgan samaradorlikka salbiy ta’sir ko‘rsatmoqda. Bunday tizimlar va texnologiyalar foydalanuvchilarida kiberxavfsizlik asoslariga oid tegishli bilim, malaka va ko‘nikmalar yetishmasligi sohani zamonaviy axborot-kommunikatsiya tizimlari va texnologiyalari asosida rivojlantirish yo‘lida jiddiy to‘siq bo‘lmoqda.

Oliy ta’lim tizimi bakalavriat yo‘nalishida ta’lim olayotgan talabalarni kiberxavfsizlik komponentlari: odamlar, axborot tizimlari majmui, shu jumladan muhim axborot infratuzilmasi obyektlari, tarmoqlar va texnologik jarayonlar resurslarining majmui, kiberxavfsizlik tahdidlari, kiberjinoyatlar va kiberhuquq, kiberxavfsizlik tahdidlaridan himoyalanish asoslari bilan tanishtirish, shu jumladan ularga kompyuter tizimida, elektron qurilmalarda, global tarmoqlarda, bulutli xizmatlarda xavfsiz ishlash usullarini o‘rgatish muhimdir. Buning uchun kiberxavfsizlik masalalarini innovatsion yondashuvlarga asoslangan ilg‘or ta’lim texnologiyalari, sifatli metodik ta’minot asosida o‘qitish yo‘lga qo‘yilishi yuqori samara beradi.

Shuning uchun “Kiberxavfsizlik asoslari” fan sifatida bakalavriatning barcha yo‘nalishlari o‘quv rejasiga kiritilishi maqsadga muvofiq bo‘lar edi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidentining 2020 yil 5 oktabrdagi “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmoni. Qonun hujjatlari ma’lumotlari milliy bazasi, 06.10.2020 y., 06/20/6079/1349-son.

2. O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyevning 2019-yil 20 noyabrda Toshkentning Mirzo Ulug‘bek tumanidagi Dasturiy mahsulotlar va axborot texnologiyalari texnologik parkiga tashrifida nutqi. Manba - https://qalampir.uz/uz/news/mirziyeev-it-park-ning-k-urilishiga-start-berdi-10920

3. https://worldmarketstudies.ru/article/userb-ot-kiberprestuplenij-vyrastet-na-tret-za-sleduusie-4-goda/

4. https://www.gartner.com/en/newsroom/press-releases/2025-04-22-gartner-survey-finds-85-percent-of-ceos-say-cybersecurity-is-critical-for-business-growth

5. https://www.itweek.ru/security/article/detail.php?ID=2303190

6. O‘zbekiston Respublikasining Jinoyat Kodeksi. https://lex.uz/docs/-111453

7. O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni. https://lex.uz/docs/-5960604

8. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.