KIBERJINOYATLARNING VUJUDGA KELISH VA SHAKLLANISH BOSQICHLARI

Ergashova Ma'mura Amangeldi qizi

O'zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi magistranti

Annotatsiya. *Kiberjinoyatlar zamonaviy axborot-kommunikatsiya texnologiyalari rivojlanishi bilan paydo bo'lgan va tobora murakkablashib borayotgan global muammolardan biridir. Ushbu tezisda kiberjinoyatlarning vujudga kelish sabablari, tarixiy shakllanish bosqichlari hamda ularning turli shakl va ko'rinishlari o'rganiladi. Tadqiqotda kiberjinoyatlarning dastlabki oddiy xakerlik amaliyotlaridan boshlab, bugungi kunning murakkab kiberhujumlari, jumladan, moliyaviy firibgarliklar, ma'lumotlarni o'g'irlash, kiberterrorizm va boshqa shakllarigacha bo'lgan jarayon yoritiladi. Shuningdek, xalqaro va milliy miqyosda kiberjinoyatlarga qarshi kurashish bo'yicha qabul qilingan huquqiy-me'yoriy hujjatlar, xalqaro hamkorlikning o'rni ham ko'rib chiqilgan.*

Kalit so'zlar: *kiberjinoyatlar, axborot xavfsizligi, xakerlik, kiberhujumlar, kiberterrorizm, xalqaro hamkorlik, huquqiy-me'yoriy hujjatlar, texnologik xavfsizlik, internet xavfsizligi, kiberjinoyatlarning oldini olish.*

Аннотация. *Киберпреступность — одна из глобальных проблем, возникшая с развитием современных информационно-коммуникационных технологий и становящаяся все более сложной. В диссертации рассматриваются причины возникновения киберпреступности, этапы ее исторического развития, а также различные ее формы и проявления. Исследование охватывает эволюцию киберпреступности — от самых ранних простых хакерских практик до современных сложных кибератак, включая финансовое мошенничество, кражу данных, кибертерроризм и другие формы. Также были рассмотрены правовые и нормативные документы, принятые на международном и национальном уровнях для борьбы с киберпреступностью, а также роль международного сотрудничества.*

Ключевые слова: *киберпреступность, информационная безопасность, хакерство, кибератаки, кибертерроризм, международное сотрудничество, нормативно-правовые документы, технологическая безопасность, интернет-безопасность, предотвращение киберпреступности.*

Annotation. *Cybercrime is one of the global problems that has emerged with the development of modern information and communication technologies and is becoming increasingly complex. This thesis examines the causes of cybercrime, the stages of its historical formation, and their various forms and manifestations. The study covers the process of cybercrime, from the initial simple hacking practices to today's complex cyberattacks, including financial fraud, data theft, cyberterrorism, and other forms. It*

also examines the legal and regulatory documents adopted at the international and national levels to combat cybercrime, and the role of international cooperation.

Key words: *cybercrime, information security, hacking, cyberattacks, cyberterrorism, international cooperation, legal and regulatory documents, technological security, internet security, prevention of cybercrime.*

Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi va jamiyatining barcha sohalarida Internetdan keng foydalanish kundalik faoliyatning bir qismini tashkil etib, xizmat ko‘rsatish, ilm-fan, ta’lim, elektron tijorat, shuningdek, insonning fikrlash tarziga o‘zining ijobiy ta’siri bilan kirib keldi. Biroq bu o’zgarishlar boshqa bir sohaning rivojlanishiga yo‘l ochmoqdaki, bu jarayon allaqachon har bir davlat uchun strategik masalaga aylanib ulgurgan. Axborot texnologiyalarining keng miqyosda rivojlanishi bir vaqtning o‘zida ko‘p turdagi jinoyatlarning sodir etilishiga ham imkon yaratdi. Shulardan biri kiberjinoyatchilikdir.

Axborot texnologiyalari zamon zayli bilan rivojlanib borgani sari kiberjinoyat tarixi ham shunga monand ravishda rivoj topib keldi. Aytish joizki, kiberjinoyatchilik uzoq yillik tarixga ega bo’lmagan yangi jinoyat dunyosi. Hozirgi kunda jahon hamjamiyatini tashvishga qo’yayotgan, insonlarning shaxsiy va mulkiy daxlsizligiga rahna solayotgan bu jinoyat yaqin tarixga ega. Kiberjinoyatchilikning paydo bo’lishini kompyuter paydo bo’lgan paytdan boshlab hisoblash mumkin va bu “kompyuter davri” deb ataladi. Umuman olganda, birinchi shaxsiy kompyuter yaratilganidan va Internet tarqalgandan beri jinoyatchilar zamonaviy axborot texnologiyalaridan o’zlarining noqonuniy harakatlarini amalga oshirishda faol foydalanib kelishmoqda. Kompyuter sohasining jadal rivojlanishi bilan bir qatorda kiberjinoyatchilik ham o’z rivojlanishini boshlaydi.

Kiberjinoyatchilik rivojlanishining tarixini bir necha bosqichlarga ajratib o’rganishimiz mumkin [1].

I bosqich. Global Internet tarmog’ining rivojlanishi va tarqalishi. Ushbu bosqichda kompyuter jinoyati hali rivojlanmagan, ammo jamiyat uchun xavf tug’diradigan harakatlarning amalga oshirilishi boshlangan edi. Internet shakllanishining tarixi o’tgan asrning 60-yillariga borib taqaladi. 1962-yilda professor Jon Liklayder o’zining “Galaktik tarmoq” (kompyuter tarmog’i orqali Internet tarmog’ini yaratish) konsepsiyasiga asos solgan. U o’zining konsepsiyasida quyidagi fikrlarni keltirgan: “Yaqin kelajakda sayyoradagi barcha kompyuter tizimlarini bog’laydigan va har kim ulanishi mumkin bo’lgan global tarmoq yaratiladi”. Ayni vaqtda uning barcha farazlari o’z isbotini topganligi hech kimga sir emas.

II bosqich. Bu bosqich kompyuter jinoyatlarining shakllanishi hamda xakerlar subkulturasining paydo bo’lishi bilan xarakterlanadi. Shuningdek, global tarmoqda jinoyatchilikning son jihatidan o’sishi kuzatildi, ammo bu davrdagi kiberjinoyatlar faqat cheklangan miqdordagi mutaxassislar tomonidan amalga oshirilmoqda edi. Kompyuter

jinoyatchilarining ixtisoslashuvi ham aynan shu bosqichda yuz berdi. Birinchi qayd etilgan Internet-xakerligi o'zlarini "414 – guruh" deb atagan bir guruh voyaga yetmagan o'spirinlar tomonidan sodir etilgan jinoiy harakat edi. To'qqiz kun ichida "414 – guruh" 60 dan ortiq shaxsiy kompyuterlarni hamda AQSHdagi Los-Alamos Davlat yadro qurolini o'rganish laboratoriyasi kompyuterlarini buzib kirishga muvaffaq bo'lgan. 1983-yilda esa ushbu dastlabki kiberterroristlar guruhi ushlangan. Shu orqali 1983-yilda "WarGames" nomli dastlabki xakerlar to'g'risidagi film yaratilgan.

III bosqich. Ushbu bosqichda jinoyatchilar an'anaviy jinoyat turlarini sodir etish uchun ham axborot–telekommunikatsiya texnologiyalaridan foydalanishni boshlashdi. Shu bilan birgalikda, bu davrda ko'pchilik davlatlarda kiberjinoyatlarning keng tarqalishi yuz berdi hamda yirik "xakerlik guruhlari" paydo bo'ldi. 1994-yilda "transmilliy tarmoq kompyuter jinoyati" maqomini olgan "Vladimir Levin ishi" butun dunyoga ma'lum bo'ldi. Bu birinchi rossiyalik kiberjinoyatchilar ishtirokidagi shov-shuvli ish edi. 12 kishidan iborat xalqaro uyushgan jinoiy guruh Internet ma'lumotlar tarmog'idan foydalanib, himoyani yengib o'tishgan va bank mijozlarining hisob raqamlaridan jami 10 million 700 ming 952 AQSh dollari miqdoridagi 40 ta pul o'tkazmalarini amalga oshirishga harakat qilishgan. Biroq, ular faqat 400 ming dollarni o'g'irlashga muvaffaq bo'lishgan, shundan keyin ularning jinoiy faoliyati to'xtatiladi.

IV bosqich. Ushbu davr kiberjinoyatchilik transmilliy xususiyatga ega bo'lgani bilan xarakterlanadi. Kiberterrorizm va xalqaro xakerlik guruhlarining paydo bo'lishi hamda kibermakonda transmilliy jinoyatchilik va kiberjinoyatchilikning birlashuvi yuz berdi. Internetdan siyosiy maqsadlarda foydalanish (urushlar), bunday hodisalarning paydo bo'lishi, kiberurush va kiberterrorizm ushbu bosqichning o'ziga xos jihatalaridir. Ushbu bosqichning yorqin namunasi 12 yoshli xakerning jinoiy harakatidir. 1998-yilda xaker Arizonadagi to'g'onni boshqaradigan kompyuter tizimiga noqonuniy kirishi oqibatida kiberterrorizm atamasi butun dunyoga tarqalib ketdi. Agar 23 ta drenaj eshigi ochilgan bo'lsa aholisi 1 milliondan ortiq bo'lgan bir nechta shaharlar suv toshqini ostida qolishi mumkin edi. Ushbu jinoyat Internet terrorizmi, kiberterrorizm atamalarining paydo bo'lishiga olib keldi [2].

Yuqoridagilar bilan bir qatorda kiberjinoyatlar tarixini xronologik jihatdan ikki davrga bo'lib ham o'rganish mumkin. Xususan:

1) birinchi kompyuter yaratilganidan 1990-yilgacha bo'lgan davr;
2) 1990-yildan hozirgi kungacha bo'lgan davr.

Nima uchun aynan 1990-yil? Gap shundaki, 1990-yildan boshlab Internet butun dunyo bo'ylab juda katta tezlikda tarqala boshladi.

Kompyuterdan jinoyat sodir etish maqsadida foydalanish mumkinligi haqidagi birinchi axborotlar 1960-yillarda ommaga ma'lum bo'ldi. Ammo 1960 – 70-yillardagi kompyuter jinoyati bugungi kundagi kiberjinoyatchilikdan farq qilar edi. Birinchidan, o'sha paytda Internet hali paydo bo'lmagan edi, ikkinchidan esa kompyuterlar tarmoqqa ulanmagandi.

O’sha paytda faqat ma’lum bir tadqiqotchilar va olimlar o’z ishlarida kompyuterdan foydalanishlari mumkin edi. Kompyuterdan cheklangan holda foydalanish va boshqa kompyuterlarga ulanishning iloji yo’qligi kompyuter jinoyatlarini sodir etish ehtimolini keskin kamaytirgan va agar ular sodir etiladigan bo’lsa faqat kompyuterda xizmat ko’rsatuvchi shaxslar tomonidan amalga oshirilgan. Bu hol Internet paydo bo’lib butun dunyo miqyosida tarqalguncha davom etdi.

1960-yillar xakerlikning kelib chiqishi bilan xarakterlanadi. Birinchi kompyuter xakerlari Massachuets tehnologiya instituti (MIT) da paydo bo’ldi. Ba’zi guruh a’zolari universitetdagi yangi kompyuter dasturlarini boshqarishni boshlaydilar.

1970-yillarga kelib xakerlar bepul qo’ng’iroqni amalga oshirish uchun mahalliy va xalqaro telefon tarmoqlarini buzishni boshlagan. Telefon xakerlarining “otasi” - Jon Draper (Cap’n Crunch nomi bilan tanilgan) Cap’n Crunch jo’xori qutisidan topgan o’yinchoq hushtagi shaharlararo telefon tarmog’iga kirish signalining chastotasiga to’g’ri keladigan 2600 Gerts tovushini chiqarishini aniqlagan. Jon Draperning telefon tarmoqlarini buzish bilan shug‘ullanishi oqibatida dastlabki kiberjinoyatlar sodir etilgan. 1979-yilda SSSRda axborot texnologiyalari sohasidagi ilk yuqori darajadagi jinoyat sodir etilgan. U Vilnyus shahrida qayd etilgan va bu holat o‘sha paytda davlatga 80 ming rubl zarar yetkazilishiga sababchi bo‘lgan va bu o‘sha paytda mashhur avtomashina bo‘lgan “Volga” rusumidagi 8 ta avtomashinaning puli degan gap edi. Bu jinoyat Interpol xalqaro tashkiloti tomonidan dastlabki ro‘yxatga olingan kiberjinoyat sifatida e’tirof etilgan.

1980-yillardan telefon xakerlari kompyuter xakerligi bilan shug’ullana boshlaydilar, birinchi elektron xabarlar taxtasi (BBS) tizimlari, Usenet yangiliklar guruhlari va elektron pochtalar paydo bo’ladi. “SherwoodForest” va “Catch-22” kabi nomlar ostida BBS xakerlar va telefon xakerlari uchun uchrashuv joylariga aylanadi. Ular parollar va kredit karta raqamlarini o’g’irlash bo’yicha tajriba almashishgan. Shuningdek, shu yillarda xakerlik guruhlari ham shakllana boshlagan. Ular dastlab AQSh (LegionofDoom) va Germaniyada (ChaosComputerClub) paydo bo’lgan. 1981-yilda Kapitan Zap nomi bilan tanilgan xaker Ian Murphy birinchi bo’lib kiberjinoyatchilikda aybdor deb topilgan. U AT&T telefon kompaniyasining tarmog’ini buzgan va qo’ng’iroqlarni ta’riflash dasturini o’zgartirgan, shundan so’ng kunduzgi telefon qo’ng’iroqlarini tungi ta’rifda va aksincha amalga oshirish mumkin bo’lgan. Sud unga 1000 soatlik jamoat ishlari va 2,5 yillik sinov muddatini bergan. 1984-yildan “2600” xakerlik jurnali muntazam ravishda nashr etila boshlangan. Jurnal muharriri Emmanuel Goldshteyn bo’lgan (Jorj Oruelning “1984” asarining bosh qahramonidan taxallus olgan), haqiqiy ismi Erik Korli. Jurnalga nom birinchi telefon xakeri Cap’n Crunch tomonidan berilgan. Jurnalda xakerlar uchun sharhlar va maslahatlar nashr etib borilgan. 1986-yilda korporativ va davlat kompyuterlarini buzish sonining ko’payishidan xavotirlangan AQSh Kongressi “Computer Fraudand Abuse Act” aktini qabul qilgan. Unda kompyuterlarni buzish jinoyat deb belgilangan. Ammo, bu voyaga yetmaganlar uchun tatbiq etilmagan. 1988 yilda Cherv Morris tomonidan dastlabki zararli virus yaratilgan, buning oqibatida AQSH

Hukumati va universitetlaridagi 6000 ga yaqin kompyuterlar ushbu zararli virus qurboni bo‘lishgan. Natijada, shu kabi zararli faoliyatga qarshi kurashish maqsadida AQSHda CERT Internet xavfsizligini ta’minlash markazi tashkil qilingan va u tomonidan 1988 yilda 6 ta, 1989-yilda 132 ta, 1990-yilda esa 252 ta kiberxodisa aniqlangan [3].

Kiberjinoyatlar rivojlanishining ikkinchi bosqichi o’tgan asrning 90-yillari o’rtalarida boshlanadi va bu kiberjinoyatchilikning navbatdagi to’lqini edi. Aynan shu davrda Internet tez sur’atlar bilan tarqaldi hamda veb-brauzerlarning rivojlanishiga sabab bo’ldi.

1990-yilda AQSHda “Sundevil” operasiyasi uyushtirilib, AQSHning 14 shahridagi xakerlarga nisbatan misli ko‘rilmagan ov uyushtiriladi. Buning oqibatida 1993-yilda Las-Vegasda xakerlarning eng katta yillik anjumani “DefCon” bo‘lib o‘tgan. Keyinchalik u har yili o‘tkaziladigan bo’ldi [4]. 1994-yilda vebsaytni ko’rish va saqlash uchun BBS ga qaraganda qulayroq bo’lgan brauzer Netscape Navigator paydo bo’ladi. Natijada xakerlar o’zlarining barcha dasturlari, yordamchi dasturlari, maslahatlari va texnologiyalarini veb-saytga ko’chirishadi. Ayni shu yilda Buyuk Britaniyalik talaba ochiq manbadan olingan ma’lumotlar orqali Koreyaning yadroviy dasturini, AQShning ayrim muassasalari va NASA kompyuter tarmoqlarini buzishga harakat qilgan. Bunda u faqat shaxsiy kompyuteri va Internetdan topgan “Blueboxing” dasturidan foydalangan. 1995-yilda makroviruslar paydo bo’ldi. Makroviruslar – bu makro tilida yozilgan, dasturlarga kiritiladigan virusli dastur hisoblanadi. 1996-yilda AQSHda Milliy razvedka boshqarmasi direktori Jon Deych xorijiy uyushgan jinoiy guruhlar AQSh hukumati tarmog’ini va boshqa korporativ tarmoqlarni buzishga urinayotgani haqida xabar bergan [5]. 1997-yilda “AOHell” (“America-on-Hell”) deb nomlangan bepul tarqatiladigan xakerlik dasturi paydo bo’ladi. Bu o’sha davrdagi eng yirik Internet-provayder “AmericaOnline” uchun katta kulfat keltirgan. Chunki uning yordami bilan har qanday foydalanuvchi AOL elektron pochta xizmatlariga ko’p megabaytli email bombalarini va suhbatlarda spam xabarlarini yuborishi mumkin bo’lgan. Shuningdek, shu yili AQSh kompaniyalarining 85% dan ortig’i xakerlik hujumiga uchragani va hujumlarning aksariyati e’tiborga olinmagani haqida Federal qidiruv byurosi xabar bergan. 1998-yilda “CultoftheDeadCow” xakerlar jamoasi Windows 95/98-ni buzish uchun “BackOrifice” dasturini yaratishadi. Bu o’chirilgan troyan yordam dasturi orqali masofadan turib boshqarish uchun kuchli vosita edi. Dastur DefCon yig’ilishida taqdim etilgan. 1999-yilda esa ko’p sonli kompyuterlarning zararlanishiga sabab bo’lgan “Melissa” virusi yaratilgan. XXI asrning dastlabki o’n yilligi kiberjinoyatlarning oltin asri hisoblanadi [6]. Bu davrda yanada murakkab hujumlar sodir etildi, shuningdek, raqamli iqtisodiyotning muhim tarmoqlariga katta zarar yetkazgan yangi viruslar yaratildi.

2001-yilda Microsoft veb-saytlari DNS serverlarining hujumlariga uchraydi. 2002-yildan Shadow veb-sayti ishlay boshlaydi. Bu veb-sayt bir tarafdan e’lonlar taxtasi va boshqa tarafdan esa xakerlar uchun aloqa platformasi hisoblangan. Uning foydalanuvchilari ma’lumot joylashtirishlari, kiberjinoyatlar bo’yicha ko’rsatmalar va sxemalarni ulashishlari, ularni aniqlash va jazolashdan qochish usullarini baham

ko’rishlari mumkin edi. Sayt razvedka idoralari tomonidan yopilishidan oldin 2 yil davomida faol bo’lgan. 2008-yilda Heartland Payment tizimiga SQL kombinatsiyadan foydalangan holda hujum uyushtirilgan. Natijada 134 million foydalanuvchilarning ma’lumotlari xavf ostida qolgan.

2010-yilda dunyodagi birinchi “raqamli qurol” deb nomlangan “Stuxnet worm” orqali Eronning atom zavodlariga hujum uyushtirilgan. Ayni shu yilda “Zeus Trojan” virusi yaratildi va butun dunyo bo’ylab elektron pochta orqali moliyaviy tashkilotlarga hujum uyushtrigan. 2015-yilda “SamSam” zararli dasturining (pul miqdori to’lanmaguncha kompyuter tizimiga kirishni blokirovka qilish uchun mo’ljallangan) dastlabki turlari paydo bo’ldi. Ma’lumotlarga ko’ra, ularning yaratuvchilari 2018-yilga qadar 6 million dollar foyda qilishgan. 2017-yilda WannaCry zararli dasturi paydo bo’ldi. U 150 ta mamlakatdagi 200,000 dan ziyod Windows kompyuterlariga zarar yetkazdi. Eng kata zarar ko’rganlardan biri Buyuk Britaniyaning Milliy Sog'liqni saqlash xizmati shifoxonalari bo’lgan. Hujum ortida Shimoliy Koreyadagi xakerlar turgani haqidagi xabarlar keng tarqalgan. 2020-yilda Neiman Marcus kompaniyasi o’zining 4,6 million mijoziga xaker shaxsiy ma’lumotlarga kirish huquqini qo’lga kiritib, onlayn hisoblarni buzganligi haqida xabar berdi.

Rasmiy xabarlar va statistikaga e’tibor beradigan bo’lsak, kiberjinoyatlar son va sifat jihatidan kundan kunga rivojlanib bormoqda. Yuqorida ko’rib o‘tganimizdek, kiberjinoyatlar uzoq yillik tarixga ega bo‘lmasa-da, qisqa vaqt ichida har bir davlat uchun strategik masalaga aylanib ulgurdi. Shu munosabat bilan O‘zbekistonda ham bir qator harakatlar amalga oshirildi. Milliy qonunchiligimizda kiberjinoyatchilik tushunchasi ilk bor O‘zbekiston Respublikasi Prezidentining 2017-yil 7-fevraldagi PF–4947-sonli Farmoni bilan tasdiqlangan 2017–2021 yillarda O‘zbekiston Respublikasini rivojlantirishning beshta ustuvor yo‘nalishi bo‘yicha Harakatlar strategiyasini “Xalq bilan muloqot va inson manfaatlari yili”da amalga oshirishga oid davlat dasturining 297-bandida tilga olingan [7]. Shu bilan birgalikda, O‘zbekiston Respublikasi Jinoyat kodeksiga “XXI bob. Axborot texnologiyalari sohasidagi jinoyatlar” bobi kiritildi va ushbu bobda axborotlashtirish qoidalarini buzish, kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish, kompyuter tizimidan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o‘tkazish maqsadini ko‘zlab tayyorlash yoxud o‘tkazish va tarqatish, kompyuter axborotini modifikasiyalashtirish, kompyuter sabotaji, zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish uchun jinoiy javobgarlik kiritildi.

FOYDALANILGAN ADABIYOTLAR:

1. Л.П. Зверянская. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений //Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 881–885. – URL: https://e-koncept.ru/2016/96090.htm.
2. Буз Стелла Ивановна Киберпреступления: понятие, сущность и общая характеристика//ЮП. 2019. №4 (91).
3. Л.П. Зверянская. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 881–885. – URL: https://e-koncept.ru/2016/96090.htm.
4. А. Николаева, М. Тумбинская. Киберпреступность: история развития, проблемы практики расследования. Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ Казань, Россия. Материалы международной конференции Sorucom 2014//13-17 октября 2014.
5. Ирма Сурикова. “Откуда приходит киберпреступность? Происхождение и эволюция киберпреступности”. https://le-vpn.com/ru/cybercrime-history.
6. “A Brief History of Cybercrime”/ November 16, 2022, by Arctic Wolf
7. https://www.lex.uz/docs/-3107036