

O‘ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI
A K A D E M I YA

R.K. KABULOV,
E.S. ABDURAXMANOV

AXBOROT TEXNOLOGIYALARI SOHASIDAGI
JINOYATLAR

Toshkent – 2009

O‘ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI
AKADEMIYA

R.K. KABULOV,
E.S. ABDURAXMANOV

AXBOROT TEXNOLOGIYALARI SOHASIDAGI
JINOYATLAR

O‘QUV QO‘LLANMA

Toshkent – 2009

*O‘zbekiston Respublikasi IIV Akademiyasining
tahririyat-noshirlik kengashida ma’qullangan*

TAQRIZCHILAR:

yuridik fanlari doktori I. ISMAILOV

texnika fanlari doktori, professor B. RAJABOV

Kabulov R.K., Abduraxmanov E.S.

Axborot texnologiyalari sohasidagi jinoyatlar: O‘quv qo‘llanma. – T.:
O‘zbekiston Respublikasi IIV Akademiyasi, 2009. – 107 b.

Qo‘llanmada axborot texnologiyalari sohasidagi jinoyatlarning jinoiy-
huquqiy tavsifi aks ettirilib, tarkibiy qismlarining mazmuni, ularni kvalifikatsiya
qilish masalalari tahlil qilinadi, bunday jinoyatlarning oldini olishga oid huquqiy
va tashkiliy-texnik chora tabirlar ko‘rib chiqiladi.

Huquqshunos olimlar, amaliyot xodimlari, doktorant, adyunkt va aspirantlar,
tinglovchi, kursant, umumta’lim muassalarining talaba va o‘quvchilari uchun
mo‘ljallangan.

© O‘zbekiston Respublikasi IIV Akademiyasi, 2009

© R.K. Kabulov, E.S. Abduraxmanov, 2009.

KIRISH

Hozirgi sharoitda axborot texnologiyalari jamiyat taraqqiyotining turli sohalariga jadal kirib bormoqda va ularni rivojlantirish uchun xizmat qilmoqda. Bunday texnologiyalarning ta'siri odamlarning turmush tarzi, ta'limi va ishida o'z natijasini ko'rsatmoqda. Axborot texnologiyalari jahon iqtisodiyotining rivojlanishi va ijtimoiy muammolarning hal etilishi uchun muhim omilga aylandi. Shu bois, axborotlashtirish milliy tizimini shakllantirish, uni iqtisodiyot va hayotning barcha sohalariga yalpi joriy etish va undan foydalanish, zamonaviy axborot texnologiyalari, kompyuter texnikasi va telekommunikatsiyalar, fuqarolarning axborotga nisbatan o'sib borayotgan ehtiyojlarini iloji boricha to'liq qondirish, jahon axborot hamjamiyatiga qo'shilish uchun qulay sharoitlar yaratish hamda dunyo axborot resurslaridan foydalanish imkoniyatlarini kengaytirish hozirgi jamiyat taraqqiyotining ustuvor yo'nalishlaridir. Shu munosabat bilan, «...Hozirgi axborot, kommunikatsiya va kompyuter texnologiyalari asrida, internet kundan-kunga hayotimizning barcha jabhalariga tobora chuqur va keng kirib borayotgan bir paytda, odamlarning ongi va tafakkuri uchun kurash hal qiluvchi ahamiyat kasb etayotgan bir vaziyatda bu masalalarning jamiyatimiz uchun naqadar dolzarb va ustuvor bo'lib borayotgani haqida gapirib o'tirishga hojat yo'q»¹, degan edi O'zbekiston Respublikasining Prezidenti I.A. Karimov

Ma'lumki, jamiyat hayotining muayyan sohasi rivojlanishi bilan yangi texnologiyalardan foydalanishni va yashirincha (qonunga xilof tarzda) o'z ehtiyojlarini qondirishni istovchilar paydo bo'ladi. Bu, o'z navbatida, jinoiy faoliyatning yangi turi – axborot texnologiyalari sohasidagi jinoyatlarning sodir etilishiga sabab bo'lmoqda. Mazkur jinoyat hozirgi bosqichda ancha yuqori darajaga chiqdi. Masalan, Angliya tahliliy kompaniyasi – LITSning bergan ma'lumotlariga qaraganda, 2003 yilda jahon iqtisodiyotiga kompyuter jinoyatlari tufayli yetkazilgan zarar 132 mlrd. AQSH dollaridan oshib ketdi (2002 yilda bu ko'rsatkich 48 mlrd. dollar edi), 2004 yilda kompyuter jinoyatlaridan ko'rilgan

¹ Каримов И.А. Бизнинг бош мақсадимиз – жамиятни демократлаштириш ва янгилаш, мамлакатни модернизация ва ислох этишдир. – Т.: 2005. – 56 б.

iqtisodiy-moddiy zarar 411 mlrd., 2005 yilda esa taxminan 687 mlrd. AQSH dollarigacha o'sdi¹. Keltirilgan statistik ma'lumotlar axborot texnologiyalari sohasidagi jinoyatlardan yetkazilayotgan moddiy zarar yil sayin ko'payib borayotganidan dalolat bermoqda. Gap shundaki, kompyuter texnikasi takomillashib borgani sayin u bilan bog'liq jinoyatlarning ustomonlik bilan sodir etilishi kuchayib bormoqda.

O'zbekiston Respublikasida yaqin vaqtlargacha kompyuter jinoyatchiligi faqat xorijiy rivojlangan mamlakatlarga xos hodisa deb hisoblanib kelgan va jamiyatimiz uncha kompyuterlashmagani bois, bunday jinoyatlar mavjud emas edi. Biroq ayni vaqda yurtimizdagi vaziyat boshqacha. Odamlar, korxonalar, tashkilotlar va davlat faoliyatining deyarli barcha tomonlariga daxldor bo'lgan jamiyatning kompyuterlashuvi ijtimoiy munosabatlarning yangi sohasini yuzaga keltirdi. Bu soha, afsuski, ko'p hollarda g'ayriqonuniy qilmishlar ob'ektiga aylanmoqda. Xo'jalikning turli tarmoqlaridagi holat, shuningdek mamlakat mudofaa qobiliyatining ob'ektiv in'ikosi bo'lgan kompyuter axborot tizimi ushbu tizimga ulkan moliyaviy-moddiy zarar yetkazishi mumkin bo'lgan jinoyatchi unsurlarning ruxsatsiz (g'ayriqonuniy) kirishidan huquqiy xavfsizlikni ta'minlash vositalariga juda muhtoj. Bu kabi holatlarni inobatga olgan holda O'zbekiston Respublikasining «Axborotlashtirish va ma'lumotlar uzatish sohasidagi qonunga xilof harakatlar sodir etganlik uchun javobgarlik kuchaytirilganligi munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritishi to'g'risida»gi 2007 yil 30 noyabr qonunida kompyuter tizimlaridan noqonuniy foydalanish bilan bog'liq xavfli qilmishlar jinoyat deb belgilandi hamda amaldagi Jinoyat kodeksi «Axborot texnologiyalari sohasidagi jinoyatlar» nomli yangi XX¹ bob bilan to'ldirildi. Mazkur bob Jinoyat kodeksi Maxsus qismining «Jamoat xavfsizligi va jamoat tartibiga qarshi jinoyatlar» deb nomlangan oltinchi bo'limga kiritildi.

Axborot texnologiyalaridan g'ayriqonuniy foydalanish bilan bog'liq ijtimoiy xavfli qilmishlarning kriminallasuvi ayni vaqtda axborot munosabatlari

¹ Qarang: Расулев А.К. Компьютерные преступления: уголовно - правовые и криминологические аспекты: Автореф. ... канд. юрид. наук. – Т., 2006. – С.3–4.

elementlariga ham, jinoyat qonunida tartibga solinadigan munosabatlarga ham aloqador bo'lgan tushunchalarning huquqiy mazmuni va mohiyatini tadqiq etishni talab etadi. O'zbekiston Respublikasining Jinoyat kodeksida axborot texnologiyalari sohasidagi jinoyatlarga oid yangi bobning paydo bo'lganligi, bir tomondan, huquqni muhofaza qilish organlarning oldiga ushbu turdagi jinoyatlarni ochish va tergov qilish vazifasini qo'yimoqda. Boshqa tomondan, axborot texnologiyasi atrofidagi munosabatlar sohasi yaqingacha texnika sohasidagi mutaxassislarning ishi hisoblanardi. Shu bois aksariyat yuristlar ushbu soha terminlari va tushunchalarini hamon yyetarli darajada bilmaydilar. Amaldagi jinoyat qonunchiligidan bir xilda va samarali foydalanish maqsadida mazkur qo'llanmada axborot texnologiyalari sohasidagi jinoyatlarning jinoiy-huquqiy tavsifi yoritildi, ayrim tarkiblari tahlil qilindi hamda bunday jinoyatlarni kvalifikatsiya qilish xususiyatlari, jumladan ularning oldini olishning huquqiy va tashkiliy-texnikaviy choralari bayon qilindi.

I. Axborot texnologiyalari sohasidagi jinoyatlarning jinoyiy-huquqiy tavsifi

Hozirgi ijtimoiy taraqqiyot voqeliklari, texnologik jarayonlarning elektron vositalar bilan boshqarish usullariga o'tilishi, EHM yordamida amalga oshiriladigan aktlarga yuridik kuch berilishi ushbu jarayonlardan axborot texnologiyalari sohasida jinoyatlar sodir etish uchun foydalanishga ham shart-sharoit yaratdi. Telekommunikatsiya tarmoqlarining tarkibiy qismlari ishiga, ular muhitida ishlovchi kompyuter dasturlariga g'ayriqonuniy aralashish, kompyuter axborotini qonunga xilof ravishda modifikatsiyalashtirish va yo'q qilib yuborish davlat infratuzilmasining nihoyatda muhim elementlari ishini buzishi mumkin hamda ko'plab odamlarning halok bo'lishi, katta miqdorda mulkiy zarar yetkazilishi yoki boshqa ijtimoiy xavfli oqibatlarining kelib chiqishi xavfini tug'diradi.

Xorijda tarmoq texnologiyalari rivojlanishining boshlang'ich bosqichida, iqtisodiyotning axborot texnologiyalariga unchalik bog'liq emasligi tufayli, virusli va boshqa turdagi kompyuter hujumlaridan yetkaziladigan zarar unchalik katta emas edi. Hozirgi vaqtda bunday hujumlar soni borgan sari ko'payib borayotgan, ularni avtomatlashtirish mexanizmlari yaratilayotgan, fuqarolar, tijoratchilar, davlat hokimiyati organlari axborotdan foydalanish va uni ayirboshlashning elektron vositalariga juda bog'liq bo'lib qolgan sharoitda axborot tizimlariga hujumlarning amalga oshirilishidan ko'rilyotgan zarar ulkan summalarni tashkil etmoqda.

Kompyuter texnologiyalari sohasidagi jinoyatlarning ko'payishi, ularning yuqori darajadagi ijtimoiy xavfliligi mazkur jinoyatlardan muhofaza qilish choralarini (avvalo kompyuter texnologiyalarining o'zini qo'riqlash orqali) ishlab chiqishni taqozo etdi. Olimlar tadqiqotlarining ko'rsatishicha, bunday muhofaza vositalarining 60 % huquqiy vositalarga, 20 % kriptografik va 20 % dasturiy, apparatga oid hamda boshqa jismoniy, tashkiliy vositalarga to'g'ri keladi.

1965 yilda AQSHda axborot texnologiyalari xavfsizligini ta'minlashga qaratilgan va 1973 yilda Shvetsiyada kompyuterni suiiste'mol qilganlik uchun jinoiy javobgarlik to'g'risidagi dastlabki qonunlar hamda 1994 yilda BMT tomonidan kompyuterlardan foydalanish bilan bog'liq jinoyatlarning oldini olish va ularga qarshi kurash bo'yicha yo'riqnoma qabul qilindi.

O'zbekistonda axborot texnologiyalari sohasidagi munosabatlarni qonun hujjatlari bilan tartibga solish va muhofaza qilish masalasi o'tgan asrning 90 – yillari boshlarida hal etila boshlangan. Bunday kechikish muayyan darajada mamlakatimizda EHM rivojlanishining darajasi pastligi bilan bog'liq edi.

1994 yil 6 mayda O'zbekiston Respublikasining «Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma'lumotlar bazalarining huquqiy himoyasi to'g'risida»gi qonuni qabul qilindi. Unga keyinchalik O'zbekiston Respublikasining 2002 yil 5 aprel va 8 avgustdagi qonunlari bilan o'zgartish va qo'shimchalar kiritildi. Mazkur qonunda ma'muriy va jinoiy javobgarlik haqida so'z yuritilgan (15-modda) va mualliflik huquqlarini buzganlik uchun javobgarlik nazarda tutilgan. O'zbekiston Respublikasining «Axborot erkinligi printsiplari va kafolatlari to'g'risida»gi 2002 yil 12 dekabr hamda «Axborotlashtirish to'g'risida»gi 2003 yil 11 dekabr qonunlarining qabul qilinishi axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurash bo'yicha qonun hujjatlarining asosini tashkil etadi. Ularda jinoyatlarni to'g'ri kvalifikatsiya qilish va aybdor shaxslarni jinoiy javobgarlikka tortish uchun printsiptial ahamiyatga ega bo'lgan ko'plab huquqiy va texnikaviy terminlarga ta'riflar berilgan.

Axborot texnologiyalari sohasidagi jinoyatlar nafaqat intellektual mulk daxlsizligini buzish, balki fuqarolarning shaxsiy hayoti haqidagi ma'lumotlarni oshkor etish, bevosita zarar va olinmagan foyda ko'rinishida mulkiy zarar yetkazilishi, firma obro'sining to'kilishi, korxonalar, muassasa va tashkilotlar huquqiy faoliyatini buzishning har xil turlari va boshqalardir.

Yuqoridagilardan kelib chiqqan holda ta'kidlash mumkinki ushbu turdagi jinoyatlar axborot texnologiyalaridan qonuniy, xavfsiz foydalanishni ta'minlovchi munosabatlarga tajovuz qiladi.

Jinoyat ob'ektining to'rt bo'g'inli tuzilishga ega ekanligi haqidagi nazariyaga asoslanadigan bo'lsak, axborot texnologiyalaridan g'ayriqonuniy foydalanish bilan bog'liq jinoiy tajovuzning **umumiy ob'ektini** jinoyat qonuni bilan muhofaza etiladigan barcha ijtimoiy munosabatlar majmui, **maxsus ob'ektini** jamoat xavfsizligi va jamoat tartibi, **turdosh ob'ektini** axborot texnologiyalaridan qonuniy va xavfsiz foydalanish borasidagi ijtimoiy munosabatlar majmui tashkil qiladi. **Bevosita ob'ekti** esa muayyan moddaning nomi va dispozitsiyasidan kelib chiqib aniqlanadi. Aksariyat hollarda axborot texnologiyalari sohasidagi jinoyatning asosiy tarkibi ob'ektining ushbu turi muqobil tarzda ifodalangan, og'irlashtiruvchi tarkiblarda ularning soni, tabiiyki, ko'paytirilgan.

Umumiy, maxsus, turdosh va bevosita ob'ektlarning ajratilishi ob'ektiv ravishda ular qamrab oladigan jinoiy-huquqiy qo'riqlash ob'ekti bo'lmish ijtimoiy munosabatlarning butun hajmini aks ettiradi va O'zbekiston Respublikasi Jinoyat kodeksining hozirgi tuzilishiga muvofiq keladi¹.

Axborot texnologiyalari sohasidagi jinoyatlarning ob'ekti nimadan iborat, degan masala hanuzgacha bahsli bo'lib kelmoqda. Jumladan, yuridik adabiyotlarda ushbu turdagi jinoyatlarning ob'ekti va predmeti xususida har xil fikrlar bor. Masalan, V. V. Krilov ushbu jinoyatlarning ob'ektini EHM ma'lumotlari tashkil qiladi, deb hisoblaydi². L. Chichko esa ob'ekt deganda EHM axborotini³, V. B. Vexov esa mashina axborotini⁴ tushunishni ta'kidlagan. Axborot jinoyat ob'ekti bo'lishi mumkin degan qarash tarafdorlari fikricha axborot, shu jumladan, kompyuter axboroti jamiyat uchun yaratilgan qulaylikdir, shu sababli ular noqonuniy yo'q qilinganida yoki modifikatsiyalashtirilganida zarar ko'rilishi ayni haqiqatdir. Ammo kompyuter axboroti (masalan, sir saqlanadigan ma'lumotlar) qonunga xilof tarzda nusxa ko'chirilishi va ular to'sib qo'yilishi mumkin. Bunda

¹ Qarang: Таджиханов Б.У. Уголовно-правовые меры борьбы с терроризмом / Отв. ред. докт. юрид. наук А.С. Якубов. – Т.:, 2003. – С.4–20; Наумов А.В. Российское уголовное право. Общая часть. – М., 1999. – С. 162–163.

² Qarang: Крылов В. Информационные преступления – новый криминологический объект // Российская юстиция. – 1997. – № 7 – С.22 – 23.

³ Qarang: Чичко Л. Компьютерные хищения // Российская юстиция. – 1996. – №5. – С.45.

⁴ Qarang: Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. – М., 1996. – С.163.

axborot o'zi aslo zarar ko'rmaydi. Vaholanki, jinoyat ob'ekti doimo jinoiy qilmishdan zarar ko'radi, aks holda, jinoyat tarkibi mavjud bo'lmaydi. Xo'sh, jinoyat nimada namoyon bo'ladi? Yuqoridagi ikki holatda nima yuz beradi? Unda nima va qanday zarar ko'radi?

Birinchi holda axborot qonuniy egasining undan monopol foydalanish munosabatlariga, ikkinchi holda esa bevosita qonuniy va xavfsiz foydalanish munosabatlariga zarar yetadi. Binobarin, kompyuter axboroti o'z-o'zicha har doim ham zarar ko'rmaydi, ammo barcha hollarda undan foydalanish munosabatlari buziladi degan xulosaga kelish mumkin.

Jinoiy-huquqiy tushunishda kompyuter axboroti axborot texnologiyalari sohasidagi jinoyatlarning predmeti hisoblanadi. Masalan bunday holatlar Jinoyat kodeksi 278¹, 278², 278⁴ va 278⁶-moddalarining dispozitsiyalarida to'g'ridan-to'g'ri ko'rsatilgan. Boshqa hollarda esa predmetning aniqlanishi jinoyat tarkibi boshqa elementlarining aniqlanishi bilan bog'langan (Jinoyat kodeksining 278³ va 278⁵-moddalari).

O'zbekiston Respublikasining «Axborot erkinligi printsiplari va kafolatlari to'g'risida»gi qonunning 3-moddasiga muvofiq, axborot deganda, taqdim etilish shaklidan qat'i nazar, shaxslar, narsalar, faktlar, hodisalar, voqea va jarayonlar to'g'risidagi ma'lumotlar tushuniladi. Jinoyat kodeksi Maxsus qismining axborot texnologiyalari sohasidagi jinoyatlarga oid bobining xususiyati shundaki, unda axborotning alohida turi – kompyuter axboroti haqida so'z boradi.

Kompyuter axboroti EHM yordamida ishlov beriladigan va foydalaniladigan hamda shaxslar, narsalar, faktlar, hodisalar, voqealar va jarayonlar to'g'risidagi ma'lumotlarga, shuningdek undan foydalanish rejimi (qoidalari)ni belgilagan mulkdorning identifikatsion atributlariga ega EHM dasturlari va ma'lumotlar bazalaridir. EHM dasturlari va ma'lumotlar bazalari ham jinoiy-huquqiy muhofaza etilishi kerak. Shu o'rinda EHM dasturlarining xususiyatlarini keltirib o'tish lozim. Ular bir jihatdan, axborotga ta'sir ko'rsatish vositasi bo'lsa, boshqa jihatdan komandalar va ma'lumotlar majmuidan iborat axborotdir. Ya'ni ularga muayyan ikki tomonlamalik xos. Bu esa EHM dasturini axborot turlaridan biri sifatida talqin etish uchun asos bo'ladi. O'zbekiston Respublikasining «Elektron hisoblash

mashinalari uchun yaratilgan dasturlar va ma'lumotlar bazalarining huquqiy himoyasi to'g'risida»gi qonunining 1-moddasida EHM dasturlariga quyidagicha ta'rif berilgan: «EHM dasturi – muayyan natija olish maqsadida EHM va boshqa kompyuter qurilmalarining ishlashi uchun mo'ljallangan ma'lumotlar va komandalar majmuini namoyon etishning ob'ektiv shakli. EHM dasturi deganda, uni ishlab chiqish davomida olingan tayyorgarlik materiallari hamda ushbu dastur yuzaga keltiradigan audiovizual tasvirlar ham nazarda tutiladi».

Xo'sh, ma'lumotlar bazasi deganda nima tushuniladi? Yuqoridagi qonunga ko'ra, «ma'lumotlar bazasi – ma'lumotlar majmuini taqdim etish va tashkil qilishning, ushbu ma'lumotlar EHM yordamida topiladigan va ishlov beriladigan tarzda tartibga solingan ma'lumotlarning ob'ektiv shakli (masalan: moddalar, hisob-kitoblar)».

Ma'lumki, kompyuter axboroti mashina tashuvchisida, EHMda, EHM tizimida, EHM tarmog'ida bo'lishi mumkin.

Mashina tashuvchisi – kompyuter axborotini doimiy saqlash va tashish uchun mo'ljallangan qurilmalar.

EHM mikroprotsessorni o'z ichiga oladigan sistema bloki, klaviatura (EHMga bosma simvol yozuvlarni kiritishga imkon beruvchi qurilma) va monitor (turli ma'lumotlarni aks ettiruvchi qurilma) kabilardan iboratdir.

Kompyuterning sistema blokiga turli qo'shimcha qurilmalar ulanishi mumkin. Ular EHMning funktsional imkoniyatlarini kengaytirish uchun mo'ljallangan. Bunday qurilmalarga printer, skaner, modem kabilar kiradi. EHM tizimini kompyuterning o'zi va barcha atrofidagi qurilmalar tashkil etadi.

EHM tarmog'i bir qancha kompyuterlarning birlashmasidan iborat bo'lib, maxsus kabellar yordamida hosil qilinadi.

Yuridik adabiyotlarda ba'zan shunday axborot texnologiyalari bilan bog'liq jinoyatlarga oid jumboqli savollar ham uchraydi. Masalan, EHMdan o'zga ob'ektga qarshi boshqa g'ayriqonuniy tajovuz sodir etish maqsadida foydalanilganda, kompyuter axboroti mazkur jinoyatning faqat predmetimi yoki vositasi ham bo'lishi mumkinmi? Bunga rossiyalik olim A. V. Sorokin shunday

javob beradi: «Axborot ham boshqa jinoyatlarni sodir etishda vosita hisoblanadi deb qabul qilish «kompyuter jinoyatlari» tushunchasining doirasini haddan tashqari kengaytirishda hamda qonun chiqaruvchi organning ham, huquqni qo‘llovchining ham ishini murakkablashtiradi»¹.

Texnik nuqtai nazardan, kompyuter axboroti haqiqatan ham kompyuter tizimi doirasidagi harakat (jinoiy harakat bo‘lishi shart emas) vositasi hisoblanadi, lekin bunda uni EHMning o‘zidan ajratmasligimiz kerak. Soddaroq aytganda, axborot kompyuterdan alohida emas, faqat u bilan birgalikdagina texnik va yuridik jihatdan vosita bo‘ladi. Shu bois, EHM vositasida amalga oshirilgan jinoyatlarni kvalifikatsiya qilishda masalani tugagan deb ham hisoblash mumkin. Buning uchun EHMni apparat va dasturiy ta‘minot kompleksi sifatida idrok etish mumkin. Qalbaki plastik kartochka yordamida xarid uchun haq to‘langanda yoki bankdagi bir hisob raqamdan boshqasiga pul mablag‘i g‘ayriqonuniy yoki haq to‘lanmay o‘tkazilganda esa qilmish muayyan shakldagi talon-torojlik deb baholanishi lozim.

Axborot texnologiyalari sohasidagi jinoyatlar tarkiblarining **ob‘ektiv tomoni** aksariyat hollarda moddiy tarkib sifatida ifodalanadi. Shu bois nafaqat ijtimoiy xavfli qilmishning sodir etilishi, balki ijtimoiy xavfli oqibatlarining yuz berishi, shuningdek qilmish bilan yuz bergan oqibat o‘rtasidagi sababiy aloqa aniqlanishi ham nazarda tutiladi. Jinoyatlarning alohida tarkiblari (JK 278³ va 278⁶-moddalar) qonunda formal tarkib sifatida ifodalangan. Ularning tugash payti sifatida, oqibatlari qachon yuz berishidan qat‘i nazar, harakat yoki harakatsizlikning sodir etilish vaqti ko‘rsatilgan. Ijtimoiy xavfli qilmishlarning o‘zi esa mazkur jinoyatlarga tatbiqan harakatlar shaklida namoyon bo‘ladi va ba‘zan harakatsizlik bo‘lishi mumkin. Bir holatda jinoyat tarkibi ob‘ektiv tomonining bunday belgisi, jinoyatni sodir etish usuli sifatida, asosiy va og‘irlashtiruvchi holatlarga ega tarkiblarining majburiy belgisi sifatida ifodalanadi. Qolgan hollarda jinoyat tarkibi, shuningdek sodir etilish joyi, vaqti, quroli, vositalari, vaziyati sud tomonidan aybni yengillashtiruvchi yoki og‘irlashtiruvchi holatlar sifatida inobatga olinishi mumkin.

¹ Qarang: Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Ресурс Интернет: http://kurgan.unets.ru/~procur/my_page.htm, 1999.

Axborot texnologiyalari sohasidagi jinoyatlar turli EHM, apparat vositalari, periferiya (atrof) qurilmalari va aloqa liniyalaridan foydalanilgan holda sodir etiladi. Bu, o'z navbatida, jinoyatning sodir etilish joyi haqidagi masalaning qo'yilishiga sabab bo'ladi. Dunyoning deyarli barcha mamlakatlaridagi vakillarni birlashtirgan jahon axborot tarmog'i (INTERNET)ning yaratilishi qilmishni zararli oqibatlar kelib chiqadigan joydan uzoqda sodir etishga ham imkon beradi. Bunday hollarda rossiyalik tadqiqotchilar YU. I. Lyapunov va A. V. Pushkin, jinoyat sodir etish joyi deganda, oqibatlar yuz beradigan joyning qayerda ekanligidan qat'i nazar, qilmish (harakat yoki harakatsizlik) sodir etilgan davlatning hududini tushunadilar. Masalani bunday hal etishda ushbu mualliflar Rossiya Federatsiyasi Jinoyat kodeksining 9-moddasi 2-qismida, oqibatlari qachon yuz berishidan qat'i nazar, qilmish sodir etilgan vaqt jinoyat sodir etish vaqti deb topilishiga asoslanadilar¹. Biroq, yuqoridagi qoidaga zaruriy aniqliklar kiritmay turib, uni O'zbekiston Respublikasi jinoyat qonuni hujjatlariga qabul qilish mumkin emas, chunki u O'zbekiston Respublikasi Jinoyat kodeksining 13-moddasi 1-qismiga ziddir. Ushbu moddaga muvofiq jinoyatning sodir etilish vaqti qanday (formal yoki moddiy tarkibli) jinoyat sodir etilganligiga qarab aniqlanadi belgilangan. Formal tarkibli jinoyatning sodir etilish vaqti deb ijtimoiy xavfli qilmish amalga oshirilgan vaqtni, moddiy tarkibli jinoyatning sodir etilish vaqti deb esa jinoyat qonunida nazarda tutilgan jinoiy oqibatlarning yuz berish vaqtini tan olish lozim². Binobarin, axborot texnologiyalari sohasidagi formal tarkibli jinoyatlarning sodir etilish joyi – ijtimoiy xavfli qilmish sodir etilgan davlat hududi, moddiy tarkibli jinoyatning sodir etilish joyi esa oqibatlar yuz bergan (axborot yo'q qilib yuborilgan, modifikatsiyalashtirilgan, to'sib qo'yilgan, nusxa ko'chirilgan) mamlakat hududi hisoblanadi.

Axborot texnologiyalari sohasidagi jinoyatlarning **sub'ektiv tomoni** aybning to'g'ri yoki egri ko'rinishidagi qasd shakli bilan tavsiflanadi. Faqatgina bitta jinoyat, ya'ni axborotlashtirish qoidalarini buzganlik uchun javobgarlikni

¹ Qarang: Уголовное право. Особенная часть. – М.,1998. – С.546.

² Qarang: Уголовное право. Общая часть / А.С.Якубов, Р. Кабулов и др. – Т., 2005. – С. 112-119.

belgilovchi JK 278¹-moddasidagi jinoyat ham qasddan, ham ehtiyotsizlik tufayli sodir etilishi mumkin.

Qonun chiqaruvchi tomonidan ikkita jinoyat uchun, JK 278³ va 278⁶ – moddalarida jinoyat sub’ektiv tomonining zaruriy belgisi sifatida *maqsad* belgilangan. Boshqa holatlarda motiv va maqsad jinoyatlarning zaruriy belgisi sifatida ko’rsatilmagan, lekin ularning belgilanishi jazoni individuallashtirish uchun katta ahamiyat kasb etadi. Ushbu jinoyatlar g’arazdan, bezorilik maqsadida, o’ch olish niyatida, “sport manfaatlari uchun”, shuningdek, siyosiy va boshqa manfaatlar motivida sodir etilishi mumkin. Mazkur turdagi jinoyatlar ustunlikka intilish, zavq olish hohishi, boshqa jinoyatlarni yashirish kabi maqsadlarda sodir etilishi mumkin.

Axborot texnologiyalari sohasidagi jinoyatlarning **sub’ekti** aqli raso, 16 yoshga to’lgan, axborotlarni qo’riqlash majburiyatiga ega yoki kompyuter axborotlariga qonunga xilof ravishda kirgan shaxslar hisoblanadi.

Psixofiziologik tavsif nuqtai nazaridan, ular ijodkor shaxs, mutaxassis, texnik chaqiruvga tavakkal bora oluvchilar. Hozirgi kunda yirik kompaniyalar tajribali xakerlarni axborot va kompyuter tizimlariga himoya tizimini yaratish maqsadida ishga olishga harakat qilmoqdalar.

Ekspert tadqiqot materiallaridan xulosa qilish mumkinki, jinoyat sodir etish vaqtida 20 yoshga yyetmaganlar 33%, 20 – 40 yoshdagilar 54 %, 40 yoshdan oshganlar 13 %ni tashkil etgan. O’tkazilgan tadqiqot natijalari xakerlarni 13 yoshdan 20 yoshgacha bo’lgan o’smirlar tashkil qiladi degan taxminlarni inkor etadi.

Kompyuter texnologiyalaridan foydalanish sohasidagi jinoyatlarni erkaklar besh martagacha ko’p sodir etishadi. Bunday jinoyatlar sub’ektining ko’pchiligi oliy yoki tugallanmagan oliy texnik ma’lumotlilar (53,7%), qolganlari esa oliy ma’lumotlilar, shuningdek tugallanmagan oliy ma’lumotlilar (19,2%) hisoblanishadi.

So’ngi vaqtlarda ularning safida ayollarning ulushi ortib bormoqda. Bu aksariyat hollarda ayollar tomonidan (kotiba, hisobchi, iqtisodchi, menedjer,

g'aznachi, nazoratchi kabilar) kompyuter asbob-uskunalarini bilan bog'liq ko'pgina ish joylari, mutaxassisliklar va mansablarning egallanishi bilan bog'liqdir.

Kriminologik tadqiqotlarning guvohlik berishicha, jinoyatchilarning 52% ini kompyuter axbortlarini ishlab chiqish sohasida maxsus tayyorgarlik ko'rganlar; 97% ini kundalik ish faoliyatida kompyuter tizimi va axborot texnologiyalaridan foydalanuvchi davlat tashkiloti va muassasalarining xodimlari; 30%ini kompyuter vositalari texnikalarining ekspluatatsiya qilishga bevosita munosabatda bo'lgan huquqbuzarlar tashkil etadi¹.

Xulosa tariqasida aytish mumkinki, axborot texnologiyalari sohasidagi jinoyatlarni sodir etuvchi shaxslarning doirasi nisbatan keng. Tadqiqot natijalaridan ko'rinib turibdiki, jinoyat sub'ektlari jamiyatning turli qatlam vakillaridan, 16 dan 60 yoshgacha, tayyorgarlik darajasi esa – tajribasizlardan tortib, mutaxassislargacha yoki kompyuter texnikasi sohasida minimal bilimga ega bo'lgan barcha yoshdagi shaxslar bo'lishi mumkin.

Ob'ektiv va sub'ektiv belgilarning tahlilidan kelib chiqib, mazkur jinoyatlarga quyidagicha ta'rif berish mumkin: *kompyuter axborotlaridan huquqiy va xavfsiz foydalanishdagi ijtimoiy munosabatlarga zarar yetkazish yoxud zarar yetkazish xavfini keltirib chiqaruvchi, aybli, jinoiy jazoga sazovor ijtimoiy xavfli qilmish axborot texnologiyalari sohasidagi jinoyatlar* deyiladi.

Axborot texnologiyalari sohasidagi jinoyatlarning ijtimoiy xavfliligi quyidagi holatlarda sezilarli darajada oshadi: a) bir guruh shaxslar tomonidan oldindan til biriktirib; b) takroran va xavfli retsivist tomonidan; v) uyushgan guruh tomonidan yoki uning manfaatlarini ko'zlab; g) juda ko'p miqdorda zarar yetkazgan holda sodir etilgan bo'lsa.

Bunday zaruriy belgilar JK 278¹-moddasida ko'rsatilgan jinoyat tarkibidan tashqari axborot texnologiyalari sohasidagi jinoyatlarning barcha turining "a" va "b" bandlarida mavjud. Jinoyatning uyushgan guruh tomonidan yoki uning manfaatlarini ko'zlab sodir etilishi JK 278², 278³, 278⁶-moddalari ikkinchi

¹ Qarang.: Крылов В.В. Информационные компьютерные преступления: Учебное и практическое пособие. – М., 1997. – С. 40-44; Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. – Красноярск, 202. – С. 8 – 14; 62-64.

qismining kvalifikatsiyaga oid belgisi hisoblanadi. Juda ko'p miqdorda zarar yetkazilishiga sabab bo'lish JK 278¹, 278⁴, 278⁶-moddalarida ikkinchi qismining kvalifikatsiyaga oid belgisi hisoblanadi¹.

JK 29-moddasi 3-qismiga muvofiq, jinoyatda ikki yoki undan ortiq shaxs birgalikda jinoyat sodir etish uchun oldindan til biriktirgan bo'lsa jinoyat bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilgan deyiladi. Axborot texnologiyalari sohasidagi jinoyatlarda jinoyat sodir etishga kelishuv (jinoyatning ob'ektiv tomoni belgilarini bajarishdan oldin yoxud to'satdan paydo bo'lgan qasd natijasida, bevosita bajarishdan oldin bo'lishini bildiradi.

Birgalikda bajaruvchilik yoki ishtirokchilikda oldindan til biriktirish deganda tor ma'noda, jinoyat sodir etishdagi vazifalarning taqsimlanishi (bajaruvchi, yordamchi, dalolatchi, tashkilotchi), shuningdek guruhning barcha ishtirokchilari sub'ekt belgilariga ega bo'lgan holda jinoyat sodir etishga birgalikda qasd qilganligi tushuniladi.

Agar guruh tarkibida bitta ishtirokchi jinoyat sub'ekti bo'lsa-yu, qolganlari voyaga yetmaganligi uchun sub'ekt sanalmasa, oldindan til biriktirgan guruh mavjud emas deb hisoblanadi. Bunday holatda yagona sub'ekt axborot texnologiyalari sohasidagi jinoyatlarni sodir etganligi uchun, shuningdek u 18 yoshga to'lmaganlarni jinoyat sodir etishga undagan bo'lsa, voyaga yetmaganlarni g'ayriijtimoiy hatti-harakatlarga jalb qilganligi uchun (JK 127-moddasi 3-qismi) jinoyatlar majmui bo'yicha javobgarlikka tortiladi.

Shu o'rinda ta'kidlab o'tish lozimki, jinoyat sub'ekti hisoblangan shaxs javobgarlik yoshiga yetmagan shaxsni jinoyat sodir etishga majburlab, unda o'zi ishtirok etmagan bo'lsa, u javobgarlik yoshiga yetmagan shaxsdan qurol sifatida foydalanganligi uchun o'sha jinoyatning bajaruvchisi sifatida javobgarlikka tortiladi.

¹ Takrorlashning oldini olish maqsadida mualliflar ko'rsatilgan kvalifikatsiya qilish belgilarining mazmunini ishning bu qismida ko'rib chiqishni maqsadga muvofiq deb hisoblaydi. "Mansab mavqeidan foydalanib" jinoyat sodir etish kabi kvalifikatsiya belgisining mazmuni JKning 278² va 278³ -moddalarida nazarda tutilgan jinoyat tarkiblarini yuridik tahlil qilishda, yuridik tavsif berishda tahlil qilinadi.

JK 32-modda 1-qismiga muvofiq, takroran jinoyat sodir etish deganda, JK Maxsus qismining aynan bir moddasi, qismi yoki Kodeksda alohida ko'rsatilgan hollarda turli moddalarda nazarda tutilgan ikki yoki undan ortiq jinoyatlarni shaxs turli vaqtlarda sodir etganligi, ammo ularning birortasi uchun ham sudlanmaganligi tushuniladi.

Shu bilan birga oldin sodir etgan jinoyati tugallangan yoki yo'qligi, bajaruvchi yoki ishtirokchilikning boshqa turi sifatida jinoyat sodir etganligi ahamiyat kasb etmaydi. Axborot texnologiyalari sohasidagi jinoyatlarda takroriylik ikki yoki undan ortiq bir-biriga o'xshash jinoyatlardan tashkil topadi.

Bu esa takroran jinoyat sodir etish agarda xuddi shunday (bir-biriga o'xshash) ijtimoiy xavfli tajovuz sodir etganligini anglatadi. Misol uchun, kompyuter sabotaji agar shaxs tomonidan ikkinchi marotaba sodir etilgan va birinchi qilmishida JK 278⁵-moddasi 1-qismidagi jinoyat alomatlari mavjud bo'lib, javobgarlikka tortilmagan bo'lsa (JK 278⁵-moddasi 2-qismi "b" bandi), unda takroran sodir etilgan hisoblanadi. Tahlil qilinayotgan zaruriy belgi qancha va qanday ko'rinishda jinoyat sodir etilganligidan qat'i nazar inobatga olinadi. Asosiysi, oldingi sodir etgan o'xshash jinoyati JK 64-moddasi bo'yicha o'zining huquqiy ahamiyatini saqlab turgan bo'lishi lozim.

JK 34-moddasi 2-qismiga muvofiq, xavfli retsivist deganda, ilgari hukm qilingan jinoyatiga o'xshash jinoyat sodir etgan shaxsning qasddan yangi jinoyat sodir etishi tushuniladi. Axborot texnologiyalari sohasidagi jinoyatlarni xavfli retsivist tomonidan sodir etilgan deb kvalifikatsiya qilish uchun huquqni qo'llovchi organlar aybdorga ushbu belgini hisobga olgan holda ayblov taqdim qilishga majburdirlar. Shaxs ilgari JK 278²-moddasi 1-qismida ko'rsatilgan komp'yuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanganligi uchun sudlanib, yangidan shunga o'xshash jinoyat sodir etsa, JK 278²-moddasi 2-qismi "b" bandi bo'yicha (xavfli retsivist sifatida) javobgarlikka tortilishi lozim.

Ta'kidlash joizki, mazkur jinoyatlarni kvalifikatsiya qilishda zaruriy belgilarni hisobga olishning asosiy sharti sifatida, jazoni ijro etish muddatining (JK 69-moddasi) o'tib ketmaganligi yoki qonunda belgilangan tartibda sudlanganlik

holatining tugallanmaganligi yoki olib tashlanmaganligi yohud shaxsning ilgari sodir etilgan o'xshash jinoyati uchun sudlanganligi to'g'risidagi faktlar hisoblanadi.

Uyushgan guruh deganda, ikki yoki undan ortiq shaxsning birgalikda jinoiy faoliyat olib borish uchun oldindan bir guruhga birlashishi tushuniladi (JK 29-moddasi 4-qismi).

Guruh jinoiy faoliyatining uzoqqa cho'zilganligi, tarkibning o'zgarmasligi, aloqalarining mustahkamligi, lider (boshqaruvchi, tashkilotchi) orqali boshqa yaqin guruhlar bilan faoliyat sohasi bo'limida guruh ishtirokchilari orasidagi rollar va vazifalarining ierarxik taqsimlanganligi (vertikal va gorizontaal bo'yicha), jinoiy faoliyatni rejalashtirishda qattiq ichki intizom jinoiy guruhning uyushganligi deb tavsiflanadi¹.

Sanab o'tilgan belgilar u yoki bu munosiblikdagi belgilar mazkur turdagi jinoiy ko'rinishlarga taalluqli bo'lib, har qanday uyushgan guruhlarda o'zlarini ko'p yoki kam darajada namoyon qiladi. Bundan tashqari, guruhni uyushgan deb hisoblash uchun guruhning kompyuter axborotlarini noqonuniy va xavfsiz foydalanish sohasida jinoiy faoliyatni olib borish maqsadida tashkil etilganligini aniqlash zarur.

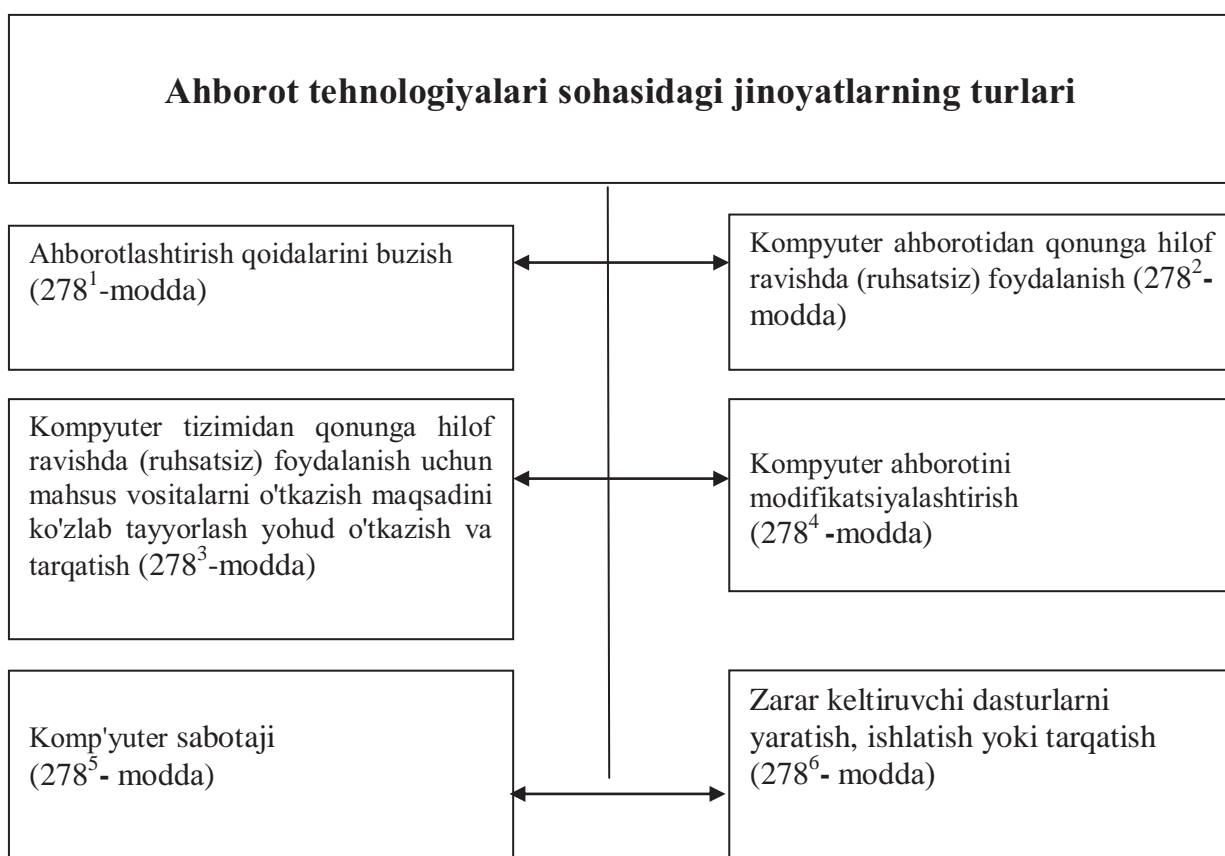
JK 278³ va 278⁶-moddalari 2-qismi "g" bandlarida uyushgan guruhni tashkil etgan yoki unga rahbarlik qilgan, shuningdek guruhning jinoyat sodir etishida qatnashgan shaxslarning jinoiy javobgarliklari asoslari, shartlari va hajmi, JK 30-moddasi 2-qismida esa guruhdagi ishtirokchilik to'g'risida so'z boradi. Bu kabi holatlarda, ma'lum bir jinoyat sodir etishda qanday rolni bajarganligidan qat'i nazar, uyushgan guruhning barcha a'zolari bajaruvchi sifatida (JK 28-moddasiga havola qilmasdan) javobgarlikka tortiladilar. Yuqorida ta'kidlangan JK Maxsus qism moddalaridagi kvalifikatsiya etish belgilari sifatida jinoyatning uyushgan guruh tomonidan yoki uning manfaatlarini ko'zlab sodir etilishi belgilanganligi sababli og'irlashtiruvchi holat sanaladi. Ularga ko'ra, jazo uyushgan guruh a'zosi bo'lmagan, lekin jinoyat sodir etishda uyushgan guruh tarkibida bir marotaba

¹ Qarang: Соттнев И.А. Уюшган жиноятчиликка қарши курашишнинг ҳуқуқий воситалари: Ўқув қўлланма – Т, 2005. – 30-43 б.

qatnashgan yoki uyushgan guruh manfaatlarini ko‘zlab, o‘z tashabbusi bilan yoxud uyushgan guruh buyrug‘i bilan jinoyatni mustaqil sodir etgan aybdor shaxslarga ham qo‘llaniladi.

JK 278¹-moddasi 2-qismi, 278⁴-moddasi 2-qismi “a” bandi va 278⁶-moddasi 2-qismi “a” bandlarida zaruriy belgi sifatida nazarda tutilgan juda ko‘p miqdordagi zarar eng kam oylik ish haqining uch yuz baravariga va undan ko‘pga teng hisoblanadi. Bunday holatda “zarar” tushunchasi nafaqat to‘g‘ridan-to‘g‘ri yetkazilgan zarar, balki boy berilgan foyda ham hisoblanadi. Alohida ta’kidlash lozimki, jinoyat sodir etilishi natijasida shaxs amalda juda ko‘p miqdordagi zarardan kamroq zarar yetkazgan, lekin aybdorning qasdi aynan shunday zarar yetkazilishiga yo‘naltirilgan bo‘lsa, mazkur jinoyat suiqasd qilish kabi kvalifikatsiya qilinadi.

O‘zbekiston Respublikasining jinoyat qonunchiligida axborot texnologiyalari sohasiga taalluqli oltita asosiy va kvalifikatsiyaga oid tarkiblarga ega jinoyatlar uchun javobgarliklar belgilangan. Ular quyidagi chizmada aks ettirilgan.



2. Axborotlashtirish qoidalarini buzish (JK 278¹-moddasi)

Ushbu jinoyatning ijtimoiy xavfliligi ijtimoiy-iqtisodiy va ilmiy-texnikaviy jarayonning tartibini buzish, axborot tizimlaridan foydalangan holda jismoniy va yuridik shaxslarning axborotga bo'lgan ehtiyojlarini qondirish uchun sharoitlar yaratmaslikdan iborat. Bunday axborotlashtirish qoidalarini buzganlik uchun jinoiy javobgarlikning belgilanishi axborot tizimidan foydalanuvchilar saqlanayotgan va ishlov berilayotgan axborotning saqlanishi va xavfsizligiga ta'sir etuvchi kasbiy majburiyatlarini bajarmasliklarining oldini olishga qaratilgan. Shu bois JK 278¹-moddasida nazarda tutilgan jinoyatning **bevosita ob'ekti** axborot tizimlari, ma'lumotlar bazalari va banklaridan qonuniy va xavfsiz foydalanilishini ta'minlovchi belgilangan qoidalarga rioya etish sohasidagi ijtimoiy munosabatlardan iborat. «Axborotlashtirish to'g'risida»gi O'zbekiston Respublikasi qonunining 3-moddasiga muvofiq, axborot tizimi deganda axborotni to'plash, saqlash, izlash, unga ishlov berish hamda undan foydalanish imkonini beradigan, tashkiliy jihatdan tartibga solingan jami axborot resurslari, axborot texnologiyalari va aloqa vositalari tushuniladi. Ma'lumotlar bazasi va banki axborot tizimining bir qismini tashkil qiladi. Ular ob'ektiv shaklda ifodalangan hamda elektron hisoblash mashinalari yordamida aniqlanish va qayta ishlanish imkonini beradigan tarzda tartibga solingan ma'lumotlar (masalan: maqolalar, hisob-kitoblar) majmui sifatida ta'riflanadi.

Ushbu jinoyatning **ob'ektiv tomoni** majburiy belgilar sifatida ijtimoiy xavfli qilmish, ijtimoiy xavfli oqibat va ular o'rtasidagi sababiy aloqani qamrab oladi.

Mazkur jinoyatni tashkil etuvchi ijtimoiy xavfli qilmishlarlar quyidagilardan iborat: axborot tizimlari, ma'lumotlar bazalari, va banklari va axborotga ishlov berish hamda uni uzatish tizimlarini yaratish, joriy etish va ulardan foydalanishda qonunga xilof ravishda faoliyat olib borish yoki belgilangan himoya choralarini ko'rmagan holda axborot tizimlaridan ruxsat bilan foydalanish qoidalarini buzish kabilar. Shu bilan birga, mazkur harakatlar o'z-o'zidan emas, balki foydalanuvchilarning axborot tizimi, ma'lumotlar bazalari va banklaridan foydalanishda himoya choralarini ta'minlamasliklari oqibatida yuz beradi.

«Axborotlashtirish to'g'risida»gi qonunning 20-moddasiga binoan, foydalanuvchilar hamma foydalanadigan axborot, davlat sirlari hamda maxfiy sirlar to'g'risidagi ma'lumotlarni o'z ichiga olgan axborot resursi va tizimlarining muhofaza qilinishini ta'minlashlari shart. Axborot tizimlarini muhofaza qilish shaxs, jamiyat va davlat xavfsizligiga tahdidlarning oldini olish, maxfiy axborotni saqlash, uning tarqalib ketishi, o'g'irlanishi, yo'qotilishi, buzib talqin etilishi, to'sib qo'yilishi, qalbakilashtirilishi va axborot tizimlariga boshqa shakllardagi noqonuniy aralashuvlarga yo'l qo'ymaslik maqsadida amalga oshiriladi.

Axborot tizimlarining muhofaza qilinishini tashkil etish tartibi ularning mulkdorlari, egalari tomonidan mustaqil belgilanadi.

Davlat sirlari hamda maxfiy sirlar to'g'risidagi ma'lumotlarni o'z ichiga olgan axborot resurslari va tizimlarining muhofaza qilinishini tashkil etish tartibi O'zbekiston Respublikasining Vazirlar Mahkamasi tomonidan belgilanadi.

Qonun chiqaruvchi organ ijtimoiy xavfli oqibatlar sifatida JK 278¹-moddasi 1-qismida fuqarolarning huquqlari, qonun bilan qo'riqlanadigan manfaatlari, davlat yoki jamoat manfaatlariga ko'p miqdorda zarar yoxud jiddiy ziyon yetkazilishini e'tirof etgan.

Ko'p miqdorda zarar deganda, eng kam oylik ish haqining 100 baravaridan 300 baravarigacha bo'lgan miqdordagi moddiy zarar yetkazilishi tushuniladi.

«Jiddiy ziyon» baholovchi tushuncha bo'lib, u qilmishning baholanishini inobatga olgan holda aniqlanadi. Jiddiy zarar deganda, texnologik jarayonning buzilishi, xo'jalik yurituvchi sub'ektning ishbilarmonlik obro'siga putur yetkazilishi, bolalarning farzandlikka olingani haqidagi ma'lumotlarni oshkor etish orqali shaxsga ma'naviy ziyon yetkazish kabilar tushuniladi.

Ushbu qonunda shaxsning axborotlashtirish qoidalarini buzganligi uchun JK 278¹-moddasi bo'yicha (agar bunday qonun buzilishi shaxs, jamiyat va davlatning qonun bilan qo'riqlanadigan manfaatlariga ko'p miqdorda zarar yoki jiddiy ziyon yetkaza olmasa) jinoiy javobgarlikka tortish mumkinligi istisno etiladi.

Xulosa qilib aytganda, mazkur jinoyatning tarkibi – moddiy. U qonunda ko'rsatilgan oqibatlar yuzaga kelgan paytdan boshlab tugallangan hisoblanadi.

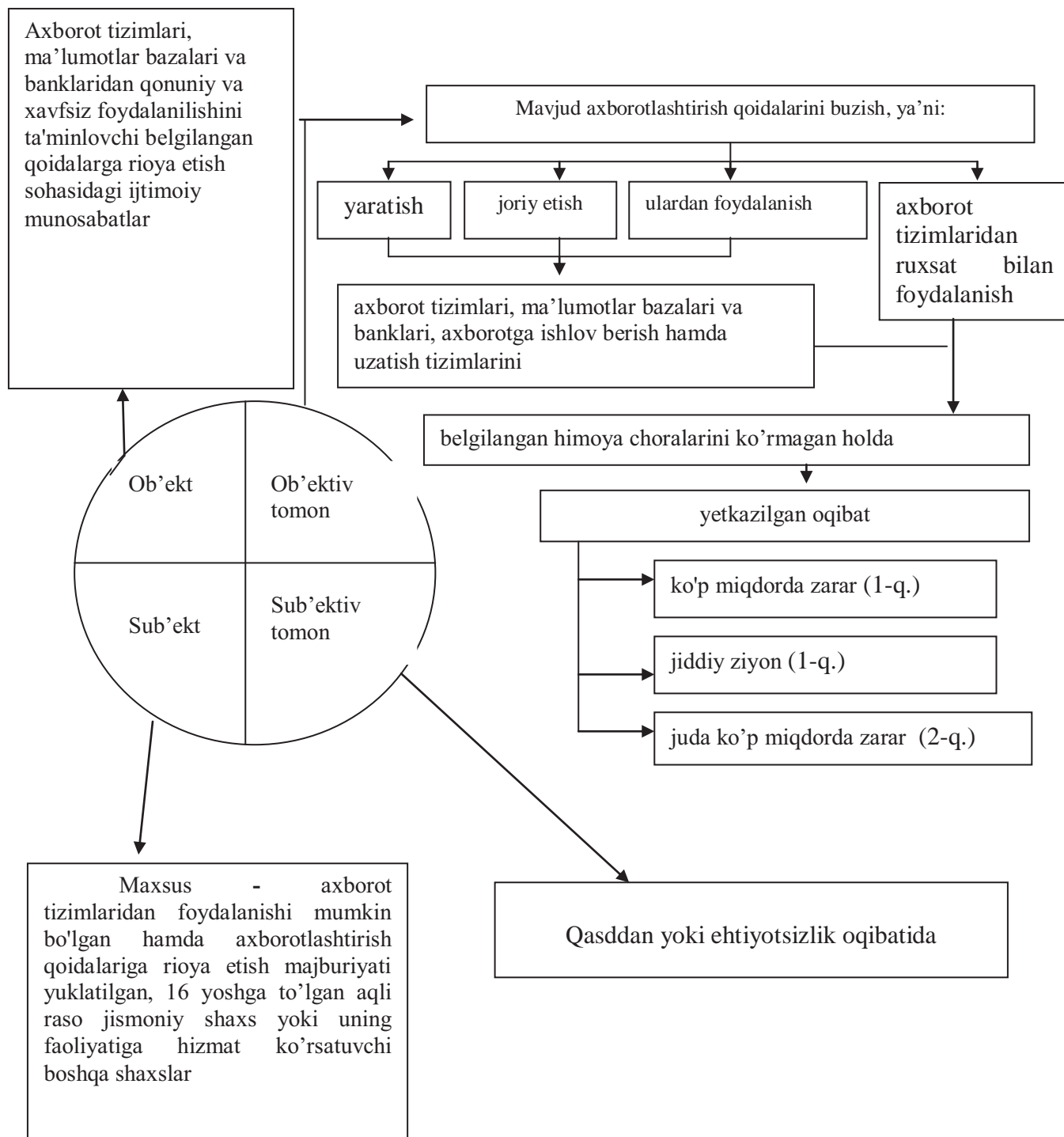
Ob'ektiv tomonni tahlil qilishda axborotlashtirish qoidalarining buzilishi bilan yetkazilgan zarar o'rtasidagi sababiy aloqani aniqlash juda muhim. Bundan tashqari, shuni nazarda tutish lozimki, kelib chiqqan oqibatlar dasturiy xato emas, balki axborotlashtirish qoidalarining buzilishi natijasidir.

Jinoyatning **sub'ektiv tomoni** qasd yoki ehtiyotsizlik shaklidagi aybda namoyon bo'ladi. Aybdor shaxs axborotlashtirish qoidalarini buzayotganligini anglaydi, o'z harakatlarining JK 278¹-moddasida ko'rsatilgan oqibatlarni keltirib chiqarishi mumkinligini oldindan biladi, ularning kelib chiqishini istaydi va ongli ravishda bunga yo'l qo'yadi. Yoxud shaxs ushbu oqibatlarni oldindan ko'radi va himoya choralariga rioya etmagan holda, asossiz ravishda ularning oldini olishga umid qiladi. Shuningdek, shaxs ushbu oqibatlarining kelib chiqishini oldindan bilmaydi, holbuki lozim darajadagi ehtiyotkorlik bo'lsa ularni oldindan ko'rishi mumkin bo'ladi.

Motiv va maqsad turli – tuman bo'lishi mumkin. Ularning aniqlanishi qilmishning kvalifikatsiyasiga ta'sir etmaydi.

Jinoyat **sub'ekti** – maxsus. Bajaradigan mehnati va kasbiy faoliyatining xususiyatlariga ko'ra, axborot tizimi, ma'lumotlar bazasi va bankidan to'sqinliksiz foydalana oladigan, qonun yoki boshqa normativ hujjatlar bilan axborotlashtirish qoidalariga rioya etish majburiyati yuklatilgan, 16 yoshga to'lgan aqli raso jismoniy shaxs jinoyat sub'ekti bo'lishi mumkin. Axborot tizimlaridan foydalanishga ruxsat etilgan shaxslar sifatida bevosita EHMda ishlaydigan yoki uning ishiga xizmat ko'rsatuvchilar (EHM operatorlari, dasturchilar, EHM tizimining abonentlari va boshqa foydalanuvchilar)ni kiritish mumkin.

Jinoyat kodeksi 278¹-moddasida nazarda tutilgan jinoyat tarkibini quyidagi chizma orqali ifodalash mumkin:



3. Kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish (JK 278²-moddasi)

Mazkur jinoyatning ijtimoiy xavfliligi favqulodda xususiyatga ega, chunki axborotning yo‘q qilinishi, to‘sib qo‘yilishi, modifikatsiyalashtirilishi, undan nusxa ko‘chirilishi yoxud uning noqonuniy qo‘lga kiritilishiga erishish, EHM, uning tizimi yoki tarmog‘i ishining buzilishi ushbu vositalarning mulkdori uchun ham, jamiyat uchun ham ulkan salbiy oqibatlarni keltirib chiqarishi mumkin.

Tizimga bunday kirishning oqibatlari haqida so‘z yuritganda, avvalo ularning dixotom xususiyatga ega ekanligini qayd etish lozim. Birinchidan, bevosita zarar noqonuniy ta’sirga duchor etilayotgan kompyuter tizimiga yetkaziladi. Ikkinchidan, elektron monitoring predmetiga, ya’ni texnologik jarayonlar, ishlab chiqarish, iste’mol, sog‘liqni saqlash, mudofa, jamoat xavfsizligi, energo-gidroresurslar, transport xizmatlari, telefon va telemetrik aloqa bilan ta’minlashning turli sohalari va boshqa jarayonlarga qayta tiklab bo‘lmas darajada zarar yetkazish mumkin.

Jinoyatning **bevosita ob’ekti** kompyuter axborotining xavfsizligi, EHM, uning tizimi yoki tarmog‘ining xavfsizligini ta’minlovchi munosabatlardir.

Mazkur jinoyatning predmetini davlat siri, mualliflik huquqi, mulk, insonning shaxsiy hayoti, tergov va sudlov sirlari, xizmat, kasb va tijorat siri kabilar haqidagi qonun hujjatlari bilan muhofaza etiladigan axborot tashkil etishi mumkin.

Davlat siriga ega bo‘lgan axborot harbiy, tashqi siyosiy, iqtisodiy, razvedka, kontrrazvedka va operativ qidiruv faoliyat sohasidagi ma’lumotlarni o‘z ichiga oladi.

O‘zbekiston Respublikasi Konstitutsiyasining 27-moddasiga muvofiq, shaxsning shaxsiy hayoti haqidagi ma’lumotlarni uning roziligisiz to‘plash, saqlash, ishlatish va tarqatishga yo‘l qo‘yilmaydi. «Shaxsiy hayot» tushunchasiga davlat, jamoat tashkilotlari, fuqarolar tomonidan nazorat qilinishi mumkin bo‘lmagan insonning oilaviy, maishiy, shaxsiy, intim munosabatlari sohasidagi hayoti va faoliyati kiradi.

Fuqarolik kodeksining 98-moddasiga binoan, xizmat va tijorat siri axborot

haqiqiy yoki imkoniyatdagi tijorat qiymatiga ega bo'lganida mavjud bo'ladi. Shu bois, axborot boshqa shaxslarga ma'lum emasligi tufayli undan erkin foydalanish qonuniy asosda cheklanadi va axborot egasi uning maxfiylikini saqlash choralarini ko'radi. Kasbiy axborot yuridik, tibbiy, pedagogik va boshqa sohalardagi inson faoliyatiga doir ma'lumotlarga ega bo'ladi.

JK 278²-moddasining normasida axborot mashina tashuvchisi, EHM, uning tizimi yoki tarmog'ida qonunga xilof tarzda bo'lganida axborotdan noqonuniy foydalanganlik uchun javobgarlik nazarda tutilgan. EHM xotirasidagi kompyuter axboroti moddiy tashuvchilar orqali bir joydan ikkinchi joyga tashiladi. Ularga disk, fleshka, disketa, magnit lentasi, EHMning apparat-texnik qismi va dasturiy ta'minoti kabilar kiradi. Kompyuter axboroti qayerda bo'lmasin va qayerda aylanmasin (EHM xotirasida, aloqa kanallarida, magnit tashuvchilarda) qonun bilan muhofaza etiladi (JK 278²-m.).

Mazkur jinoyatning **ob'ektiv tomoniga** aybdorning kompyuter axboroti yoki axborot resurslari (tizimlardagi hujjatli axborot massivlari)dan noqonuniy foydalanishida namoyon bo'ladigan harakatlari xos. Kompyuter axborotidan noqonuniy foydalanish EHM, uning tizimi yoki tarmog'idan foydalanish orqali axborotga ishlov berish texnologik jarayonining barcha bosqichlarida (ma'lumotlarni to'plash va tashuvchilarga ko'chirish; axborot massivini shakllantirish va EHM xotirasiga kiritish, axborotni aloqa kanallari orqali uzatishda) amalga oshirilishi mumkin.

Qonunda kompyuter axborotidan noqonuniy foydalanish usullari ko'rsatilmagan. Ular turlicha bo'lib, ko'plab omillarga bog'liq. Masalan o'zganing axborot tizimiga kirish, dasturning tuzilish mantig'idagi xatodan foydalanish yoki ulanish keltirib chiqargan xatolar oqibatida, avtomatlashgan tizimlar himoyasining o'jiz joylarini aniqlash (muhofaza tizimini bevosita buzish) orqali, kompyuter ishi tugaganidan so'ng yoki uning qonuniy foydalanuvchisidan keyin axborotni kompyuterdan o'qib olish natijasida birovning nomi (paroli)dan foydalanish, ishlab turgan EHMning elektromagnit nurlarini tutib qolish texnikasi vositalaridan foydalanish kabilar shular jumlasidandir.

Agar shaxs axborotdan foydalanish huquqiga ega bo'lmasa yoki shunday huquqqa ega bo'lsayu, uni belgilangan tartibda va axborotni himoya qilish qoidalarini buzgan holda amalga oshirsa, kompyuter axborotidan foydalanishni qonunga xilof deb hisoblash lozim.

«Axborotlashtirish to'g'risida»gi qonunning 11-moddasi 1-qismiga muvofiq, g'ayriqonuniy munosabatda bo'lish natijasida axborot resurslari yoki tizimlarining mulkdorlari, egalari yoxud boshqa yuridik hamda jismoniy shaxslarga zarar yetkazilishi mumkin bo'lsa, muhofaza qilinishi kerak. Biroq faqat g'ayriqonuniy munosabat bilan cheklanib qolish mumkin emas, chunki JK 278²-moddasi 1-qismidagi dispozitsiya g'ayriqonuniy munosabat bilan cheklanib qolmaydi, balki aybdorning kompyuter tizimiga kirish uchun huquqi (ruxsati) yo'qligini nazarda tutadi yoxud u axborotdan foydalanish huquqiga ega bo'ladiyu, biroq axborotni tizimga kirishning belgilangan tartibini buzish orqali oladi.

Tizimga kirishning belgilangan tartibi muhofaza qilishning muayyan dasturiy tizimiga ega. U axborot mulkdori tomonidan yoxud uning buyurtmasi bo'yicha yaratiladi (ko'pincha namunaviy muhofaza qilish vositalaridan foydalaniladi).

JK 278²-moddasi 1-qismida nazarda tutilgan jinoyatning ob'ektiv tomonining majburiy belgisi axborotni yo'q qilib yuborish, to'sib qo'yish, modifikatsiyalashtirish, undan nusxa ko'chirish yoxud uni qo'lga kiritish, EHM ishi, tizimi yoki tarmog'ini buzish kabilardan iborat. Ushbu jinoyat moddiy bo'lib, sanab o'tilgan oqibatlar kelib chiqqan taqdirda tugallangan hisoblanadi.

Aybdor kompyuter axboroti, egasi va mulkdoriga axborotni uni yo'q qilish, to'sib qo'yish, modifikatsiyalashtirish kabi yo'lar bilan zarar yetkazadi. Mazkur oqibatlarning kelib chiqishi bilan kompyuter axborotidan noqonuniy foydalanish o'rtasidagi sababiy aloqa aniqlanishi lozim.

Axborotni yo'q qilib yuborish deganda, axborot tashuvchisini batamom yoki qisman yo'q qilish tushuniladi. Bu esa uning sifat belgilari, mohiyati yo'qotilishini keltirib chiqaradi.

Yo'q qilib yuborilgan axborotni dasturiy ta'minot vositalari yordamida tiklash yoki uni boshqa foydalanuvchidan olish mavjud imkoniyatlari axborotdan

noqonuniy foydalanish hisoblanadi va uning ilgari yo‘q qilib yuborilgani javobgarlikni istisno etmaydi. Axborotni yo‘q qilib yuborish eng xavfli hodisa bo‘lib uning oqibatida axborotning egasi yoki mulkdoriga eng ko‘p darajada real zarar yetadi.

Kompyuter axborotini *to‘shib qo‘yish* – kompyuter axboroti saqlanib qolgan holda u bilan hech qanday operatsiyalarni amalga oshirib bo‘lmasligiga olib keladigan harakatlarning sodir etilishi. Axborotni to‘shib qo‘yish operatsiyalari huquqbuzar tomonidan axborot mulkdorining ma‘lumotlaridan o‘z ehtiyojlari maqsadida foydalanishiga to‘sqinlik qiluvchi parollar va qulflar qo‘yilishi bilan bog‘liq.

Kompyuter axborotini *modifikatsiyalashtirish* uning dastlabki holatini o‘zgartirishda (fayllardagi yozuvlarni o‘chirish yoki qo‘shib qo‘yish, ma‘lumotlar bazalarini boshqa tilga o‘tkazish kabilarda) namoyon bo‘ladi. EHM uchun dasturlar yoki ma‘lumotlar bazalarini adaptatsiyalash (moslashtirish) O‘zbekiston Respublikasining «Elektron hisoblash mashinalari uchun dasturlar va ma‘lumotlar bazalarini huquqiy muhofaza qilish to‘g‘risida»gi qonunining 12-moddasi 2-qismiga ko‘ra, kompyuter axborotini modifikatsiyalashtirish hisoblanmaydi.

Nusxa ko‘chirish deganda, kompyuter axborotini mashina yoki boshqa tashuvchiga o‘tkazish tushuniladi (masalan, EHMning ichki xotirasidagi faylni disketa, flesh-kartaga yozish, uni bosib chiqarish va hokazo sh.k.).

Kompyuter axborotini *qo‘lga kiritish* axborotni egallab olish va ushlab turishdir. Buning natijasida axborotning qonuniy egasi yoki foydalanuvchisi axborot bilan tanishish yoki undan foydalanish imkoniyatidan mahrum bo‘ladi yoxud uning raqobatchisi olingan axborotdan foydalanib, axborotning haqiqiy mulkdori uchun ma‘lum muddat ichida noqulay sharoitlar yaratishga ulguradi. Bundan tashqari, moliyaviy hisobvaraqa egasi elektron imzosining qo‘lga kiritilishi jinoyatchiga jabrlanuvchining moliyaviy mablag‘larini tasarruf etish uchun qulay sharoit yaratadi yoxud aybdorning maxfiy yoki boshqa muhim axborotdan foydalanishiga imkon beradi.

EHM, uning tizimi yoki tarmoqlari ishining buzilishi axborotga avtomat

tarzda ishlov berish uchun mo'ljallangan texnik vositalar ishidagi muvaqqat yoki barqaror uzilish bo'lib, bu ularni tiklash imkoniyatini yo'q qilmaydi. Bunday holat dasturiy ta'minotning ishdan chiqishi, monitorda noto'g'ri ko'rsatilishi, komandalarni bajarish tartibidagi nosozlik va chalkashliklar, buzilgan axborotning berilishi yoxud axborotni tushunarsiz kriptografik belgilarda tasvirlanishi kabilarda namoyon bo'lishi mumkin.

Mazkur jinoyatning **sub'ektiv tomoniga** bevosita yoki bilvosita (to'g'ri yoki egri) qasd ko'rinishidagi g'arazli ayb xosdir.

Aybdor ushbu jinoyatni sodir etayotganida qonun bilan muhofaza etiladigan kompyuter axborotidan qonunga xilof tarzda foydalanayotganligini anglaydi va o'z harakatlari natijasida axborotni yo'q qilib yuborish, to'sib qo'yish, modifikatsiyalashtirish, undan nusxa ko'chirish yoxud uni qo'lga kiritish, EHM, uning tizimi yoki tarmoqlari ishida buzishlar kelib chiqishi mumkin yoki muqarrarligini oldindan biladi hamda yuqoridagi kabi zararli oqibatlar kelib chiqishini istaydi yoki bila turib bunga yo'l qo'yadi yoxud ularning kelib chiqishiga befarq munosabatda bo'ladi.

Jinoyatning motiv va maqsadlari turlicha: g'arazdan tortib bezorilik maqsadlarigacha.

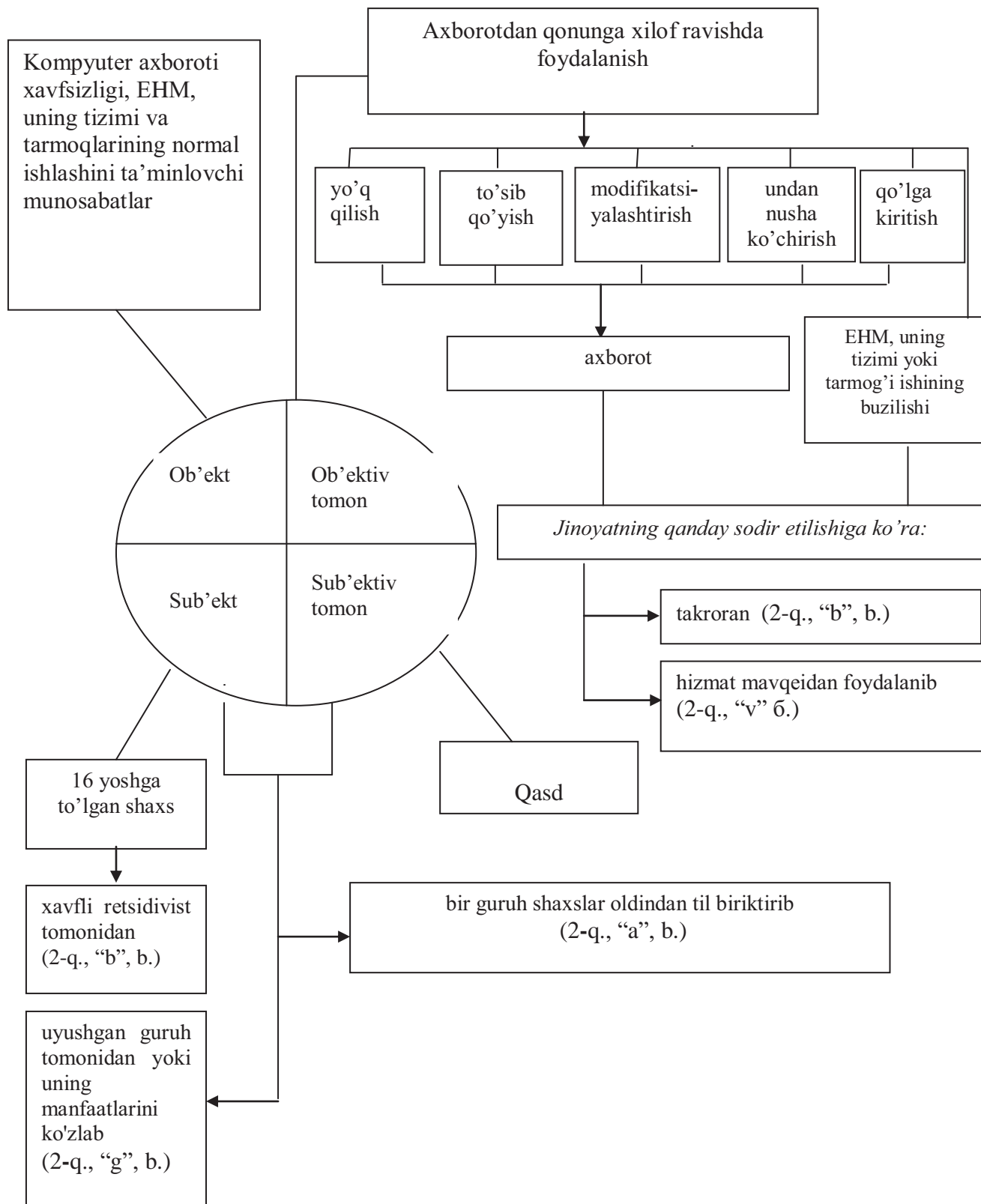
Jinoyatning **sub'ekti** 16 yoshga to'lgan, qonun bilan muhofaza etilayotgan kompyuter axborotidan qonunga xilof ravishda foydalangan va bu bilan qonunda ko'rsatilgan oqibatlarni keltirib chiqargan har qanday aqli raso jismoniy shaxs bo'lishi mumkin.

Shaxsning xizmat mavqeidan foydalangan holda kompyuter axborotidan qonunga xilof ravishda foydalanishi mazkur sohadagi jinoyatlarning og'ir turlaridan va u JK 278²-moddasining 2-qismi «v» bandiga muvofiq tavsiflanadi (kvalifikatsiya qilinadi).

Xizmat mavqeidan foydalanish deganda, qonun bilan muhofaza etilayotgan kompyuter axborotidan aybdorning egallab turgan xizmat mavqei yoki xizmatdagi bunday axborotdan foydalanish uchun ruxsati bo'lgan shaxslarga ta'siri natijasida foydalanishi tushunilmog'i lozim.

Jinoyat kodeksining 278²-moddasida nazarda tutilgan jinoyat tarkibini

quyidagi chizma orqali ifodalash mumkin:



4. Kompyuter tizimidan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o'tkazish maqsadini ko'zlab tayyorlash yoxud o'tkazish va tarqatish (JK 278³-moddasi)

Himoyalangan kompyuter tizimi yoki tarmog'idan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus dastur yoki apparat vositalarini o'tkazish yoxud shu maqsadni ko'zlab tayyorlash va tarqatishning ijtimoiy xavfliligi shundaki, bunday turdagi jinoyatlarni hattoki maxsus bilimlarga ega bo'lmagan har qanday foydalanuvchi ham sodir etishi mumkin.

Kompyuter texnologiyalari sohasidagi jinoyatlarni keltirib chiqaruvchi dasturlardan bu sohada yetarli bilimlarga ega bo'lmagan shaxslarning foydalanishi EHMdan xavfsiz foydalanish imkoniyatining yo'qolishiga olib kelishi mumkin.

Mazkur jinoyatning bevosita ob'ekti – kompyuter axborotlaridan xavfsiz va qonuniy foydalanishni tartibga soladigan ijtimoiy munosabatlar. Jinoyatning *predmeti* esa, kompyuter axboroti hisoblanadi.

Ushbu **jinoyatning ob'ektiv tomoni** himoyalangan kompyuter tizimi yoki tarmog'idan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus dastur yoki apparat vositalarini o'tkazish yoxud shu maqsadni ko'zlab tayyorlash va tarqatish harakatlarida namoyon bo'ladi. Yuqorida ta'kidlangan harakatlardan hattoki bittasining sodir etilishi ham aybdorni JK 278³-modda birinchi qismi bo'yicha javogarlikka tortish uchun asos bo'ladi.

Maxsus dastur yoki apparat vositalarini tayyorlash deganda qonunga xilof ravishda ularni to'liq yaratish, ularning mazmuniga qo'shimcha va o'zgartirishlar kiritish orqali mavjud bo'lgan vositalarni qalbakilashtirish ko'zda tutiladi.

Maxsus dastur va vositalarni tayyorlash texnologiyalari kompyuter texnikasi ishlab chiqarilishining zamonaviy rivojlangan holati bilan tavsiflanadi va ularning manbalari sifatida «Intel», «Microsoft», «Apple», «IBM PC» kompaniyalari hisoblanadi. Ular kompyuter bilan birga kompyuter dasturlarini ham ishlab chiqadilar. Mazkur kompaniyalar ishlab chiqqan rasmiy dasturlar asosida keyinchalik yangi dasturlarni ishlab chiqishda tegishli kasbiy qobiliyatga ega bo'lgan aybdor shaxslar qonunga xilof tarzda ularni modifikatsiya qiladilar yoki

elektron qulf va shifr (kod)larni ochish uchun maxsus mo'ljallangan kriminal (jinoiy) dasturlarni yaratadilar, jabrlanuvchilarning tijorat, xizmat yoki boshqa sirlarini fosh etish maqsadida noqonuniy faoliyat bilan shug'ullanadilar.

Maxsus dastur yoki apparat vositalarini o'tkazish deganda, himoyalangan kompyuter tizimi yoki tarmog'idan qonunga xilof ravishda (ruxsatsiz) foydalanishni ko'zlab tayyorlangan yoki tuzatishlar kiritilgan maxsus dastur yoki apparat vositalarini turli usullar bilan o'tkazish (masalan: sotish, almashtirish, qarzga berib yuborish kabilar)ni tushunish lozim.

Maxsus dastur yoki apparat vositalarini tarqatish deganda, bir shaxsga maxsus dastur yoki apparat vositalarini berib yuborish, jo'natish, sovg'a (hadya) qilish kabi hatti-harakatlar tushuniladi.

Qonunga xilof ravishda (ruxsatsiz) foydalaniladigan vositalar *maxsus dastur va apparatlarga* bo'linadi.

Maxsus dastur deganda, *birinchidan*, dasturiy-matematik ta'sir etuvchi, axborotlarni buzilishga, yo'q qilishga yoki og'dirishga olib keluvchi yoxud hisoblash texnikasi vositalarining ishini izdan chiqaruvchi vositalar; *ikkinchidan*, texnik vositalar (terminallar, kirish-chiqishning guruhiy boshqarish vositalari, EHM, axborotlarni saqlash vositalari) identifikatsiyasi, vazifa va foydalanuvchilarni chetlab o'tishga imkoniyat beruvchi vositalar; *uchinchidan*, axborot (axborotlarni qayta ishlashning texnik vositalari va vazifalarini foydalanishga ruxsat etilgan ish vaqti va kuni)dan foydalanuvchilar (iste'molchilar)ning huquqlarini o'zgartiruvchi vositalar; *to'rtinchidan*, foydalanuvchilar va texnik vositalar ishlashining nazoratini chetlab o'tishga imkoniyat beruvchi vositalar.

Qonunga xilof ravishda foydalanish maqsadida ishlab chiqarilgan dasturlarni quyidagi kategoriyalarga ajratish mumkin: a) amaliy dasturlar va operatsion tizimlarda ma'lum bo'lgan xatolar yordamida ruxsatsiz foydalanishga imkon beradigan stsenariyalar yoki shunday dasturlar; b) ko'p qo'llaniladigan parollarni va lug'at bo'yicha kodlashtirilgan yoki parollashtirilgan axborotlarni ochish uchun mo'ljallangan dasturlar; v) elektron pochta orqali berilayotgan

axborotlardagi matnlar, ma'lumotlar bazasidan chiquvchi parollashtirilgan va jiddiy axborotlarni ajratib olishga imkon beruvchi tarmoqli trafikning filtratsiyali tizimi; g) foydalanuvchi tizimiga qalloblarga kirishni taqdim etadigan "Backdoor" funktsiyali troyan dasturlar.

Maxsus apparatlar shunday vositalarki, ular elektromagnit nurlanish va qaratish, shuningdek elektroakustik qayta tashkil etilishlar natijasidan qayta ishlanadigan axborotlarni olishga imkon beradi. Masalan, axborotlarni qayta ochish uchun mo'ljallangan uskunalar, qalbaki elektron kalitlar, qalbaki magnit kartalar shular jumlasidandir.

Ta'kidlash joizki, bunday vositalar kompyuter tarmog'i yoki shaxsiy kompyuterga bog'lanadi va himoyalangan kompyuter tarmog'i kabi o'zini namoyon qiladigan, himoya vositalari bilan ta'minlangan yashirin axborotlarni aybdor shaxsning qonunga xilof ravishda olishi uchun imkon beruvchi elektron qo'ng'izlar (juchoklar) rolini bajaradi.

Himoyalangan kompyuter tarmog'i axborotdan foydalanishni chegaralovchi dasturli yoki texnik jihatdan maxsus himoya tizimi o'rnatilgan kompyuter tarmog'idir. Bunday tarmoq uchun uning huquqiy himoyasini ta'minlaydigan muayyan rejim o'rnatiladi (masalan, davlat, xizmat, tijorat va bank sirlari, shaxsiy ma'lumotlar, ma'lumotlar bazasi singari). Shu bilan birga, unda yoki tarmoqdagi axborotlardan qonunga xilof ravishda foydalanish, ko'chirma olish ularni yo'q qilib yuborish, modifikatsiya qilish, bloklashtirish, taqdim etish, tarqatish kabi hatti-harakatlarni sodir etishdan tarmoqdagi axborotlarni himoyasini ta'minlash maqsadida kompleks ko'riladi.

Jinoyatning sub'ektiv tomoni to'g'ri qasd shaklida namoyon bo'ladi. Aybdor himoyalangan kompyuter tizimi yoki tarmog'idan noqonuniy (ruxsatsiz) foydalanishni ko'zlab maxsus dastur yoki apparatlarni tayyorlash, o'tkazish, tarqatish harakatlarining ijtimoiy xavfliligini anglaydi, oxir-oqibatda mulkdorga, foydalanuvchiga yoki egalik qiluvchiga zarar yetkazishiga ko'zi yetadi va shuni istab jinoyat sodir etadi. Maxsus vositalarni tayyorlashda o'tkazish maqsadi jinoyat sub'ektiv tomonining zarururiy belgisi hisoblanadi. Shuning uchun ham jinoyat

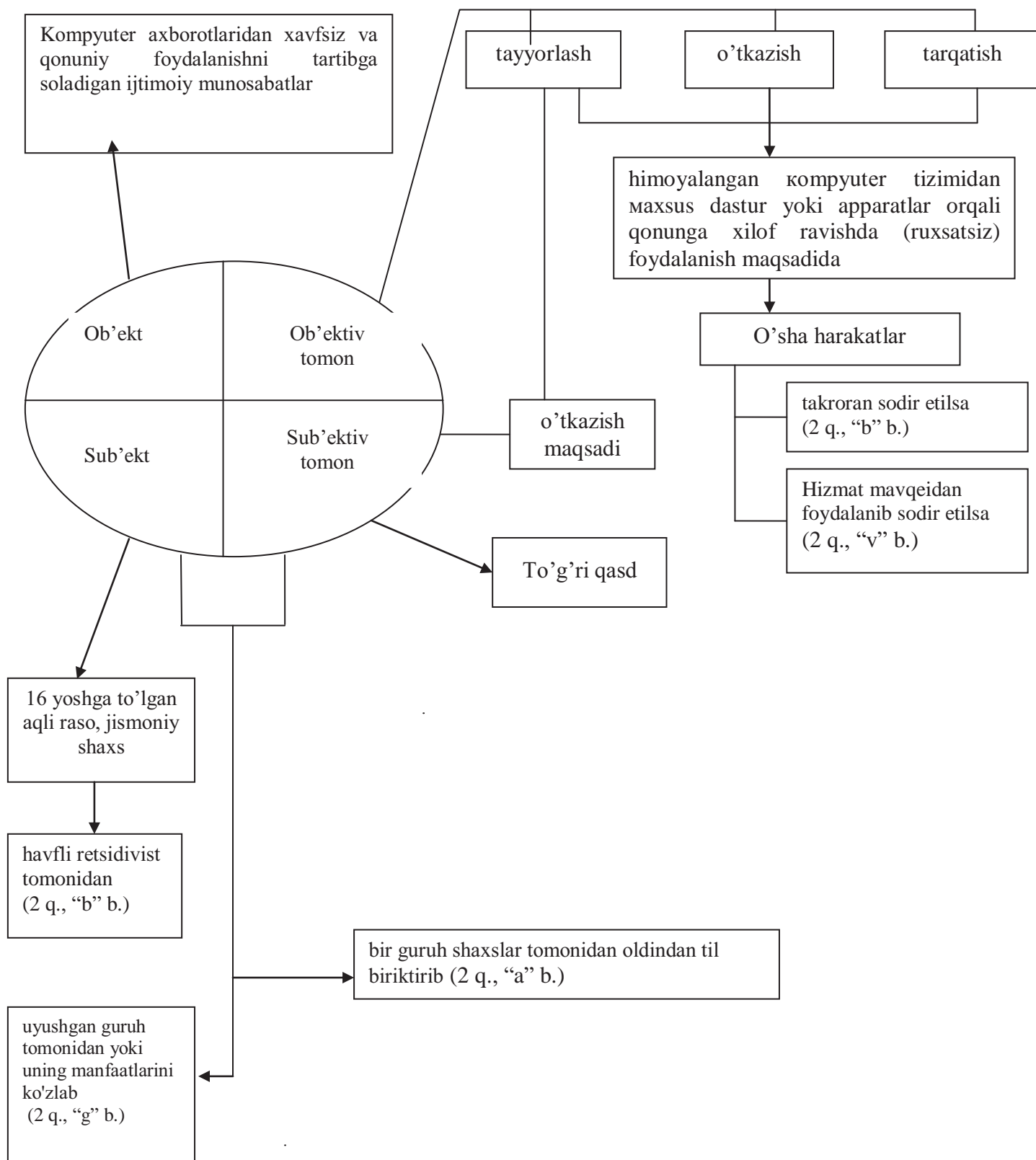
ishini tergov qilish jarayonida mazkur belgi shartli ravishda aniqlanishi va isbotlanishi lozim.

Jinoyatning sub'ekti har qanday 16 yoshga to'lgan, aqli raso jismoniy shaxs bo'lishi mumkin.

JKning 278³-modda 2-qism "v" bandida javobgarlikning og'irlashtiruvchi holati (ya'ni, 1-qismda nazarda tutilgan harakatlarning xizmat mavqeidan foydalangan holda sodir etilishi) to'g'risida so'z boradi.

Xizmat mavqeidan foydalanilgan holda jinoyat" sodir etilsa degan kvalifikatsion belgining mazmuni JK 278²-moddasi, 2-qismida nazarda tutilgan jinoyatning nomidagi belgi bilan bir xil.

JK 278³-moddasida nazarda tutilgan jinoyat tarkibining quyidagicha namoyon qilish mumkin:



5. Kompyuter axborotini modifikatsiyalashtirish (JK 278⁴-moddasi)

Kompyuter axborotini modifikatsiyalashtirishning ijtimoiy xavfliligi shundan iboratki, kompyuter tizimida saqlanayotgan axborotlarning shikastlanishi, o'chirilishi, o'zgartirilishi natijasida axborotdan aniq maqsadsiz foydalanilishni keltirib chiqaradi. Kompyuter axborotidan maqsadsiz foydalanish o'zining mazmuniga ko'ra, kriminallashtirilgan (jinoiy) xususiyatga ega hamda noqonuniy foyda olishga, jamoat xavfsizligi va jamoat tartibini buzish uchun sharoit yaratishga qaratilgan, shuningdek mualliflik huquqi sohasidagi munosabatlarning buzilishiga olib keladi.

Ushbu **jinoiatning bevosita ob'ekti** kompyuter axborotlaridan xavfsiz va qonuniy foydalanishni tartibga soladigan ijtimoiy munosabatlardir. Jinoiatning *predmeti* esa, jinoiy-huquqiy normaning o'zida belgilangan kompyuter axboroti hisoblanadi.

Jinoiatning ob'ektiv tomoni kompyuter tizimida saqlanayotgan axborotni qonunga xilof ravishda modifikatsiyalashtirishda namoyon bo'ladi.

JK 278⁴-moddasining dispozitsiyasiga binoan, modifikatsiya deganda kompyuter tizimi, tarmog'i (doimiy eslab qoladigan uskunalar, qattiq disk kabilar) yoxud kompyuter axborotlarini olib yuradigan vositalar (disketalar, flesh-karta, disk kabilar)da saqlanayotgan (qonuniy foydalanuvchi yoki mulkdorning tasarrufida bo'lgan) axborotni o'zgartirish, unga shikast yetkazish, uni o'chirish, shuningdek bila turib unga noto'g'ri axborotni kiritish singari hatti-harakatlar tushuniladi.

Kompyuter axborotini o'zgartirish kompyuter tizimi, tarmog'i (doimiy eslab qoladigan uskunalar, qattiq disk kabilar) yoki kompyuter axborotlarini tashuvchi vositalar (disketa, flesh-karta, disk kabilar)da saqlanayotgan axborotni qisqartirish yoxud asossiz kengaytirishga qaratilgan harakatlardir.

Kompyuter axborotiga shikast yetkazish deganda axborotning o'zgartirilishi natijasida holati yomonlashishi, foydali xususiyatlarining ma'lum qismi yo'qolishi, qisman yoki umuman foydalanish uchun yaroq bo'lib qolishi tushuniladi. Nobud qilish, ya'ni axborotning umuman qayta tiklanmasligidan farqli

o'laroq, shikast yetkazish faqat axborot sifatining yomonlashganligini anglatadi, biroq qayta ishlov berish hisobiga uni oldingi holatga qaytarish mumkin bo'ladi. Asl holatiga keltirish uchun sarf qilinadi ishlar ma'lum vaqtni talab etadi. Shu bois, undan foydalanishga erishish uzoqqa cho'zilib ketadi.

Kompyuter axborotini o'chirish – axborot tashuvchidan informatsiyani o'chirish. Axborot o'chirilgandan keyin agar uni qayta tiklash imkoniyati bo'lmasa, unda axborot yo'q qilib yuborilgan deb topiladi. Bunday hollarda JK 278²-moddasiga asosan javobgarlik belgilanadi.

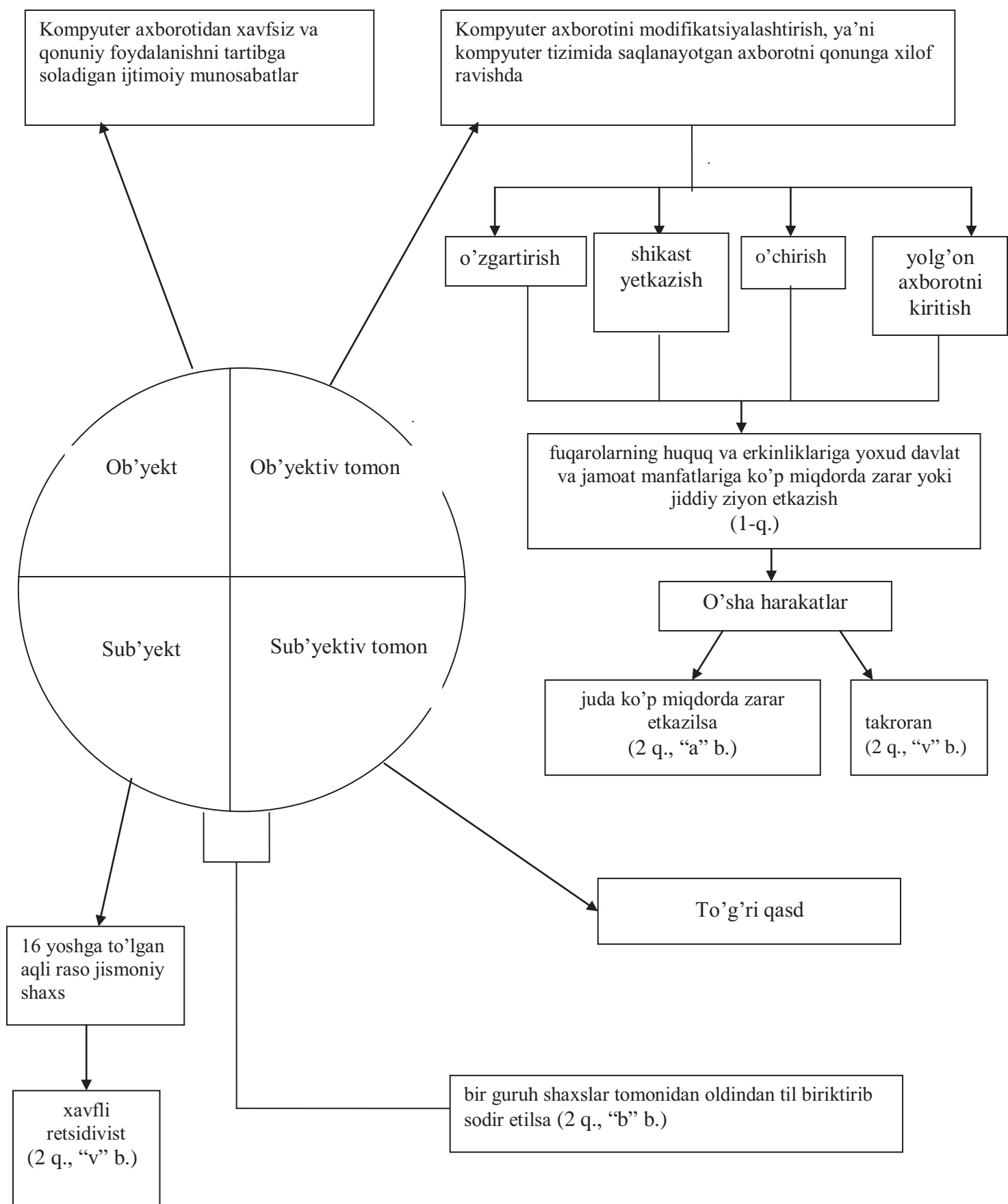
Yolg'on axborotni kiritish – zamonaviy informatsion texnologiyalardan foydalanish orqali hujjatlarning mazmuniga semantik o'zgartirishlar (qo'shish, o'zgartirish, ma'lumotlarni yo'q qilib yuborish kabi) shaklidagi kompyuter axborotlarini qalbakillashtirish.

JK 278²-moddasining 1-qismi bo'yicha jinoiy javobgarlikka tortishning zaruriy sharti sifatida fuqarolarning huquq va erkinliklariga, jamoat yoki davlat manfaatlariga ko'p miqdorda zarar yoki jiddiy ziyon yetkazilishi hisoblanadi. Bunda qilmish va ko'p miqdorda zarar yoki jiddiy ziyon yetkazish ko'rinishidagi oqibatlar o'rtasida sababiy bog'lanish bo'linishi lozim. Xulosa qilib aytish mumkinki, kompyuter axborotini modifikatsiyalashtirish moddiy tarkibli jinoyat turiga kiradi.

Agar aybdor o'z qilmishining ijtimoiy xavfliligini anglagan va uning sodir etilishi natijasida ijtimoiy xavfli oqibatlarning kelib chiqishiga ko'zi etgan va buni istagan bo'lsa, mazkur jinoyat tarkibining **sub'ektiv tomoni** to'g'ri qasd shaklida namoyon bo'ladi.

Jinoyatning sub'ekti, 16 yoshga etgan aqli raso jismoniy shaxs hisoblanadi.

JK 278⁴-moddasida nazarda tutilgan jinoyat tarkibining chizmasini quyidagicha namoyon qilish mumkin.



6. Kompyuter sabotaji (JK 278⁵-moddasi)

Kompyuter sabotajini ijtimoiy xavfliligi kompyuter tizimi orqali axborotlardan foydalanish va axborot almashish sohasidagi munosabatlarni tartibga soluvchi amaldagi qonunchilik talablarini bajarilmasliklardan iboratdir. Shu bilan birga, aybdor shaxs ma'lum vositalardan foydalanib, kompyuter tizimi ishini to'liq hajmda izdan chiqarishi mumkin bo'lgan axborotlarni yoki ularning ommaviy o'chirilishi yoxud operatsion dasturlarga shikast yetkazilishini vujudga keltiradi. Buzuvchi vositalar qimmatbaho (ahamiyatga ega bo'lgan) dasturlarni yo'q qilishi, tizimni uzoq muddatga yopishi, buning natijasida jamoat tartibi va xavfsizligini buzish uchun sharoit yaratish mumkin. Masalan, yo'l harakati xavfsizligini kuzatuvchi elektron tizimda axborotlar o'chirilishi sodir bo'lsa, yo'lda boshqarib bo'lmay xavfli vaziyat yuzaga keladi va natijada o'lim yoki yo'l-transport hodisasi holatlari kuzatiladi.

Jinoyatning **bevosita ob'ektini** kompyuter axborotlaridan qonuniy va xavfsiz foydalanish sohasidagi ijtimoiy munosabatlar tashkil qiladi. Mazkur soha yetarlicha keng va o'zida inson hayot kechirishining barcha jabhalarini, jumladan ishlab chiqarish, iste'mol, tarqatish va ta'minlashda ma'lum maqsadga erishish uchun bilvosita kompyuter uskunalaridan foydalanishning qamrab oladi. Kompyuter axborotlaridan qonuniy va xavfsiz foydalanishni sohaviy tavsifi biron-bir soha faoliyatidagi maqsad va vazifalar bilan chegaralanadi.

Jinoyatning **ob'ektiv tomoni** kompyuter sabotajida tavsiflanadi.

Maxsus adabiyotlarda "sabotaj" tushunchasi ochiqdan-ochiq bosh tortish yoki qasddan lozim darajada bajarmaslik orqali ongli ravishda ishni buzish yoxud muayyan jarayonni amalga oshirishga yashirin ravishda qarshilik ko'rsatish¹ deb ta'riflanadi.

Yuqorida berilgan ta'rifdan kelib chiqqan holda, "kompyuter sabotaji" tushunchasiga aybdorning mavjud tizimining sifatsiz ishlashi yoxud butunlay to'xtatishiga olib keluvchi va parametrlarni o'zgartirish yoki yo'q qilish yo'li bilan kompyuter elektron tizimi ishini buzishga yo'naltirilgan harakatlarni kiritish lozim.

¹ Словарь иностранных слов. 12-е изд. – М., 1985. – С. 440.

Ushbu jinoyatni sodir etishda aybdorning ijtimoiy xavfli qilmishi asosan navbatda kompyuter yoki telekommunikatsiya tizimlarining odatiy boshqarilishiga to'sqinlik qilishga yo'naltiriladi. Shundan kelib chiqib, kompyuter sabotaji umumiy tushunchasi o'z ichiga kompyuter tizimiga barcha ko'rinishdagi aralashishlarni qamrab oladi. Masalan, tizim ishini buzish uchun noto'g'ri ma'lumotlarni kiritish, kompyuterga barcha ko'rinishdagi jismoniy shikast yetkazish, kompyuter kuchlanishi yoki uskunasi biron-bir qismining o'chirilishi va boshqalar shular jumlasidandir.

JK 278⁵-moddasida ko'rsatilgan kompyuter sabotaji jinoyati quyidagicha faqat ikkita muqobil qilmishni o'z ichiga qamrab oladi: 1) o'zganing yoki xizmatda foydalaniladigan kompyuter uskunasini ishdan chiqarish; 2) kompyuter tizimini buzish.

O'zganing yoki xizmatda foydalaniladigan kompyuter uskunalarini ishdan chiqarish – kompyuter uskunasi vazifalarning buzilishi, axborotlarning noto'g'ri kiritilishi yoki yo'q qilinishi, kompyuter uskuna yoki uning qandaydir qismini o'chirib qo'yish, unga shikast (jismoniy yoki mexanik) yetkazish singari hatti-harakatlar.

Kompyuter uskunolari deganda, foydalanuvchi tomonidan dastur yoki ramzli va obrazli axborot ustidan (axborotni qayta ishlash va uskunalarni boshqarish bo'yicha harakatlarning ketma-ketligi) operatsiyalarni o'tkazish, shuningdek unga kirish-chiqish, yo'q qilish, nusxa ko'chirish, modifikatsiyalashtirish, kompyuter tarmog'iga axborotni uzatish va boshqa jarayonlarni amalga oshiruvchi elektron uskunalar majmuasi tushuniladi.

Kompyuter uskunolari bajaradigan vazifalariga ko'ra ikki asosiy guruhga bo'linadi: 1) apparat vositalari (Hard Ware); 2) dasturiy vositalar (Soft Ware).

Apparat vositalari deganda, ma'lumotlarni qayta ishlash uchun foydalaniladigan texnik vositalar: axborotlarni qayta ishlash maqsadida foydalaniladigan elektr, mexanik va elektron uskunalar tushuniladi. Ularga shaxsiy kompyuter, periferiy uskunolari va mashina axborotlarini tashuvchilar kiradi.

Dasturiy vositalar deganda, ma'lum bir natija olish maqsadida kompyuter va uning qurilmalari vazifalarini bajarish uchun mo'ljallangan komandalar hamda ma'lumotlar majmui taqdimotining ob'ektiv shakli, shuningdek, tayyorlangan va moddiy tashuvchilarda qayd qilingan materiallar, ularni qayta ishlash paytida olingan va ular tomonidan hosil qilingan audiovizual ko'rinishlar tushuniladi. Ular quyidagilardan iborat: a) tizimli, qo'shimchali va jihozli dasturlarni o'z ichiga oluvchi dasturiy ta'minot; b) foydalanuvchi (ishlatuvchi)ning mashina axboroti.

Kompyuter tizimini buzish kompyuter tizimi vazifalarining buzilishi unda saqlanayotgan axborotlarning noto'g'ri yoritilishi, yo'q qilinishi yoki to'sib qo'yilishiga olib keluvchi hatti-harakatlar, shuningdek kompyuter tizimini o'chirib qo'yish, unga shikast yetkazish yoki qandaydir qismini o'chirishdir. Yuqorida kompyuter tizimi deganda, hech bo'lmaganda bitta kompyuterning tizim elementi bo'lishi yoxud bir nechta kompyuterlarning tizimni tashkil qilishi nazarda tutilgan.

Jinoyat moddiy tarkiblidir. Kompyuter uskunasi ishdan chiqarilgan yoki kompyuter tizimi buzilgan paytdan jinoyat tugallangan hisoblanadi.

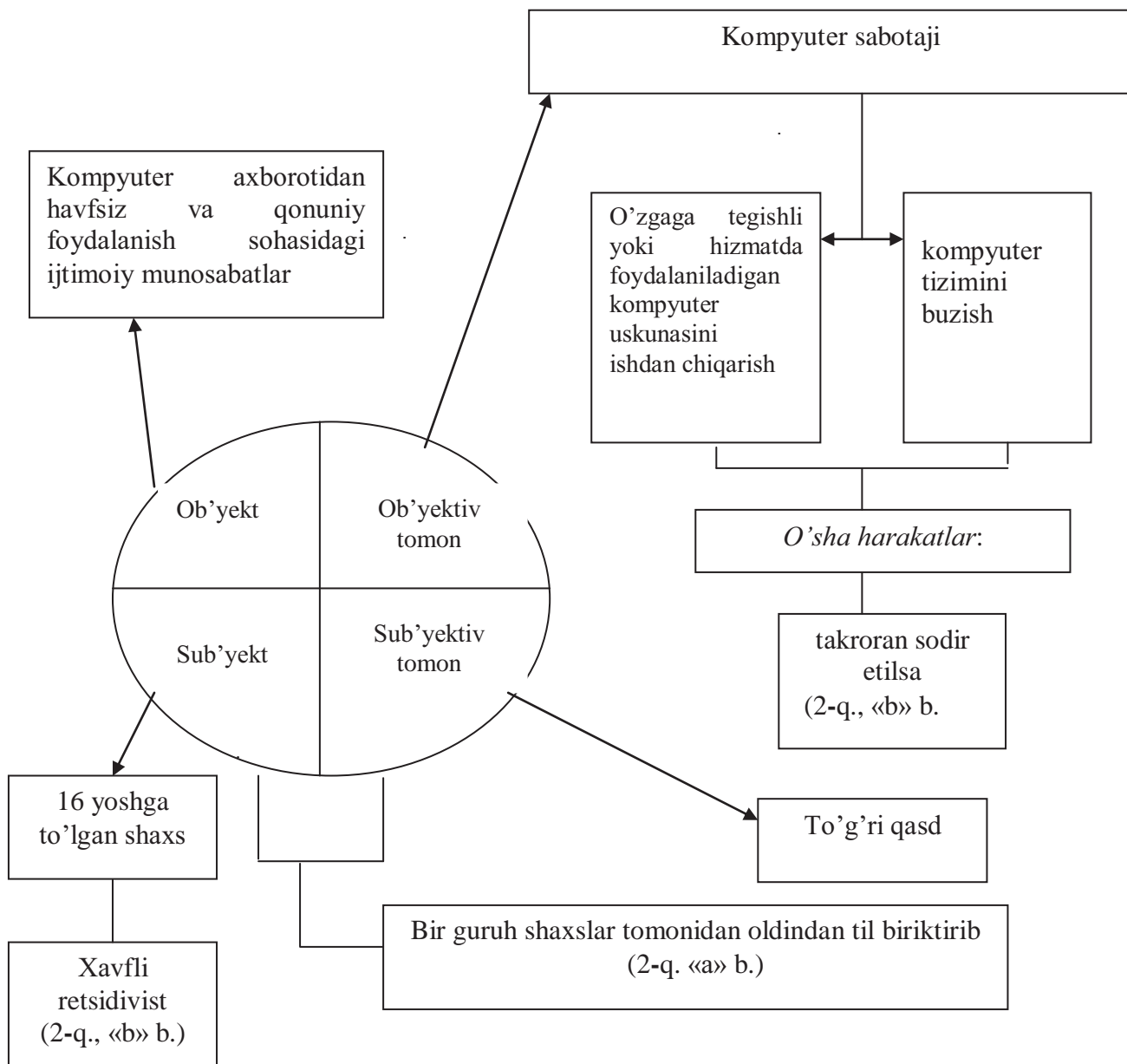
Kompyuter sabotajining **sub'ektiv tomoni** to'g'ri qasdda tavsiflanadi. Aybdor shaxs kompyuter uskunasining ishdan chiqishi yoki kompyuter tizimi buzilishining ijtimoiy xavfliligini biladi va harakatlari oqibatida kompyuter yoki telekommunikatsiya tizimining odatiy vazifalarini bajarishga to'sqinlik qilishini oldindan ko'radi va kompyuter axborotidan foydalanuvchiga, uni egasiga ziyon yetkazishni hohlaydi.

Motivlar turli xil bo'lishi mumkin – raqobatchidan qutilish istagi, sug'urta olish, firmadan yoki ish beruvchidan o'ch olish, o'zining kompyuter ustidan hukmronligini isbotlash va hokazo. Ular kvalifikatsiyada ahamiyat kasb etmaydi.

Jinoyat **sub'ekti** 16 yoshga to'lgan aqli raso, jismoniy shaxs bo'lishi mumkin.

JKning 278⁵-moddasida nazarda tutilgan jinoyat tarkibining chizmasini

quyidagi ko'rinishda namoyon qilish mumkin:



7. Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish (JK 278⁶-moddasi)

Ushbu jinoyatning ijtimoiy xavfliligi kompyuter tizimi yoxud tarmog'iga virus dasturlari tushishining aniq xavfi mavjudligida namoyon bo'ladi. Viruslar nafaqat tizimning normal ishlashini buzadi, balki keyinchalik tizimning o'zi orqali kompyuter ishini buzish va to'xtatishni keltirib chiqaradigan shaxsiy virus dasturlarini multiplitsirlashni boshlaydi, unda bajariladigan ijtimoiy foydali vazifalarning uzilishini keltirib chiqaradi. Bu esa kompyuter tizimida monitoringga uchraydigan jarayonlarning xavfsizlik shartini yo'q qiladi. Ayni vaqtda mavjud bo'lgan MS-DOS kompyuter operatsion tizimi virus dasturlarini o'tkazuvchidir. Shaxsiy kompyuterlarning keng tarqalganligi natijasida viruslar ularning ofatiga aylangan. Hozir dunyoda 10 mingdan ortiq faqat faol ta'sir qiluvchi viruslar mavjud bo'lib ularning soni muntazam o'sib bormoqda. Bu esa yangidan-yangi antivirus dasturlar («revizorlar», «detektorlar», «vaksinalar», «faglar»)ni ishlab chiqishni taqozo etmoqda.

Jinoyatning **bevosita ob'ekti** kompyuter tizimidan xavfsiz foydalanish sohasidagi ijtimoiy munosabatlar, kompyuter tizimining dasturiy ta'minoti va axborotli tuzilishi hisoblanadi. Kompyuter axboroti predmet sifatida namoyon bo'ladi.

Jinoyatning **ob'ektiv tomonini** quyidagilar tashkil qiladi: a) zarar keltiruvchi kompyuter dasturlarini yaratish va mavjud dasturlarga ularni zarar keltiruvchi dasturlarga aylantiradigan o'zgartishlar kiritish; b) maxsus virus dasturlarini ishlab chiqish; v) kompyuter tizimlariga zarar keltiruvchi dasturlarni tashuvchi vositalardan foydalanish va tarqatish.

Zarar keltiruvchi dasturlarni yaratish yoki mavjud dasturlarga o'zgartishlar kiritish, shunday qilmishlar kompyuter tizimida saqlanayotgan yoki uzatilayotgan axborotlarni ruxsatsiz yo'q qilib yuborish, to'sib qo'yish, modifikatsiyalashtirish, ulardan nusxa ko'chirish yoki ularni qo'lga kiritish real xavfini keltirgan taqdirda jinoyat sifatida baholanadi. Boshqa holatlarda shaxs tomonidan zarar keltiruvchi va virus dasturlarining yaratilishi, foydalanilishi yoki tarqatilishi jinoyat sifatida

ko‘rilmaydi. Masalan, shaxs monitor ekranida shtrix xosil qiladigan va shu paytning o‘zida yo‘qoladigan uncha zararsiz dastur-virus yaratasa, uning qilmishi jinoiy-qilmish deb topilmaydi. Bunday holatlarda zarar keltiruvchi dastur foydalanuvchi yoki axborot egasi uchun xavf tug‘dirmaydi va JK 278⁶-moddasi 1-qismida ko‘rsatilgan oqibatlarga olib kelmaydi. Shu bois shaxsning qilmishi JK 36-moddasiga asosan kam ahamiyatli qilmish deb topilib jinoiy javobgarlikdan va jazodan ozod qilinadi.

Dastur deganda, ma’lum algoritmni realizatsiya qilish maqsadida ma’lumotlarni qayta ishlash tizimining aniq komponentlarini boshqarish uchun mo‘ljallangan ma’lumotlar tushuniladi.

Zarar keltiruvchi dastur – ishga tushgach, foydalanuvchi yoki axborot egasiga axborotlarni yo‘q qilib yuborish, to‘siq qo‘yish, modifikatsiyalashtirish, nusxa ko‘chirish yoki ularni qo‘lga kiritish tarzida ziyon yetkazish imkoniga ega bo‘lgan maxsus yozilgan (yaratilgan) dastur.

Zarar keltiruvchi dasturlarni *yaratish* deganda, axborotlarni yo‘q qilish, to‘siq qo‘yish, modifikatsiyalashtirish, nusxa ko‘chirish yoki ularni qo‘lga kiritish maqsadida tizimni aniq komponentlarni boshqarish uchun mo‘ljallangan chiquvchi ma’lumotlarni tayyorlash, axborotlar ustida ishlash kabi kompleks operatsiyalar tushuniladi.

Mavjud dasturlarga *o‘zgartishlar kiritish* – JK 278⁶-moddasi dispozitsiyasida ko‘rsatilgan zararli oqibatlarni keltirib chiqarish darajasigacha bo‘lgan dasturlarni modifikatsiyalashtirish jarayoni (alohida fragmentlarni o‘chirish yoki qo‘shish, yangilash yo‘li bilan ma’lumotlarni yig‘ish yoki dasturlarni qayta ishlash)dir.

Zarar keltiruvchi dasturlarning nisbatan xavfliroq ko‘rinishlaridan biri virus (kompyuter virusi) dasturlaridir. Virus o‘zida maxsus ishlab chiqilgan dasturni namoyon qilib, boshqa dasturlarga o‘z-o‘zicha qo‘shiladi (shuningdek, ularni «zaharlaydi») va so‘nggi yoqilganda turli noxush harakatlarni, jumladan fayl va kataloglarni buzish, qayd qilish natijalarini noto‘g‘ri yoritish, xotirani o‘chirish yoki so‘rib olishi, EHM ishida noqulaylik tug‘diruvchi faoliyatlarni amalga oshiradi. Bunday dasturlar tillar assemblerida tarkib topadi va monitor ekraniga

hech qanday xabar uzatmaydi. Viruslar diskdan diskka nusxa ko‘chirish yoxud tarmoq orqali tarqatiladi.

Hozirgi vaqtda kompyuter viruslarining xilma-xil ko‘rinishlari mavjud. Misol tariqasida «Troya oti» virusini keltirish mumkin. U zararsiz kompyuter dasturi ostida niqoblanadi va ishga tushirilganda buzish ishlarini sodir etadi. «Cherv» dasturiy ta’minotdagi «tuynuk» orqali kiber bo‘shlig‘iga tushadi, o‘zidan kompyuter xotirasiga nusxa ko‘chiradi va unga yuklatilgan vazifani bajaradi.

«Troya oti»ning yana bir ko‘rinishi «Mantiqiy bomba» nomli virusdir. Uskuna ma’lum muddat o‘tgandan so‘ng o‘z-o‘zidan yoki kompyuterdan foydalanuvchi ma’lum harakatni sodir etgan vaqtdan ishga tushadi.

«Pochta viruslari» elektron pochta orqali yoyiladi, o‘z-o‘zini avtomatik tarzda ishlab chiqaradi va kompyuter xotirasiga kiritilgan manzillarga uzatiladi.

Insonning eng kuchli va hayot uchun xavfli ixtirolaridan biri – bu o‘lim virusi № 666. U o‘z-o‘zidan ishga tushadi va insonga quyidagicha ta’sir qiladi: №666 kompyuter ekranida maxsus tanlangan rangli kombinatsiya namoyon bo‘ladi. Monitor oldida o‘tirgan inson gipnoz bosimi ostida qoladi va yurak-qon tomir tizimi faoliyati to‘satdan buzilib, ahvol miya qon tomirlarining to‘lib qolishigacha yomonlashadi va natijada o‘lim holati yuzaga keladi.

Zarar keltiruvchi dasturlar (viruslar) yoki ularning mashina tashuvchilarini *ishlatish* deganda, ularni yuzaga chiqarish, ishlab chiqarish, tarqatish yoxud xo‘jalik aylanmasiga, jumladan modifikatsiyalashtirilgan shaklga kiritish (O‘zbekiston Respublikasining «Elektron hisoblash mashinalari uchun dasturlar va ma’lumotlar bazalarini huquqiy himoyalash to‘g‘risida»gi qonunining 1-moddasi) harakatlari tushuniladi. Masalan, zarar keltiruvchi dasturlarni ishlatish ularni kompyuter xotirasiga kiritish (o‘rnatish)da namoyon bo‘ladi.

Zarar keltiruvchi dasturlarni *tarqatish*, biron bir material shaklida ishlab chiqarilgan dasturlarni EHM yoki ma’lumotlar bazasiga kiritish (jumladan, tarmoq orqali yoki boshqa usullarda) sotish, ijaraga berish, qarzga berish, qarzi evaziga berish va mazkur maqsadlarda import qilishlarni o‘z ichiga qamrab oladi (yuqorida ko‘rsatilgan qonunning 1-moddasi). Masalan, bunday dasturlarni aybdor o‘zganing

kompyuterida ishlash chog'ida virus yozilgan disketadan foydalanish modem yoki kompyuter tarmog'i orqali tarqatish kabi holatlar.

EHM uchun zarar keltiruvchi va virus dasturlarini yaratish, ishlatish va tarqatish har doim ushbu jinoyatni sodir etgan shaxsdan faol harakatlarni sodir etishni taqozo qiladi. Mazkur jinoyatni harakatsizlik orqali sodir etish mumkin emas.

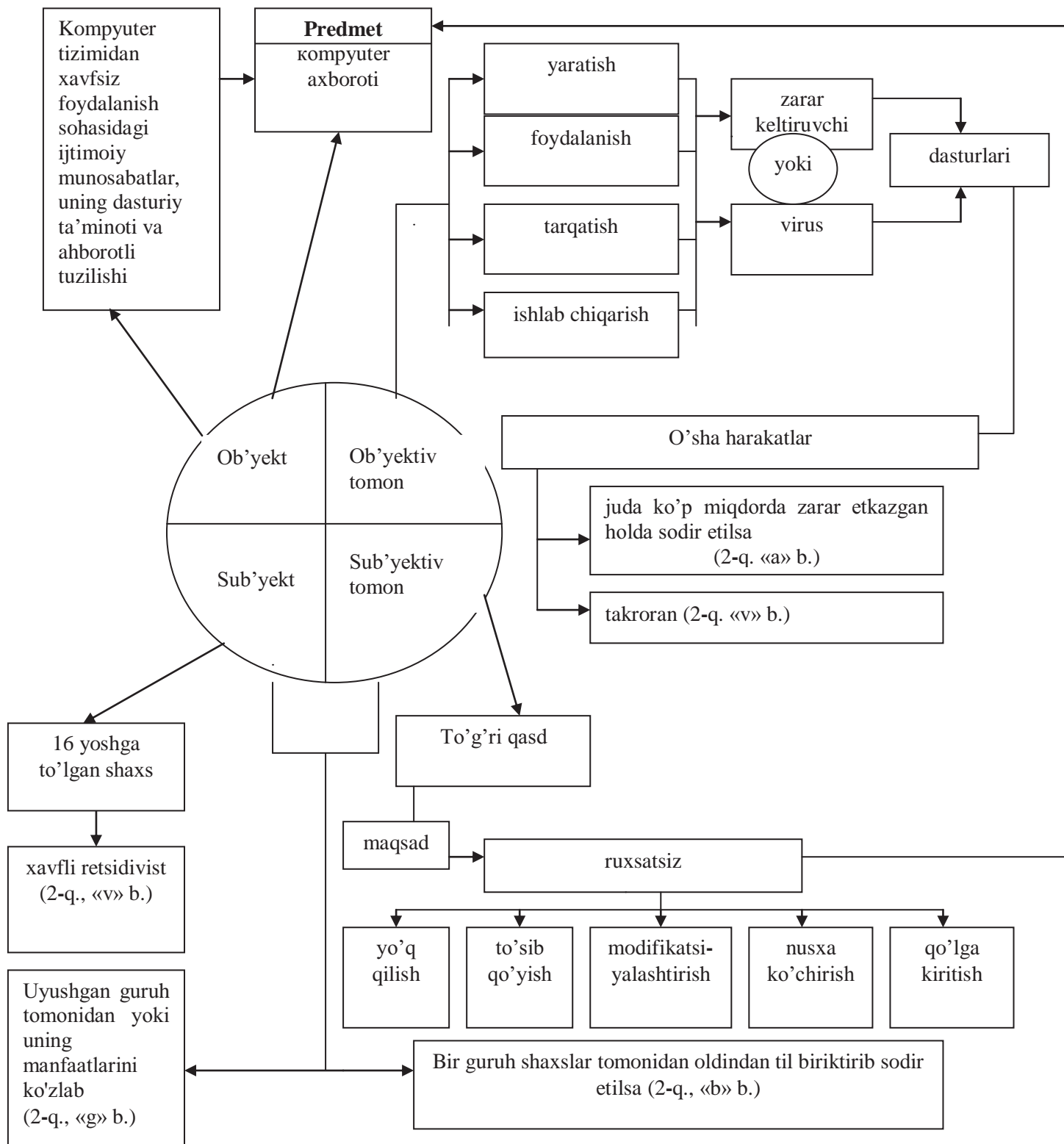
JK 278⁶-moddasida nazarda tutilgan jinoyat tarkibi formaldir. Jinoyatni tugallangan deb topish uchun axborotlarni yo'q qilish, to'sib qo'yish, modifikatsiyalashtirish, nusxa ko'chirish yoki qo'lga kiritish kabi salbiy oqibatlarining kelib chiqishi talab qilinmaydi. JK 278⁶-moddasi dispozitsiyasida qayd etilgan qilmishlardan hech bo'lmaganda bittasining sodir etilishi faktini aniqlashning o'zi kifoya.

Agar EHM uchun zarar keltiruvchi dastur viruslarni yaratish, ishlab chiqish, foydalanish va tarqatish kompyuter tuzilmasining ishdan chiqishiga olib kelsa (masalan, EHM yoki asosiy qurilmalar butunligining tiklab bo'lmas darajada buzilishi), mulkni qasddan nobud qilish yoki unga shikast yetkazish (JK 173-moddasi) va zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish (JK 278⁶-moddasi) uchun javobgarlikni nazarda tutuvchi moddalar bilan jinoyatlar majmui tariqasida kvalifikatsiya qilinadi.

Tahlil qilinayotgan jinoyatning **sub'ektiv tomoni** to'g'ri qasddan sodir etiladi. Aybdor shaxs o'zi tomonidan axborotlarni yo'q qilish, to'sib qo'yish, modifikatsiyalashtirish, nusxa ko'chirish yoki qo'lga kiritishga qodir dastur yaratilayotgani, ishlatilayotgani yoxud tarqatilayotganini angelaydi va ushbu qilmishni sodir etishni hohlaydi. Jinoyat maqsadi – ruxsatsiz axborotlarni yo'q qilish, to'sib qo'yish, modifikatsiyalashtirish, nusxa ko'chirish yoki qo'lga kiritish.

Mazkur jinoyatning **sub'ekti** – jinoyat sodir etish vaqtida 16 yoshga to'lgan aqli raso jismoniy shaxs hisoblanadi.

JK 278⁶-moddasida nazarda tutilgan jinoyat tarkibining chizmasini quyidagi ko'rinishda namoyon qilish mumkin.



8. Kompyuter texnologiyalari sohasidagi jinoyatlarning

oldini olish

Ushbu turdagi jinoyatlarning oldini olish masalalariga to'xtalganda, avvalam bor oldini olish chora-tadbirlarini ikkita asosiy (huquqiy va tashkiliy-texnikaviy choralar) guruhga ajratish maqsadga muvofiqdir.

Axborot texnologiyalari sohasidagi jinoyatlarning oldini olishning *huquqiy choralari* deganda, kompyuter axborotini qo'llash, saqlash, jo'natish, nusxa ko'chirish sohasidagi xavfsizlikni ta'minlashga qaratilgan normativ material (hujjat)lar tushuniladi. Ushbu material O'zbekiston Respublikasining axborotlashtirish va ma'lumotlarni uzatish sohasidagi g'ayriqonuniy qilmishlar uchun javobgarlikni belgilovchi amaldagi jinoyat qonunlari normalari bilan ham, axborot munosabatlari sohasidagi boshqa normativ hujjatlar bilan ham kafolatlangan¹. Bundan tashqari, mamlakatimizda axborot texnologiyalari sohasidagi jinoyatlarning oldini olishga bevosita qaratilgan bir qator normativ hujjatlar qabul qilindi. Ular orasida O'zbekiston Respublikasi Prezidentining «Milliy axborot-kommunikatsiya tizimlarining kompyuter xavfsizligini ta'minlash bo'yicha qo'shimcha chora-tadbirlar to'g'risida»gi 169-sonli 2005 yil 5 sentyabr qarori alohida ahamiyatga ega. Unda ta'kidlanishicha, O'zbekiston Respublikasining «Axborotlashtirish to'g'risida»gi qonuniga muvofiq, yuridik va jismoniy shaxslarning axborot-kommunikatsiya texnologiyalari va Internet tarmog'idan foydalanishining xavfsizligini ta'minlash bo'yicha milliy tizimni yanada takomillashtirish, kompyuter xavfsizligiga tahdidlarni o'z vaqtida aniqlash, zararsizlantirish va ularning oldini olish masalalarida ularga ko'maklashish maqsadida... Keyinchalik, ushbu qaror asosida O'zbekistonda «O'zinfokom»

¹ Birinchi qismida «Elektron hisoblash mashinalari uchun dasturlar va ma'lumotlar bazalarini huquqiy muhofaza qilish to'g'risida»gi O'zbekiston Respublikasining 1994 yil 6 may qonuni (O'zbekiston Respublikasining 2002 yil 5 aprel va 8 avgustdagi keyingi qo'shimcha va o'zgartishlari bilan) haqida so'z yuritildi. «Axborot erkinligining prinsiplari va kafolatlari to'g'risida»gi O'zbekiston Respublikasining 2002 yil 12 dekabr hamda «Axborotlashtirish to'g'risida»gi 2003 yil 11 dekabr qonunlari ham kompyuter texnologiyalari sohasidagi jinoyatlarning oldini olish uchun huquqiy asos hisoblanadi.

kompyuter va axborot texnologiyalarini rivojlantirish va joriy etish markazi qoshida Kompyuter intsidentlariga chora ko‘rish xizmati tashkil etildi.

Mazkur xizmatning asosiy vazifalari quyidagi yo‘nalishlarda amalga oshiriladi: milliy axborot tarmog‘i sub’ektlarining kompyuter xavfsizligi bo‘linmalari harakatlarini muvofiqlashtirish, kompyuter xavfsizligiga tahdid va intsidentlar bo‘yicha ma’lumotlar bazasini yuritish, axborot xavfsizligini ta’minlash yuzasidan tavsiyalar ishlab chiqish, konsultativ xizmat ko‘rsatish va texnik jihatdan qo‘llab-quvvatlash (eng muhimi – intsidentlar chog‘ida zudlik bilan yordam ko‘rsatish), normativ-huquqiy bazani takomillashtirish yuzasidan takliflar ishlab chiqish. Bunday xizmatning mamlakatda tashkil etilishi (masalan, elektron-raqamli imzo uchun raqamli sertifikatlar yasash, Jinoyat va Jinoyat-protsessual kodekslariga kompyuter jinoyatlariga doir tegishli o‘zgartishlar kiritish kabi boshqa tadbirlar) davlatning axborot texnologiyalari va axborot xavfsizligi sohasida muayyan darajada yetukligidan dalolat beradi.

Darhaqiqat, axborot texnologiyalari kundalik hayotimizga borgan sari chuqurroq kirib bormoqda. Yuridik va jismoniy shaxslar axborot almashinuvi jarayonining faol ishtirokchilariga aylanmoqdalar. Muammolar yuzaga kelganda, ayniqsa malakali mutaxassis bo‘lmagan foydalanuvchining o‘z ona tilida tegishli xizmatga murojaat etish imkoniyati intsident vaziyatni muvaffaqiyatli hal etish uchun katta ahamiyatga ega bo‘lishi mumkin. Xalqaro telefon so‘zlashuvlari uchun xarajatlarning yo‘qligi, yagona vaqt mintaqasi (binobarin, yagona ish vaqtlari), zarur bo‘lganida bir guruh mutaxassislarning kerakli joyga yetib borish imkoniyati, yagona normativ-huquqiy makon va boshqa omillar inobatga olinsa, intsidentlarga chora ko‘rish milliy xizmatining boshqa muqobil xizmatlardan foydalanishga nisbatan oldida shubhasiz ustunlikka ega ekanligi ayon bo‘ladi.

Alohida ta’kidlash joizki, mazkur xizmat aynan shu davlatga xos bo‘lgan axborot texnologiyalari ishining xususiyati va alohida yo‘nalishlarini baholashga imkon beradi. Masalan, O‘zbekistonda smart-kartalar asosidagi elektron to‘lov tizimlari keng tarqalgan. Tizimlarda foydalaniladigan xavfsizlik modeli, oddiy kredit kartalardan farqli o‘laroq, jinoyatchiga karta raqami (yoki unda ifodalangan

boshqa rekvizitlar)ni bilishi hech qanday imkoniyat bermaydi. Dasturiy ta'minot to'g'ri amalga oshirilganida esa foydalanuvchining smart-kartasi, magnit tasmas kartadan farqli ravishda, masalan, sotuvchining smart-kartasi bilan ma'lumotlar ayirboshlash uchun himoyalangan kanal yaratishi mumkin. Ushbu xususiyatlar to'lov tizimining ishini tahlil qilishda bir qator hujumlarni ko'rib chiqmaslikka imkon beradi. Albatta, yuqoridagi fikrlar ushbu xizmatning faqat smart-kartalar bilan bog'liq axborot hujumlariga e'tibor qaratishi kerakligini bildirmaydi, chunki boshqa turdagi kartalardan g'arazli maqsadlarda foydalanish ham mumkin. Buzg'unchik vositalari borgan sari takomillashib bormoqda. Shunga qaramay, tizimlar ishining xususiyatlarini yaxshi bilish zarur.

Security.uz sayti o'quvchilarining savollariga berilgan javoblarda axborot xavfsizligini buzishlarga qarshi kurashda kompyuter mexanizmlaridan foydalanish davlatning maxsus xizmatlari olib boradigan operativ qidiruv tadbirlarida foydalaniladigan usullarni qo'llashning taqiqlanishini bildirmaydi. Bu intsidentlarga chora ko'rish xizmatining tegishli aloqalarni yo'lga qo'yishi va ichki ishlar organlari, shuningdek boshqa tuzilmalar (masalan, Davlat bojxona qo'mitasi bo'linmalari) bilan hamkorlik mexanizmini ishlab chiqishi kerakligini bildiradi. Shuningdek, ushbu xizmat intsidentlar haqida buyurtmalar yoki xabarlarini qabul qilish tartibini ham nazarda tutishi zarur. Aks holda, xizmat kiruvchi ma'lumotlarning tagida qolib ketishi va DoS (Denial of Service – xizmat ko'rsatishni rad etish) yoki DDoS (Distributed Denial of Service – xizmat ko'rsatishni taqsimlab rad etish) hujumlariga o'xshab qolishi mumkin. Bunday hujumlarning kompyuter analogiyalariga tayanib, aytish mumkinligi, DoS hujumidan qutulish retsepti – axborot manbaini bloklash yoki uni pisand qilmaslik, DDoS hujumi uchun esa yagona amaliy variant – kirish so'rovlarini filtrlash va ishlab chiqarish resurslarini oshirish. Xizmat ishiga nisbatan olganda, bu (yuqorida so'z yuritilgan) axborotni qabul qilish tartibini ishlab chiqish, qo'llash va ishlab chiqarish hajmi oshib ketgan hollarda tashqaridan mutaxassislarni zudlik bilan jalb etish imkoniyatini nazarda tutadi.

Xizmat axborot xavfsizligi bo'yicha keng miqyosda maqsadli xizmatlar ko'rsata boshlagach, unga axborot xatarlarini boshqarish va avariya rejalarini tuzish bo'yicha mutaxassislar kerak bo'ladi. Ushbu yo'nalishlarning o'zi kompyuter hujumlarining texnik jihatlariga nisbatan keyingi qadam hisoblanadi hamda axborot texnologiyalarini tashkil qilish va boshqarish printsiplarini tushunishni talab etadi. Bu esa xizmatdagi mutaxassislarning muntazam o'rganishlari va malaka oshirish bilan shug'ullanishlari kerakligini bildiradi. Mutaxassislarning tajribasiga tayangan holda, xizmat mutaxassislariga bir qator materiallarni tavsiya etish masadga muvofiqdir. Jumladan Stiven Nortkat va Aleksey Lukatskiylarning tarmoq hujumlari bo'yicha kitoblarini o'qish foydali. Ayniqsa, bizga mutlaqo boshqa maqsadlar uchun mo'ljallanganligi ma'lum bo'lgan "Telnet" protokolining paketlariga yashirilgan maxfiy ma'lumotlarni uzatishni niqoblash yo'llari tavsiflangan misollar juda qiziqarlidir. O'zbekistondagi bir qancha katta tashkilotlar (masalan, Milliy bank) bir necha yildan buyon hujumlarni aniqlashning avtomatlashgan vositalaridan foydalanmoqdalar va, shubhasiz, bu sohada qimmatli tajriba to'pladilar. Ko'pgina tashkilotlar 2000 yil muammosini hal qilishga tayyorgarlik ko'rayotganlarida chora ko'rish xizmatining ba'zi analoglarini yaratganlar. Aftidan, bunday ma'lumotlarni berish uchun tashkilotlar yoki xususiy shaxslarga mo'ljallangan tegishli seminarlar uyushtirib, to'plangan bilimlardan foydalangan ma'qul. Ushbu xizmat sub'ektlarning hamkorlikdan manfaatdorlik mexanizmini ishlab chiqishi kerak. Bunday mexanizmlar ro'yxatiga, masalan, jiddiy intsident haqida xabar olinganidan so'ng korxonaga uchun himoyaning samaradorligini bepul tahlil qilish yoxud hujum qurbonlari bo'lgan jismoniy shaxslar uchun seminarlar tashkil qilish kabilarni kiritish mumkin.

Xizmatning dastlabki qadamlaridan birini xizmat faoliyati uchun huquqiy makon yaratuvchi normativ hujjatlarning loyihalarini ishlab chiqish (xususan, kompyuter xavfsizligi turli jihatlarining yuridik muhim ta'riflarini ishlab chiqish) tashkil etishi kerak.

Masalan yuqori darajadagi hujjatlarda foydalansa bo'ladigan hamda qaror va uning ilovasida qo'llaniladigan «xakerlik hujumi» tushunchasining ta'rifini

amaliyotda qo'llash befovdadir. Kompyuter jinoyatchilarini qanday qilib to'g'ri nomlash mumkinligi (xaker, kraker yoki boshqacha) masalasida uzoq vaqtdan buyon bahs-munozaralar davom etayapti.

Ma'lumki, kompyuter himoyasi bo'yicha xizmat ko'rsatuvchi aksariyat kompaniyalar o'z buyurtmachilarining axborot tizimlari xavfsizligini tekshirish uchun xakerlar ishlab chiqqan texnik vositalardan foydalanadilar. Bunday vositalarning ishini amalda real hujumdan farqlab bo'lmaydi. Tarmoq analizatorlari (snifferlari)ning ma'lum variant (tur)lari tarmoqni boshqarish texnik vositasining tarkibiga kiradi.

Shu bilan birga, jinoyatchilar tizimlarni buzib kirish uchun ijtimoiy ijeneriyadan keng foydanadi. U, yuzaki qaraganda, oddiy odamlarning suhbatidek tuyulishi mumkin, aslida esa haqiqiy hujum bo'ladi.

Yuzaga keluvchi savollarga javob berishda intsident (hujum) tushunchasining o'zidan, shuningdek hujjatlarda foydalanish va mutaxassislar uchun intuitiv tushunarli bo'lgan bir qator qo'shimcha boshqa terminlardan foydalanish (DoS, DDoS hujumlar, sniffer va hokazo) maqsadga muvofiq bo'ladi.

Mazkur jinoyatlarning dalillar bazasini aniqlash ham yana bir muhim qadam hisoblanadi. Hujum to'xtatilganidan so'ng jinoyatchini topish va jazolashga urinib ko'rish zarur. Biroq hujumdan (muvaqqiyatli yoki muvaqqiyatsizligining farqi yo'q) keyin qoladigan aksariyat izlar – elektron qayd jurnallaridagi yozuvlar bo'ladi, xolos. Buning ustiga, elektron jurnallardan turli dasturlar sababli, shuningdek odamlar (tarmoq ma'murlari)ning foydalanishlari tufayli qandaydir hujum bo'lgani haqidagi yozuvning mavjudligi har doim ham haqiqatan hujum bo'lganligini bildirmaydi. Bu tizimdagi nosozlik bo'lishi yoki biror sababga ko'ra hujum bo'lgandek ko'rsatishga urinayotgan tarmoq ma'murining g'arazli qasdi ham bo'lishi mumkin. Nima dalil ekanligini, shuningdek qanday sharoitlarda uning topilishi, olib qo'yilishi, qayta ishlanishi, ko'rib chiqish uchun qabul qilinishi mumkinligini aniqlash mazkur xizmatdan o'z ishini muvaqqiyatli bajarish va asoslab berishni talab qiladi.

Jahon axborot hamjamiyatida bunday xizmatlarning faoliyati borasida muayyan tajriba to'plangan. Masalan "Kompyuter intsidentlariga chora ko'rish bo'yicha taxminiy funktsiyalar (Expectations for Computer Security Incident Response)" nomli RFC2350 bazaviy internet-tavsiya ko'pchilikka ma'lum. Ayniqsa mutaxassislar o'rtasida www.cert.org sayti juda ommalashgan bo'lib, uning birinchi sahifalaridayoq intsidentlarga chora ko'rish xizmati (CSIRT)ni tashkil qilish uchun zarur bo'lgan materiallar to'plami, shuningdek xizmat mutaxassislarining malakasiga qo'yiladigan namunaviy talablar qayd etildi.

Ushbu talablarning bo'limlaridan biri texnikaviy ko'nikmalardir saytda ko'rsatilishicha, xizmat mutaxassislaridan quyidagilar talab etiladi:

- xavfsizlik printsiplarini tushunish;
- axborot ob'ektlarining ojiz tomonlari va kamchiliklarini bilish;
- internetning tuzilishi haqida tasavvurga ega bo'lish;
- axborot xatarlarini tahlil qila olish;
- tarmoq protokollarini bilish;
- tarmoq ilovalari va servislarini bilish;
- tarmoq xavfsizligi masalalarini bilish;
- uzul yoki tizim xavfsizligi masalalarini tushunish;
- zararli dasturlar (viruslar, chuvalchanglar, troyanlar) haqida bilish;
- dasturlash ko'nikmasiga ega bo'lish.

Mazkur xizmat muvaffaqiyatli faoliyat ko'rsatishi uchun tegishli sohalardagi professional bilimlarga ega bo'lgan malakali mutaxassislar bilan jamlangan bo'lishi kerak. Aks holda, u intsidentlarni qayd etish apparatiga, tarmoq hodisalarining o'ziga xos arxiviga aylanadi, vaqti kelib esa (foydalanuvchilar amaliy foyda yo'qligini bilgach) ishini to'xtatishi mumkin. tabiyki malakali mutaxassislar yaxshigina to'lov talab qiladilar. Xizmat bunda zarur maqsadli moliyalashtirishsiz haddan tashqari tijoratlashib ketishi, ya'ni sub'ekti xizmat mehnatiga haq to'lashga tayyor bo'lgan intsidentlargagina haqiqatan chora ko'radigan holatga kelishi mumkin.

Ushbu xizmatni yanada rivojlantirish uchun mutaxassislarning mehnati uchun haq to'lash bilan birga, zamonaviy texnik jihozlar ham zarur bo'ladi. Bu esa xavfsizlikni ta'minlash uchun zamonaviy dasturlar, turli vositalar va apparatning so'ngi versiyalarini muntazam sotib olishni talab etadi, chunki bularsiz o'z ishida o'g'rincha dasturlardan foydalanuvchi xakerlarga qarshi kurash xizmatini tasavvur etish qiyin.

Butun dunyoda bunday darajadagi xizmatlar uchun yana bir muammo kompyuter hujumlari qurbonlarining yashirinligidir. Hujumga duch keladigan sub'ektlar axborot xavfsizligi bo'yicha xizmatlardan foydalanishni (agar mavjud bo'lsa), ko'rgan zararlariga tan berishni yoxud qandaydir texnik tafsilotlari u yoqda tursin, yuz bergan hujum faktining o'zi haqida ham hech narsa demaslikni ma'qul ko'radilar.

Axborot texnologiyalari sohasidagi jinoyatlarning oldini olishning ikkinchi guruhi – *tashkiliy-texnikaviy choralar bo'lib*, ularga quyidagilar kiradi: foydalanilayotgan kibermakonning lozim darajadagi kompyuter xavfsizligini boshqarishni tashkil qilish; kompyuter zallari hamda axborot olish, ishlash, uzatish va tahlil qilish vositalarini himoya qilish masalalarini ishlab chiqish; kompyuter xavfsizligini ta'minlash maqsadida kadrlar siyosatini yuritish.

AQSHda Milliy standartlar byurosi tomonidan kompyuter tarmoqlariga qo'yiladigan xavfsizlikning bazaviy talablari ishlab chiqilgan bo'lib, ular (standartlar) quyidagilardan iborat:

- 1) ruxsat etilgan holda tarmoqqa kirilishini ta'minlash maqsadida tarmoq beradigan kafolat sifatidagi yaroqlilik standarti;
- 2) ma'lum vazifalarni bajarish uchun ruxsatnomasi bor foydalanuvchilarninggina tarmoqqa kirishlarini ta'minlashi tarmoq funktsiyasi sifatidagi nazorat qilinuvchi foydalanish standarti;
- 3) ma'lumotlarni ruxsat etilmagan o'zgarishlar va yo'q qilishlardan himoya qilishda namoyon bo'ladigan daxlsizlik standarti;
- 4) ma'lumotlarning ruxsat etilmagan ochilishlardan himoyalanihini nazarda tutuvchi maxfiylik standarti;

5) foydalanuvchilarning identifikatsiyasi, uzatiladigan ma'lumotlarning sifati, axborotlarni uzatish vaqti yoki davomiyligi ta'minlanishining kafolati sifatidagi ma'lumotlarni uzatish xavfsizligi standarti.

Mazkur standartlar asosida quyidagi mezonlarga javob beruvchi tegishli texnik nazorat mexanizmlari ishlab chiqilgan:

a) yaxlitlik mezoni – mexanizmning kerakli rejimda ishlashini kafolatlovchi bazaviy ishonchlik;

b) tekshirish mumkinligi mezoni – kompyuter texnikasi vositalariga tajovuz qilishga urinishlar va tizim xavfsizligi masalalariga doir boshqa hodisalarni ochish va tekshirish uchun ahamiyatga ega bo'lishi mumkin bo'lgan axborotlarni yozish qobiliyati.

Ushbu choralarning amalga oshirilishi natijasida quyidagi imkoniyatlar yuzaga keladi:

- 1) kompyuter texnikasi vositalari (KTV)dan jismonan foydalanishni nazorat qilish;
- 2) KTV apparatlarining elektromagnit nurlanishini nazorat qilish;
- 3) KTVga tahdidlar imkoniyatlarini kuzatish va har bir ana shunday urinishlarni (monitoring usuli bilan) qayd etish.

Yuqorida keltirilgan xorijiy mamlakatlar tajribasi axborotlarni himoya qilishning asosiy maqsadlari va qoidalari bir qator bazaviy pozitsiyalarga ko'ra axborotlashtirish va ma'lumotlarni uzatish sohasidagi O'zbekiston Respublikasi qonunlarining profilaktik jihatini takomillashtirishga imkon beradi. Bu esa quyidagi imkoniyatlarni yaratadi:

- axborotlarning chiqib ketishi, o'g'irlanishi, yo'qotilishi, buzilishi va soxtalashtirilishining oldini olish;
- shaxs, jamiyat va davlat xavfsizligiga tahdidlarning oldini olish;
- axborotlarni yo'q qilish, modifikatsiyalash, buzish, ulardan nusxa ko'chirish, ularni bloklashga qaratilgan noqonuniy harakatlarning oldini olish;
- axborot resurslari va tizimlariga noqonuniy aralashishlarning oldini olish;
- mulk ob'ekti sifatidagi hujjatlashgan axborotlar faoliyatining huquqiy rejimini ta'minlash;

- davlat sirini va hujjatlashgan axborotlarning maxfiyligini saqlab qolish;
- sub’ektlarning axborot jarayonlari, tizimlari, texnologiyalari va ularni ta’minlash vositalarini yaratish, ishlab chiqarish va qo‘llashdagi huquqlarini ta’minlash.

Soha mutaxassislari mazkur jinoyatlarning oldini olishni uchta asosiy guruhga ajratadilar:

- 1) tashkiliy;
- 2) texnikaviy;
- 3) kompleks (dastlabki ikki guruhning ayrim usullarini birlashtiruvchi).

KTVni himoya qilishning tashkiliy choralari quyidagilarni o‘z ichiga oladi:

- axborot jarayonining barcha bosqichlarida ishtirok etuvchi xodimlarni tanlash, tekshirish va ularga yo‘l-yo‘riq berish bo‘yicha tashkiliy tadbirlar majmui;
- axborot ob’ektlari ishdan chiqqanidan keyin ularni tiklash rejasini ishlab chiqish;
- KTVga dasturiy-texnikaviy xizmat ko‘rsatilishini tashkil qilish;
- muayyan KTVlar xavfsizligini ta’minlash uchun mas’ul shaxslarga intizomiy javobgarlik yuklatish;
- kompyuter tizimlarining faoliyati chog‘ida maxfiylik rejimini amalga oshirish;
- ob’ektlarning jismoniy qo‘riqlanishi rejimini ta’minlash;
- moddiy-texnikaviy ta’minot va hokazo.

Axborot tizimlari xavfsizligi masalalari bilan shug‘ullanuvchi aksariyat mutaxassislarning fikricha, tashkiliy chora-tadbirlar axborotni himoya qilishning muhim va samarali, shu bilan birga, keyinchalik butun himoya tizimiga asos bo‘ladigan vositalaridan biridir.

Xorijdagi jinoyat ishlarining tergov qilinishiga oid materiallar tahlili aksariyat hollarda kompyuter jinoyatchigining sabablari va ularga imkon beradigan asosiy shart-sharoitlar quyidagilardan iborat bo‘lganligi haqida xulosa chiqarishga imkon beradi:

- xodimlarning ham alohida, ham moliyaviy operatsiyalarni amalga oshirish jarayonida dastlabki buxgalteriya hujjatlarining ma’lumotlarini masofadan turib

uzatish uchun mo'ljallangan avtomatlashgan tarmoqning ish stantsiyasi sifatida foydalaniladigan kompyuterning boshqaruv pulti (klaviaturasi)dan nazoratsiz foydalanishlari;

– xizmat ko'rsatayotgan xodimlarning harakatlarini nazoratsiz qoldirish jinoyatchining EHMdan jinoyat sodir etish quroli sifatida erkin foydalanishiga yordam beradi;

– dasturiy ta'minotning kiritilayotgan axborotning tegishliligi va to'g'riligini tekshirishni ta'minlovchi nazorat himoyasiga ega bo'lmagan darajadagi pastligi;

– ish stantsiyasi va uning dasturiy ta'minotidan ruxsatsiz foydalanishlardan himoyalashning parolli tizimining nomukammalligi va individual biometrik ko'rsatkichlar bo'yicha foydalanuvchining ishonchli tanilishi ta'minlamasligi;

– maxfiylik rejimi hamda tijorat axborotining maxfiyligi, shuningdek ularda kompyuter texnikasi vositalaridan ruxsatsiz foydalanishdan himoyalash xavfsizligi uchun javobgar mansabdor shaxsning yo'qligi;

– qat'iy moliyaviy hisobot hujjatlari, jumladan, mashina axboroti shaklidagilardan xodimlarning foydalanish uchun ruxsatlarida qat'iylikning yo'qligi;

– xodimlar bilan tijorat va xizmat sirlari, xodimlarga oid ma'lumotlar va boshqa maxfiy axborotlarni oshkor qilmaslik masalalarida shartnomalar (kontraktlar)ning yo'qligi.

Mazkur shaxslarning xizmat vazifalariga, avvalo, KTV xavfsizligini ta'minlashning tashkiliy choralarini amalga oshirishga doir quyidagi bandlarni kiritish maqsadga muvofiqdir:

- 1) muayyan tashkilot rahbariyati tomonidan KTVni himoya qilish talablarini qo'llab-quvvatlashning ta'minlanishi;
- 2) axborotni himoya qilish bo'yicha kompleks rejaning ishlab chiqilishi;
- 3) tashkilot faoliyatining xususiyatidan kelib chiqib axborotni himoya qilishga qaratilgan ustuvor yo'nalishlarning belgilab qo'yilishi;

4) ishlab chiqilgan rejaga muvofiq qo'riqlash tadbirlarini moliyalashtirish xarajatlari umumiy smetasining tuzilishi hamda tashkilot rahbariyatining uni rejaga ilova sifatida tasdiqlashi;

5) xodim bilan ma'muriyat o'rtasida tegishli shartnomalar tuzish orqali tashkilot xodimlarining o'z vakolatlari doirasida axborot xavfsizligi uchun javobgarliklarining belgilab qo'yilishi;

6) ruxsat berish shakllari, axborotning maxfiylik darajasi, maxfiy ma'lumotlar bilan ishlashiga ruxsat etilgan aniq shaxslar va shu kabilarni tartibga soluvchi yo'riqnomalar, qoidalar va buyruqlarning ishlab chiqilishi, joriy etilishi va bajarilishining nazorat qilinishi;

7) KTV himoyasini buzuvchilarga qarshi kurashning samarali choralarini ishlab chiqish.

Ayni vaqtda, amaliyotdan ma'lum bo'lishicha, KTV xavfsizligi choralarini samaradorligi oshirilishining eng ishonchli vositasi – xodimlarga muayyan tashkilotda qo'llanilayotgan tashkiliy-texnikaviy himoya choralarini o'rgatish va ular bilan tanishtirish.

Texnik choralar maxsus vazifaga ega bo'lgan quyidagi qurilmalardan foydalanishni nazarda tutadi:

- a) uzluksiz elektr ta'minoti manbalari;
- b) kompyuter texnikasi apparatlari, aloqa simlari va ular joylashgan xonalarni ekranlash qurilmalari;
- v) telefon tarmog'ini kompleks himoya qilish qurilmalari;
- g) yong'indan himoyalash qurilmalari;
- d) kompyuter portlarini himoya qilish vositalari.

Shuningdek, dasturiy ta'minotni himoya qilish uchun kompyuterdan foydalanishga ruxsat berish parametrlarini kiritish zarur. Ruxsat berishlar quyidagicha bo'lishi mumkin:

- 1) umumiy (har bir foydalanuvchiga shartsiz taqdim etiladigan);
- 2) rad etish uchun (shartsiz rad etish, masalan, axborotning bir qismini yo'q qilishga ruxsat so'ralganida);

- 3) hodisaga bog'liq bo'lgan (hodisa bilan boshqariladigan) (u foydalanuvchining murojaati bloklashirilishini nazarda tutadi, masalan, muayyan vaqt oralab yoki muayyan terminaldan kompyuter tizimiga murojaat etilganida bu holat kuzatiladi);
- 4) ma'lumotlarning mazmuniga bog'liq bo'lgan (bunda ruxsat berish haqidagi qaror ma'lumotlarning joriy ma'nosiga asoslanadi, masalan, ba'zi bir foydalanuvchilarning ayrim ma'lumotlarni o'qishlari taqiqlanadi);
- 5) holat (jumladan kompyuter tizimining dinamik holat)ga bog'liq bo'lgan (bunda kompyuter tizimi, uni boshqaruvchi dasturlar va himoya tizimining joriy holatiga bog'liq holda amalga oshiriladi, masalan, agar mashina axborotining tashuvchisi «faqat o'qish uchun» holatida bo'lmasa yoxud ushbu fayl joylashgan mantiqiy disk ochilmagunicha fayldan foydalanish taqiqlanishi mumkin);
- 6) qisman bog'liq bo'lgan (masalan, foydalanuvchining bir yoki bir necha marta foydalanishiga ruxsat etish orqali hodisalarni dinamik boshqarish imkoniyatining oldi olinadi);
- 7) foydalanuvchining ismi yoki boshqa belgilari bo'yicha (masalan, foydalanuvchi kamida 18 yosh bo'lishi kerak);
- 8) vakolatlarga bog'liq bo'lgan (foydalanuvchining ma'lumotlarga rejimdan – faqat o'qish yoki bajarish yoxud boshqa holatlardan – kelib chiqib murojaat etishini nazarda tutadi);
- 9) murojaatning tarixiga bog'liq bo'lgan;
- 10) parol bo'yicha.

Antivirus dasturlari xususida olimlar hozirgi vaqtda antiviruslar deyarli har qanday virusni zararsizlantirish uchun yetarli deb yakdil fikr bildirmoqdalar. Rossiyada ishlab chiqilgan bunday dasturlar orasidan quyidagilarni alohida ajratib ko'rsatish mumkin: AIDSTEST, AVP Systems, Adinf, Sheriff, Doctor Web. Ayniqsa oxirgi dastur hatto o'zini kodlashtiruvchi viruslarni ham yo'q qilish imkoniyatiga ega. Virusga qarshi dasturlar kompyuterning viruslardan 97 % gacha himoyalanihini ta'minlaydi. 3 % esa mutlaqo ishonchli tizimlar bo'lmasligining tasdig'idir. Umuman olganda, agar eng oddiy qoidalar (masalan kerakli dasturlarning arxivlarini yaratish, kompyuterga viruslarni olib kelishi ehtimoli

bo'lgan axborot tashuvchilarni o'rnatmaslik, kompyuterni vaqti-vaqti bilan viruslar bor-yo'qligi masalasida tekshirib turish kabilar)ga rioya etilsa, ortiqcha muammolarga yo'liqmaslik mumkin.

O'zbekistonda kompyuter intsidentlariga chora ko'rish xizmati (UZ-CERT) milliy axborot tizimlari va internet tarmog'ining segmentidan foydalanuvchilar uchun mo'ljallangan bo'lib, u kompyuter intsidentlari bo'yicha ma'lumotlarning to'planishi va tahlil qilinishi, foydalanuvchilarga kompyuter xavfsizligi tahdidlarining oldini olishda maslahatlar berish va ularni texnik jihatdan qo'llab quvvatlashni ta'minlovchi yagona markaz. Shu bois, agar kompyuter resursi hujumga uchrasa, <http://www.uz-cert.uz> manzili bo'yicha maxsus xizmatga murojaat etish maqsadga muvofiqdir. Bu esa axborot texnologiyalari bilan bog'liq jinoyatlarda yakka tartibdagi viktimologik profilaktikani ta'minlaydi.

Shuni alohida ta'kidlash lozimki, O'zbekiston Respublikasida axborot texnologiyalari sohasidagi jinoyatlarning oldini olish jarayonining tashkil qilinishi kompyuter xavfsizligi tizimini rivojlantirish bosqichidadir. Bu esa nafaqat kuchga asoslanuvchi tuzilmalar, balki kompyuter va axborot texnologiyalarini rivojlantirish va joriy etish markazi qoshida yangi tashkil qilingan kompyuter intsidentlariga chora ko'rish xizmati (UZ-CERT)dan ham kompleks yondashuv va sa'y-harakatlarni talab qiladi.

XULOSA

Mazkur qo‘llanmada axborot huquqiy munosabatlar sohasida yangilik bo‘lgan jinoiy-huquqiy munosabatlar choralari fikrlashga yo‘nalgan tadqiqotni amalga oshirishga harakat qilingan. Mazkur sohadagi tadqiqotning boshlang‘ich yakuni bo‘lib, “axborot texnologiyalari sohasidagi jinoyatlar” tushunchasini ta’riflovchi asosiy qoidalarni ishlab chiqish va uning alohida turlarini tahlil qilish hisoblanadi. O‘quv qo‘llanmada o‘z aksini topgan mazkur qoidalar keyingi tadqiqotlar uchun asos bo‘lib xizmat qilishi yoki ulardan huquqni qo‘llash amaliyotida uslubiy qo‘llanma sifatida foydalanish mumkin bo‘ladi.

Axborot texnologiya sohasidagi jinoyatlarga qarshi kurashdagi MDH mamlakatlari huquqni muhofaza qilish organlarining tajribasi shuni ko‘rsatmoqdaki, mazkur jinoyatlar osonlik bilan amalga oshirilayotgan bo‘lsa-da, ularni ochish (fosh etish) nihoyatda murakkabdir. Shuningdek, mazkur jinoyatlarni tergov qilish (JK Maxsus qismi XX¹ bob normalariga O‘zbekiston Respublikasi Oliy sudi Plenumini tomonidan rasmiy sharhlar amalga oshirilmaganligi sababli) ham murakkablashmoqda.

Ushbu turdagi jinoyatlarga qarshi kurash bo‘yicha xorijlik hamkasblarning tajribasini tahlil etish foydadan holi bo‘lmaydi, masalan Rossiyada, bir tomondan, jamiyatida kompyuterlashtirish jarayonlari tezkorlik bilan amalga oshirilayotganligi, ikkinchi tomondan, mamlakatda kompyuter orqali sodir etilayotgan jinoyatlardan jabr ko‘rayotganlar soni oshib borayotganligi ko‘zga tashlanadi. Kompyuter tizimi yuqori darajadagi texnologiyalarga egaligi va ushbu xususiyat bu tizim egalarini ob‘ektiv sabablari va shaxsiy omillariga ko‘ra turli-tuman jabr ko‘rishlariga olib kelmoqda. Bu haqda axborot texnologiyalari rivojlangan xorij mamlakatlarining tajribasi ham guvohlik beradi. Unga ko‘ra, kompyuter tajovuzlaridan jabr ko‘rganlar va bu haqda ariza bilan murojaat qilayotgan shaxslarning soni anchagina. O‘zbekistonda ham boshqa mamlakatlardagi kabi kompyuter jinoyatlaridan jabr ko‘rganlar soni oshib borishi va ularga keltirilgan moddiy zararlar jinoyatlarning boshqa turlaridagiga nisbatan ikki hissa va undan ham ko‘p bo‘lishi mumkin.

Axborot texnologiyalari sohasidagi jinoyatlarning sodir etilishi natijasida nafaqat jismoniy shaxslar, balki yuridik shaxslar, hatto davlatlar ham zarar ko'rishlari mumkin. Kompyuter texnologiyalari asrida portlovchi kurilmalardan foydalangandan ko'ra, kompyuter klaviaturasi va "sichqoncha" sini ishga solib zarar keltirish osonroqdir. Shuning uchun ham viktimologik ma'noda jabrlanuvchi – bu "jismoniy shaxs", degan ilmiy tushuncha kompyuter jinoyatlari sohasida ham qo'llanilganda unchalik o'zini oqlamaydi. Boshqacharoq aytganda, ular nafaqat jismoniy shaxs, balki har qanday shakldagi kishilar jamoasi ham bo'lishlari, shu bilan birga, jabrlanuvchilar (bevosita yoki bilvosita) jismoniy, axloqiy va moddiy zarar ko'rishlari mumkin. Ma'lum bir holatlarda ushbu turdagi jinoyatlar sodir etilganda, bir vaqtning o'zida ulardan nafaqat jismoniy shaxslar balki, yuridik shaxslar ham jabr ko'rishlari mumkin. Bunday hollarda jabrlangan shaxslarning faoliyat xususiyatlari, moliyaviy ahvoli, foydalangan hisoblash texnikasining taktik-texnik ko'rsatkichlari, aloqa va telekommunikatsiya vositalari, zararlarining tashkiliy-huquqiy shakllari kabilar ham hisobga olinishi lozim. Axborot texnologiyalari sohasidagi jinoyatlar kompyuter texnikasiga ega har qanday tashkilotlar uchun xavf tug'dirishi mumkin. Kompyuter qurilmalarining izdan chiqarilishi yoki tizimning buzilishi tufayli eng katta bank ham to'rt sutkada, kichik muassasalar esa bir sutkada inqirozga yuz tutishi mumkin. Shuning uchun tashkiliy-huquqiy shakliga ko'ra, yuridik shaxs maqomiga ega yoki ega emasligidan qat'iy nazar, turli muassasa, korxonalar va tashkilotlar (ya'ni aktsiyadorlar jamiyati, mas'uliyati cheklangan korxonalar, notijorat tashkilotlar) teng darajada kompyuter jinoyatlaridan jabr ko'rishlari mumkin.

Kompyuter viruslarining axborot tarmoqlariga tushishi nafaqat fuqarolar, korxonalar, tashkilotlar, muassasalar, kompaniyalar yoki firmalarga zarar keltiradi, balki davlatga ham, jamiyatga ham ziyon keltiradi. Masalan, axborot terrorizmi natijasida aholiga biror xavf-xatar bo'lsa, muayyan davlatdagi insonlar jabr ko'rishlari mumkin (2005 yilning 14 iyulida Belorussiya Respublikasidagi temir yo'lining minalashtirilganligi to'g'risidagi fakt yuqoridagi fikrni tasdiqlaydi). Kompyuter jinoyatlarining global oqibatlari haqida amaliyotda misollar yo'q,

ammo “dunyo terroristik virusi” mavjudligi sababli bu holat sodir bo‘lishi mumkin. Yadro markazlarining axborot tizimiga tajovuz qilinganligi to‘g‘risida ma’lumotlar mavjud. 1998 yilda Baba nomidagi Hindiston yadro tadqiqotlari markaziga terrorchilar hujum qilib, reaktorning boshqarish tizimini izdan chiqarish bilan qo‘rqo‘vga solganlar. Afsuski, buning oqibatida reaktor portlashi mumkin edi. Internet tarmoqlarida katta va kichik islom tashkilotlari, jumladan radikal qiyofadagi (“Xalqaro islom fronti”, “Islom guruhi”, “O‘zbekiston islom harakati” singari) tashkilotlarning saytlari mavjud bo‘lib, ular g‘arazli maqsadlarni noto‘g‘ri, yolg‘on axborotlarni targ‘ibot-tashviqot qilish orqali faoliyat yuritadilar. Mutaxassislar yangi turdagi islom tashkilotining tuzilishi haqida so‘z yuritishib, uning asosida aniq tashkiliy aloqa emas, balki yagona axborot makoni bo‘lishini ta’kidlaydilar.

Yuqoridagi fikrlardan kelib chiqqan holda, jinoyat qonunchiligining kiberterrorizm qismiga huquqiy tartibga solishdagi kamchiliklarni bartaraf etish uchun JK Maxsus qismi XX¹ bobi normalariga kiberterrorizm aktlarini sodir etganlik uchun jinoiy javobgarlikni ko‘zda tutuvchi normalarni kiritish maqsadga muvofiq bo‘ladi.

Kompyuterdan foydalanuvchilarni xavf-xatardan himoya qilish uchun jinoiy–huquqiy jihatlarni kuchaytirish zarur, chunki kelgusida jinoiy–huquqiy muhofazaga muhtoj ob’ektlarga keng miqyosda tajovuz bo‘lish ehtimoli mavjud. Jumladan, “Comruter Emergency Response Team” (CERT) koordinatsion markazining ma’lumotlariga ko‘ra, kompyuter xavfsizligiga qarshi tajovuzlarning yaqin yillarda 170 minggacha oshishi bashorat qilinmoqda. Bu esa SERT tomonidan 1988 yildan buyon to‘plangan axborotlardagi ro‘yxatga mos keladi. Shu bois huquqni muhofaza qilish organlarining ulkan axborot mahsulotlari foydalanuvchilari, korxonalar, tashkilotlar, bank va firmalarning kompyuter xavfsizligi xizmatlari (xodimlari) bilan (hozirda mamlakatimizda ko‘pchilik korxonalarda bunday xodimlar bo‘lmas-da) o‘zaro hamkorlik o‘rnatishlari viktimologik profilaktikaning muhim sharti hisoblanadi. Bugungacha kompyuter jinoyatchiligining viktimologik profilaktikasini tashkil etish va taktikasi bo‘yicha

qo‘llanilishi mumkin bo‘lgan metodik ko‘rsatma yoki uslubiy qo‘llanmalar ishlab chiqilmagan, mazkur jinoyatlardan jabr ko‘rganlar uchun metodik ishlar qilinmagan. Kasbiy bilim va amaliy ko‘nikmalarning yetarli darajada emasligi huquqni muhofaza qilish organlari tomonidan axborot texnologiyalari sohasidagi jinoyatchilikning oldini olish bo‘yicha profilaktik tadbirlarni zarur darajada o‘tkazish imkonini bermayapti. Hozirgi davrda mazkur yo‘nalishlardagi jinoyatchilikka qarshi kurash moliyalashtirilmagan va xodimlarning malakasini oshirish hamda qayta tayyorlash uchun zarur asos yo‘q. Masalan, AQSHda ham kiberjinoyatchilarga qarshi kurash uchun hukumat tomonidan ajratilgan mablag‘ huquqni muhofaza qilish organlari uchun ajratilgan mablag‘ning yuzdan biridan ham kamroqni tashkil etadi.

Axborot tizimining himoyasizligi jihatidan ham bizda huquqiy bo‘shliq mavjud, ya’ni jinoyat qonunida kompyuter axborotlariga noqonuniy egalik qilganlik uchun jinoiy javobgarlik ko‘zda tutilmagan. Aslida, bunday javobgarlik kompyuter axborotlarining qalbakilashtirilganligi uchun ko‘zda tutiladigan javobgarlikdan ko‘ra zarurroqdir. Mazkur masalada dunyoning rivojlangan mamlakatlarida Osiyo va Yevropa bozorlarini to‘ldirib tashlagan lazer disklarning nusxalarini “qaroqchilarcha” ko‘paytirib tarqatish bilan bog‘liq vaziyatlar mavjudki, natijada bunday faoliyatlar bilan shug‘ullanayotganlarga rahbarlik qilayotgan jinoiy guruh tashkilotchilari juda katta foydaga ega bo‘lib, noqonuniy boylik orttirmoqdalar. Ushbu tajovuzkorlikning oqibatlari nihoyatda ayanchli bo‘lishi sababli, mazkur qilmish uchun jinoiy javobgarlikning o‘rnatilishi shart.

Alohida qayd etilishi lozimki, O‘zbekistonda kompyuter bilan bog‘liq jinoyatlarga qarshi kurash tashkiliy–huquqiy asosga ega bo‘lib bormoqda. Jumladan, O‘zbekiston Respublikasi Prezidentining 2005 yil 5 sentyabrda qabul qilingan “Milliy axborot–kommunikatsiya tizimining kompyuter xavfsizligini ta’minlash bo‘yicha qo‘shimcha chora–tadbirlar to‘g‘risida”gi qaroriga asosan “O‘zinfokom” (UZ-CERT) kompyuter va axborot texnologiyalarini joriy etish va rivojlantirish markazi qoshida kompyuterlar asosida kelib chiqadigan ziddiyatlarni kuzatib borish xizmati tashkil etilgan. Aynan mazkur xizmat huquqni muhofaza

qilish organlari bilan samarali hamkorlik olib borish orqali axborot texnologiyalari sohasidagi jinoyatlarni aniqlashi, ochishi va monitoringini ta'minlashi mumkin.

Ta'kidlash joizki, sud kompyuter texnikalari ekspertizasini o'tkazish metodikasining ishlab chiqilmaganligi tashkiliy–huquqiy jihatdagi dolzarb muammolardan biridir. Shu sababli, O'zbekiston Respublikasi huquqni muhofaza qilish organlarining ekspertiza xizmatlari e'tiborni o'z tarkibini sud kompyuter texnikalari ekspertizasini o'tkazish sohasidagi mutaxassislar bilan ham to'ldirishga qaratishlari lozim. O'zbekiston Respublikasi IIV Akademiyasida esa ekspert–kriminalistlar tayyorlash bo'yicha yangicha yo'nalish ishlab chiqilib, unda sud kompyuter texnikalari ekspertizasini o'tkazish uchun malakaga ega bo'lgan ekspert–kriminalistlar o'qitishi va bu maqsadda Moskva, Sankt–Peterburg va Volgogradagi mazkur soha mutaxassislarni tayyorlash bo'yicha tajribalarni o'rganish maqsadga muvofiqdir.

Bundan tashqari, mazkur turdagi ekspertiza metodikasi to'g'risidagi axborotni izlab topish va taqdim etish UZ–CERT xizmatining eng asosiy va doimiy vazifasi bo'lmog'i lozim. Bularning barchasi kiberjinoyatchilikka qarshi kurash va oldini olishda samaradorlikka erishishga xizmat qiladi.

Nazorat savollari va topshiriq:

1. Axborot texnologiyalari sohasidagi jinoyatlar uchun jinoiy javobgarlik o'rnatishning ijtimoiy holatini belgilang.
2. Axborot texnologiyalari sohasidagi jinoyatlarning umumiy, ma'lum turdagi (rodovoy), ma'lum ko'rinishdagi (vidovoy) va bevosita ob'ektlarini aytib bering.
3. Qanday ijtimoiy-xavfli qilmishlar axborot texnologiyalari sohasidagi jinoyatlar hisoblanadi?
4. "Axborot texnologiyalari sohasidagi jinoyatlar" tushunchasini ta'riflang.
5. Axborot texnologiyalari sohasidagi jinoyatlar boshqa o'xshash jinoyatlar tartibidan nimasi bilan farq qiladi?
6. Axborot olish qoidalarini buzish deganda nimani tushunasiz?
7. Axborot texnologiyalari sohasidagi jinoyatlarda qo'llaniladigan «katta zarar», «sezilarli ziyon» va «o'ta katta zarar» tushunchalarini ta'riflang.
8. Axborot olish qoidalarini buzuvchi sub'ekt deganda nimani tushunasiz?
9. JK 278¹-moddasida ko'zda tutilgan jinoyatning sub'ektiv tomonini tavsiflang.
10. Kompyuter axborotlariga noqonuniy egalik qilish deganda nimani tushunasiz?
11. Kompyuter axborotlarini yo'q qilish, blokka olish, modifikatsiyalash, undan nusxa ko'chirish, noqonuniy egallash deganda nimani tushunasiz?
12. JK 278²-moddasida ko'zda tutilgan jinoyatga qo'llanuvchi EHM, uning tizimi yoki tarmoqlari ishining buzilishi deganda nimani tushunasiz?
13. "Kompyuter axborotlari" tushunchasini ta'riflang?
14. Kompyuter tizimiga noqonuniy ravishda kirish uchun zarur bo'ladigan maxsus vositalarni sotish maqsadida tayyorlash, sotish yoki tarqatish uchun qanday javobgarlik belgilangan?
15. JK 278³-moddasida ko'zda tutilgan jinoyatni sodir etish uchun "qo'llanuvchi maxsus dasturiy yoki apparat vositalari" tushunchasini ta'riflang?

16. Himoyalangan kompyuter tizimi nimani anglatadi?
17. JK 278³-moddasida ko‘zda tutilgan jinoyat turini aytib bering.
18. Kompyuter tizimida saqlanayotgan axborotlarni o‘zgartirish, shikast yetkazish, o‘chirib tashlash deganda nimani tushunasiz?
19. “Kompyuter sabotaji” tushunchasini ta’riflang.
20. Begona yoki xizmat kompyuter qurilmasini ishdan chiqarish yoxud kompyuter tizimini buzish nimani bildiradi?
21. Qanday sharoitda kompyuter sabotaji tugallangan jinoyat deb tan olinadi?
22. “Zarar keltiruvchi va virusli dasturlar” tushunchasini ta’rifini keltiring.
23. JK 278⁶-moddasida ko‘zda tutilgan jinoyatning ob’ektiv tomonini nima tashkil etadi?
24. JK 278⁶-moddasida ko‘zda tutilgan jinoyatning sub’ektiv tomoni qanday?
25. Axborot texnologiyalari sohasidagi jinoyatlarning oldini olishga yo‘naltirilgan huquqiy hujjatlarni sanab bering.
26. Axborot texnologiyalari sohasidagi jinoyatlarning oldini olishning tashkiliy -texnik choralari deganda nimani tushunasiz?

O‘zbekiston Respublikasining Qonuni
AXBOROTLASHTIRISH VA MA’LUMOTLAR UZATISH SOHASIDA
QONUNGA XILOF HARAKATLAR SODIR ETGANLIK UCHUN
JAVOBGARLIK KUCHAYTIRILGANLIGI MUNOSABATI BILAN
O‘ZBEKISTON RESPUBLIKASINING AYRIM QONUN HUIJATLARIGI
O‘ZGARTISH VA QO‘SHIMCHALAR KIRITISH TO‘G‘RISIDA

(O‘zbekiston Respublikasi qonun hujjatlari to‘plami, 2007 y., 52-son, 532-
modda)

Qonunchilik palatasi tomonidan 2007 yil 27 sentyabrda qabul qilingan

Senat tomonidan 2007 yil 30 noyabrda ma’qullangan

1-modda. O‘zbekiston Respublikasining 1994 yil 22 sentyabrda qabul qilingan 2012-XII-sonli qonuni bilan tasdiqlangan O‘zbekiston Respublikasining Jinoyat kodeksiga (O‘zbekiston Respublikasi Oliy Kengashining Axborotnomasi, 1995 yil, №1, 3-modda; O‘zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 1996 yil, №9, 144-modda; 1997 yil, №2, 56-modda, №9, 241-modda; 1998 yil, №5-6, 102-modda, №9, 181-modda; 1999 yil, №1, 20-modda, №5, 124-modda, №9, 229-modda; 2000 yil, №5-6, 153-modda; 2001 yil, №1-2, 23-modda, №9-10, 165-modda; 2002 yil, №9, 165-modda; 2003 yil, №1, 8-modda, №9-10, 149-modda; 2004 yil, №1-2, 18-modda, №9, 171-modda; O‘zbekiston Respublikasi Oliy Majlisi palatalarining Axborotnomasi, 2005 yil, №9, 314-modda, №12, 417, 418-moddalar; 2006 yil, №6, 261-modda, №12, 656-modda; 2007 yil, №4, 158, 166-moddalar, №6, 248-modda, №9, 416, 422-moddalar) quyidagi o‘zgartish va qo‘shimchalar kiritilsin:

- 1) 174-modda chiqarib tashlansin;
- 2) Quyidagi mazmundagi XX¹ bob bilan to‘ldirilsin:

«XX¹ bob. Axborot texnologiyalari sohasidagi jinoyatlar
278¹-modda. Axborotlashtirish qoidalarini buzish

Axborotlashtirish qoidalarini buzish, ya'ni belgilangan himoya choralarini ko'rmagan holda axborot tizimlari, ma'lumotlar bazalari va banklarini, axborotga ishlov berish hamda uni uzatish tizimlarini yaratish, joriy etish va ulardan foydalanish hamda axborot tizimlaridan ruxsat bilan foydalanish fuqarolarning huquqlariga yoki qonun bilan qo'riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko'p miqdorda zarar yoxud jiddiy ziyon yetkazilishiga sabab bo'lsa, —

eng kam oylik ish haqining ellik baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari bilan jazolanadi.

O'sha harakatlar juda ko'p miqdorda zarar yetkazgan holda sodir etilgan bo'lsa, —

eng kam oylik ish haqining ellik baravaridan yuz baravarigacha miqdorda jarima yoki bir yildan ikki yilgacha axloq tuzatish ishlari yoxud olti oygacha qamoq bilan jazolanadi.

278²-modda. Kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish

Kompyuter axborotidan, ya'ni axborot-hisoblash tizimlari, tarmoqlari va ularning tarkibiy qismlaridagi axborotlardan qonunga xilof ravishda (ruxsatsiz) foydalanish, agar ushbu harakat axborotning yo'q qilib yuborilishi, to'sib qo'yilishi, modifikatsiyalashtirilishi, undan nusxa ko'chirilishi yoxud uning qo'lga kiritilishiga, elektron hisoblash mashinalari, elektron hisoblash mashinalari tizimi yoki ularning tarmoqlari ishining buzilishiga sabab bo'lsa, —

eng kam oylik ish haqining yuz baravarigacha miqdorda jarima yoki uch yilgacha muayyan huquqdan mahrum qilish yoxud bir yilgacha axloq tuzatish ishlari bilan jazolanadi.

O'sha harakat:

- a) bir guruh shaxslar tomonidan oldindan til biriktirib;
- b) takroran yoki xavfli retsivist tomonidan;
- v) xizmat mavqeidan foydalangan holda;

g) uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilgan bo‘lsa, —

eng kam oylik ish haqining yuz baravaridan uch yuz baravarigacha miqdorda jarima yoki bir yildan ikki yilgacha axloq tuzatish ishlari yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

278³-modda. Kompyuter tizimidan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o‘tkazish maqsadini ko‘zlab tayyorlash yoxud o‘tkazish va tarqatish

Himoyalangan kompyuter tizimidan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus dasturiy yoki apparat vositalarini o‘tkazish maqsadini ko‘zlab tayyorlash yoxud o‘tkazish va tarqatish —

eng kam oylik ish haqining ikki yuz baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari bilan jazolanadi.

O‘sha harakatlar:

a) bir guruh shaxslar tomonidan oldindan til biriktirib;

b) takroran yoki xavfli retsidivist tomonidan;

v) xizmat mavqeidan foydalangan holda;

g) uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilgan bo‘lsa, —

eng kam oylik ish haqining ikki yuz baravaridan uch yuz baravarigacha miqdorda jarima yoki bir yildan uch yilgacha axloq tuzatish ishlari bilan jazolanadi.

278⁴-modda. Kompyuter axborotini modifikatsiyalashtirish

Kompyuter axborotini modifikatsiyalashtirish, ya’ni kompyuter tizimida saqlanayotgan axborotni qonunga xilof ravishda o‘zgartirish, unga shikast yetkazish, uni o‘chirish, xuddi shuningdek bila turib unga yolg‘on axborotni kiritish fuqarolarning huquqlariga yoki qonun bilan qo‘riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko‘p miqdorda zarar yoxud jiddiy ziyon yetkazilishiga sabab bo‘lsa, —

eng kam oylik ish haqining yuz baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari yoxud ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

O‘sha harakatlar:

a) juda ko‘p miqdorda zarar yetkazgan holda;

b) bir guruh shaxslar tomonidan oldindan til biriktirib;

v) takroran yoki xavfli retsivist tomonidan sodir etilgan bo‘lsa, —

bir yildan ikki yilgacha axloq tuzatish ishlari yoki ikki yildan uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

278⁵-modda. Kompyuter sabotaji

O‘zganing kompyuter uskunasini yoki xizmatda foydalaniladigan kompyuter uskunasini qasddan ishdan chiqarish, xuddi shuningdek kompyuter tizimini buzish (kompyuter sabotaji) —

uch yilgacha muayyan huquqdan mahrum qilib, eng kam oylik ish haqining uch yuz baravaridan to‘rt yuz baravarigacha miqdorda jarima yoki ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

O‘sha harakatlar:

a) bir guruh shaxslar tomonidan oldindan til biriktirib;

b) takroran yoki xavfli retsivist tomonidan sodir etilgan bo‘lsa, —

ikki yildan uch yilgacha axloq tuzatish ishlari yoxud ikki yildan uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

278⁶-modda. Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish

Kompyuter tizimida saqlanayotgan yoki uzatilayotgan axborotni ruxsatsiz yo‘q qilib yuborish, to‘sib qo‘yish, modifikatsiyalashtirish, undan nusxa ko‘chirish yoki uni qo‘lga kiritish maqsadini ko‘zlab kompyuter dasturlarini yaratish yoki mavjud dasturlarga o‘zgartirishlar kiritish, xuddi shuningdek maxsus virus dasturlarini ishlab chiqish, ulardan qasddan foydalanish yoki ularni qasddan tarqatish —

eng kam oylik ish haqining yuz baravaridan uch yuz baravarigacha miqdorda jarima yoki ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

O'sha harakatlar:

a) juda ko'p miqdorda zarar yetkazgan holda;

b) bir guruh shaxslar tomonidan oldindan til biriktirib;

v) takroran yoki xavfli retsivist tomonidan;

g) uyushgan guruh tomonidan yoki uning manfaatlarini ko'zlab sodir etilgan bo'lsa, —

ikki yildan uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi».

O'zbekiston Respublikasining Prezidenti

I. KARIMOV

Toshkent sh.,

2007 yil 25 dekabr

O‘ZBEKISTON RESPUBLIKASINING QONUNI
ELEKTRON HISOBLASH MASHINALARI UCHUN YARATILGAN
DASTURLAR VA MA’LUMOTLAR BAZALARINING HUQUQIY
HIMOYASI TO‘G‘RISIDA

(O‘zbekiston Respublikasi Oliy Kengashining Axborotnomasi, 1994 y., 5-son, 136-modda; O‘zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2002 y., 4-5-son, 74-modda, 9-son, 165-modda)

Ushbu qonun EHM uchun dasturlar va ma’lumotlar bazalarini yaratish, ularning huquqiy himoyasi va ulardan foydalanish bilan bog‘liq munosabatlarni tartibga soladi.

Qoraqalpog‘iston Respublikasida EHM uchun yaratilgan dasturlar va ma’lumotlar bazalarining huquqiy himoyasi borasidagi munosabatlar Qoraqalpog‘iston Respublikasining qonun hujjatlari bilan ham tartibga solinadi.

1-modda. Asosiy tushunchalar

Ushbu Qonunda qo‘llaniladigan asosiy tushunchalar:

ma’lumotlar bazasi — ob‘ektiv shaklda ifodalangan hamda elektron hisoblash mashinalari (EHM) yordamida topish va ishlov berish mumkin bo‘ladigan tarzda bir tizimga solingan ma’lumotlar (masalan: maqolalar, hisob-kitoblar) majmui;

EHM uchun yaratilgan dastur — ob‘ektiv shaklda ifodalangan hamda muayyan natija olish maqsadida EHM, EHM shoxobchalari va boshqa kompyuter vositalarining ishlashi uchun mo‘ljallangan ma’lumotlar va ko‘rsatmalar majmui;

(1-moddaning birinchi qismi ikkinchi va uchinchi xatboshilari O‘zbekiston Respublikasining 2002 yil 5 apreldagi 364-II son qonuni tahririda — Oliy Majlis Axborotnomasi, 2002 y., 4-5-son, 74-modda)

boshlang‘ich matn — birorta dasturlash tilida yozilgan, biron-bir kompilyator qayta ishlamagan matn;

ob'ekt kodi — boshlang'ich matnning mashina kodiga aylantirilishi natijasida yuzaga kelgan dastur;

EHM uchun yaratilgan dasturni dekomplyatsiya qilish — EHM uchun yaratilgan dasturning tarkibiy tuzilishi va kodlanishini o'rganish maqsadida ob'ekt kodini boshlang'ich matnga aylantirishni o'z ichiga oladigan texnikaviy usul;

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining adaptatsiyasi — yuzaga kelgan muayyan sharoitda EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining ishlashini ta'minlash maqsadidagina amalga oshiriladigan hamda (dekomplyatsiya qilish oqibatida) muallifning boshlang'ich matni o'zgarishiga olib kelmaydigan qo'shimchalar kiritish;

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini modifikatsiyalash (qayta ishlash) — ularni adaptatsiya deb hisoblanmaydigan va boshlang'ich matn o'zgarishiga olib keladigan har qanday tarzda o'zgartirish;

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasidan nusxa olish — EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini har qanday moddiy shaklda bitta yoki ko'proq nusxada tayyorlash hamda ularni EHMning xotirasiga yozish;

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini tarqatish — EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining har qanday moddiy shaklda, shu jumladan tarmoqlar vositasida va boshqa usullar yordamida, shuningdek sotish, prokatga berish, ijaraga topshirish, qarzga berib turish, jumladan ushbu maqsadlarning istalgani uchun import qilish yo'li bilan olingan nusxalaridan foydalanishni ta'minlash;

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini bosib chiqarish (e'lon qilish) — EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining nusxalarini muallifning roziligi bilan nomuayyan shaxslar doirasiga berish (jumladan, EHM xotirasiga yozish va bosma matn chiqarish yo'li bilan berish);

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasidan foydalanish — ularni bosib chiqarish, ulardan nusxa olish, ularni tarqatish hamda xo'jalik muomalasiga (jumladan, modifikatsiyalashtirilgan shaklda) kiritish yuzasidan

boshqa harakatlarni amalga oshirish. EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining bosib chiqarilganligi to'g'risidagi xabarlarini ommaviy axborot vositalarining ma'lum qilishi EHM uchun yaratilgan dastur yoki ma'lumotlar bazasidan foydalanish deb e'tirof qilinmaydi.

Huquq egalari — muallif, — uning merosxo'rlari, shuningdek qonun yoki shartnoma asosida mutlaq shaxsiy va mulkiy huquqlarga ega bo'lgan har qanday jismoniy yoki yuridik shaxslar.

2-modda. Xalqaro shartnomalar va bitimlar

Basharti, O'zbekiston Respublikasining xalqaro shartnomalari yoki bitimlarida ushbu qonunda nazarda tutilganidan o'zgacha qoidalar belgilangan bo'lsa, xalqaro shartnoma yoki bitim qoidalari qo'llaniladi.

3-modda. Huquqiy himoya ob'ekti

Ushbu qonun EHM uchun yaratilgan dasturlar va ma'lumotlar bazalarini mualliflik huquqi ob'ektlari sirasiga kiritadi.

Vazifasi va afzalliklaridan qat'i nazar, ob'ektiv shaklda ifodalangan, bosib chiqarilgan hamda bosib chiqarilmagan, muallif (hammualliflar) ijodiy faoliyatining natijasi bo'lgan, EHM uchun yaratilgan har qanday dasturlar va ma'lumotlar bazalariga nisbatan mualliflik huquqi tatbiq etiladi. EHM uchun yaratilgan dastur yoki ma'lumotlar bazasiga mualliflik huquqi toki aksi isbotlanmagunga qadar saqlanib qolaveradi.

(3-moddaning ikkinchi qismi O'zbekiston Respublikasining 2002 yil 5 apreldagi 364-II son Qonuni tahririda — Oliy Majlis Axborotnomasi, 2002 y., 4-5-son, 74-modda)

Ushbu qonun bilan beriladigan huquqiy himoya:

har qanday dasturlash tilida va har qanday shaklda ifodalanishi mumkin bo'lgan EHM uchun yaratilgan dasturlarning barcha xiliga (shu jumladan, operatsiya tizimlari va dasturiy majmualarga) nisbatan, boshlang'ich matn va ob'ekt kodiga nisbatan ham, shuningdek ma'lumotlarni tanlash va tashkil etish bo'yicha ijodiy mehnatning natijasi bo'lgan ma'lumotlar bazalariga nisbatan tatbiq etiladi;

EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalari yohud ularning biron-bir qismiga asos bo'lgan g'oyalar va printsiplarga, shu jumladan interfeys hamda algoritm tashkil qilish g'oyalari va printsiplariga, shuningdek dasturlash tillariga nisbatan tatbiq etilmaydi.

4-modda. EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalariga nisbatan mualliflik huquqini e'tirof etish shartlari

EHM uchun dasturlar yoki ma'lumotlar bazalariga nisbatan mualliflik huquqi ular yaratilgach yuzaga keladi. EHM uchun yaratilgan dastur yoki ma'lumotlar bazasiga bo'lgan mualliflik huquqi e'tirof etilishi va ro'yobga chiqarilishi uchun ro'yxatdan o'tkazish yoki o'zga rasmiyatchiliklarga rioya etish talab qilinmaydi.

Mualliflik huquqi ob'ekti bo'lmagan materiallardan (asarlardan) tarkib topgan ma'lumotlar bazasiga nisbatan mualliflik huquqi ma'lumotlar bazasini yaratgan shaxslarga tegishli bo'ladi.

Boshqa shaxsning mualliflik huquqi ob'ekti bo'lgan materiallarni o'z ichiga olgan ma'lumotlar bazasiga bo'lgan mualliflik huquqi bunday materiallarning har biriga nisbatan mualliflik huquqiga rioya qilingan taqdirdagina e'tirof etiladi.

Ma'lumotlar bazasiga kiritilgan materiallarning har biriga nisbatan mualliflik huquqi saqlanadi. Bu materiallar ma'lumotlar bazasidan qat'i nazar ishlatilishi mumkin.

Ma'lumotlar bazasiga bo'lgan mualliflik huquqi boshqa shaxslarning ushbu ma'lumotlar bazasiga kirgan materiallar va asarlarni mustaqil ravishda tanlashi va tashkil etishiga mo'nelik qilmaydi.

Huquq egasi o'z huquqlaridan xabardor qilish maqsadida EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining birinchi bor bosib chiqarilishidan e'tiboran mualliflik huquqining uch qismdan: doira yoki kichik qavs ichiga olingan «S» harfi; huquq egasining nomi (ismi); EHM uchun yaratilgan dastur yoki ma'lumotlar bazasi birinchi bor bosib chiqarilgan yil ko'rsatilgan yozuvdan tarkib topgan himoya belgisini qo'llashi mumkin.

EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalariga bo'lgan mualliflik huquqi ularning moddiy ashyosiga nisbatan mulk egaligi huquqi bilan

aloqador emas. Moddiy ashyoga nisbatan bo'lgan huquqlarni o'zgalarga har qanday tarzda berish EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalariga bo'lgan mualliflik huquqlaridan birortasining o'zgalarga o'tib qolishiga sabab bo'lmaydi.

5-modda. Mualliflik huquqining amal qilish muddatlari

EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalariga bo'lgan mualliflik huquqining amal qilish muddatlari qonun hujjatlarida ko'zda tutilgan mualliflik huquqi normalariga muvofiq belgilanadi.

6-modda. Mualliflik, shaxsiy va mulkiy huquqlar

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasiga mualliflik, shuningdek muallifning (mualliflarning) yoki o'zga huquq egasining shaxsiy va mulkiy huquqlari amaldagi qonun hujjatlariga muvofiq aniqlanadi. EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining muallifi (mualliflari) yoxud o'zga huquq egasi EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini modifikatsiyalashni, shu jumladan dasturni bir dasturlash tilidan boshqa tilga o'tkazishni amalga oshirish va (yoki) amalga oshirishga ruxsat etish borasida mutlaq huquqqa ham egadir.

7-modda. Mulkiy huquqlarni o'zgalarga o'tkazish

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasiga bo'lgan mulkiy huquqlar shartnoma bo'yicha o'zga jismoniy yoki yuridik shaxslarga to'liq yoki qisman o'tkazilishi mumkin. Shartnoma yozma shaklda tuziladi va unda albatta quyidagilar belgilab qo'yiladi: EHM uchun yaratilgan dastur yoki ma'lumotlar bazasidan foydalanish hajmi va usullari, haq to'lash tartibi va mukofot puli miqdori, shartnomaning amal qilish muddati.

EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazasiga bo'lgan mulkiy huquqlar qonunda belgilangan tartibda meros bo'lib o'tadi.

8-modda. Xizmat vazifalarini bajarish tartibida yaratilgan EHM uchun dastur yoki ma'lumotlar bazasiga bo'lgan mulkiy huquqlar

Xizmat vazifalarini bajarish tartibida yoki ish beruvchining topshirig'iga binoan yaratilgan EHM uchun dastur yoki ma'lumotlar bazasiga bo'lgan mulkiy

huquqlar ish beruvchiga, basharti u bilan muallif o'rtasidagi shartnomada o'zgacha qoida nazarda tutilmagan bo'lsa, tegishli bo'ladi.

Haq to'lash tartibi va mukofot puli miqdori muallif bilan ish beruvchi o'rtasidagi shartnomada belgilab qo'yiladi.

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasiga nisbatan mulkiy huquqlarga ega bo'lgan tashkilot yoki korxonalar (mulkchilik shaklidan qat'i nazar) qayta tashkil qilinsa, tarqatib yuborilsa yoki tugatilsa, barcha mulkiy huquqlar tegishli ravishda sudning yoki tugatish komissiyasining qaroriga ko'ra muallifga (mualliflarga), davlatga yoki boshqa huquqiy vorisga o'tkazilishi mumkin.

9-modda. EHM uchun yaratilgan dasturlar va ma'lumotlar bazalarini ro'yxatdan o'tkazish huquqi hamda ularni ro'yxatdan o'tkazish

EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalariga nisbatan barcha shaxsiy va mulkiy yoki shartnomaga ko'ra faqat mulkiy huquqlarga ega bo'lgan O'zbekiston Respublikasining, boshqa davlatlarning jismoniy yoki yuridik shaxslari dasturlar yoki ma'lumotlar bazalarini ro'yxatdan o'tkazish huquqiga egadirlar. Huquq egasi EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini bevosita yoki o'z vakili orqali Dasturiy mahsullar davlat reestri yoki Ma'lumotlar bazalari davlat reestrda (matnda bundan buyon Reestr deb yuritiladi) O'zbekiston Respublikasi Davlat patent idorasiga (bundan buyon matnda Patent idorasi deb yuritiladi) talabnoma berish orqali ro'yxatdan o'tkazadi.

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini rasmiy ro'yxatdan o'tkazish so'ralgan talabnoma (matnda bundan buyon ro'yxatdan o'tkazish talabnomasi deb yuritiladi) EHM uchun yaratilgan bitta dastur yoki bitta ma'lumotlar bazasiga taalluqli bo'lishi kerak. Ro'yxatdan o'tkazish talabnomasini rasmiylashtirish qoidalarini Patent idorasi belgilaydi.

Ro'yxatdan o'tkazish talabnomasi kelib tushgach, Agentlik kerakli hujjatlarning bor-yo'qligi va qoidalarning talablariga qanchalik muvofiqligini tekshirib chiqadi. Tekshirish natijasi ijobiy bo'lsa, Patent idorasi EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini tegishli Reestrga kiritadi, talabnoma beruvchiga rasmiy ro'yxatdan o'tkazilganlik to'g'risida guvohnoma topshiradi

hamda ro'yxatdan o'tkazilgan EHM uchun yaratilgan dasturlar va ma'lumotlar bazalariga doir ma'lumotlarni Patent idorasi rasmiy axborotnomasida e'lon qiladi.

Talabnoma beruvchi Patent idorasi so'roviga ko'ra yoki o'z tashabbusi bilan ma'lumotlar rasmiy axborotnomada bosib chiqarilguniga qadar talabnoma materiallarini to'ldirish, ularga aniqlik kiritish va ularni tuzatishga haqlidir. Tekshirish natijasi salbiy bo'lsa, Patent idorasi talabnoma beruvchiga rasmiy ro'yxatdan o'tkazish rad etilganligini bildiruvchi hujjat topshiradi.

Rasmiy ro'yxatdan o'tkazish tartibini, rasmiy ro'yxatdan o'tkazilganlik to'g'risidagi guvohnoma shakllarini, ularda ko'rsatiladigan ma'lumotlar tarkibini Patent idorasi belgilaydi. Rasmiy axborotnomada e'lon qilinadigan ma'lumotlar ro'yxati ham Patent idorasi tomonidan belgilanadi.

Ro'yxatdan o'tkazilgan EHM uchun yaratilgan dastur yoki ma'lumotlar bazasiga bo'lgan barcha mulkiy huquqlar butunlay o'zgalarga berilishi to'g'risidagi shartnoma Patent idorasida ro'yxatdan o'tkazilishi lozim. EHM uchun yaratilgan dastur yoki ma'lumotlar bazasiga bo'lgan mulkiy huquqlarning o'zgalarga o'tkazilishi to'g'risidagi shartnomalar tomonlarning kelishuviga binoan Patent idorasida ro'yxatdan o'tkazilishi mumkin.

Reestrda kiritilgan ma'lumotlar toki aksi isbotlanmagunga qadar to'g'ri deb hisoblanadi. Ko'rsatilgan ma'lumotlarning to'g'riligi uchun talabnoma beruvchi javobgar bo'ladi.

EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalarini ro'yxatga olish hamda EHM uchun yaratilgan dasturlar va ma'lumotlar bazalaridan foydalanishga bo'lgan mulkiy huquqlarni boshqa shaxsga o'tkazish to'g'risidagi shartnomalarni ro'yxatga olish bilan bog'liq yuridik ahamiyatga ega harakatlarni bajarganlik uchun patent bojlari undiriladi. Patent bojlari Patent idorasiga to'lanadi. Patent bojlarining miqdori va ularni to'lash muddatlari, ularni to'lashdan ozod qilish, to'lovlarning miqdorini kamaytirish yoki ularni qaytarib berish asoslari, shuningdek patent bojlaridan foydalanish tartibi O'zbekiston Respublikasi Vazirlar Mahkamasi tomonidan belgilanadi.

(9-moddaning sakkizinchi qismi 2002 yil 30 avgustdagi 405-II-son Qonuni tahririda — Oliy Majlis Axborotnomasi, 2002 y., 9-son, 165-modda)

(9-modda O‘zbekiston Respublikasining 2002 yil 5 apreldagi 364-II-son qonuni tahririda — Oliy Majlis Axborotnomasi, 2002 y., 4-5-son, 74-modda)

10-modda. EHM uchun yaratilgan dastur yoki ma’lumotlar bazasini boshqa davlatlarda ro‘yxatdan o‘tkazish

O‘zbekiston Respublikasining yuridik va jismoniy shaxslari EHM uchun yaratilgan dasturlar yoki ma’lumotlar bazalarini boshqa davlatlarda ro‘yxatdan o‘tkazishga yoki ularni xalqaro miqyosda ro‘yxatdan o‘tkazishga haqlidirlar.

EHM uchun yaratilgan dastur yoki ma’lumotlar bazasini O‘zbekiston Respublikasining yuridik va jismoniy shaxslari tomonidan boshqa davlatlarda ro‘yxatdan o‘tkazish Patent idorasiga talabnoma topshirilganidan keyin amalga oshiriladi.

11-modda. EHM uchun yaratilgan dastur yoki ma’lumotlar bazasidan huquq egasi bilan tuzilgan shartnoma asosida foydalanish

EHM uchun yaratilgan dastur yoki ma’lumotlar bazasidan boshqa shaxslarning (foydalanuvchilarning) foydalanishi huquq egasi bilan tuzilgan shartnoma asosida amalga oshiriladi, ushbu Qonunning 13-moddasida ko‘rsatilgan hollar bundan mustasno.

EHM uchun yaratilgan dasturlar yoki ma’lumotlar bazalari sotilganda yohud ommaviy foydalanuvchilar uchun berib qo‘yilganda shartnomalar tuzishning alohida tartibi qo‘llanishi, xususan EHM uchun yaratilgan dasturlar yoki ma’lumotlar bazalarining berilayotgan nusxalarida shartnomaning tipik talablari bayon etib qo‘yilishi mumkin.

12-modda. EHM uchun yaratilgan dasturlar yoki ma’lumotlar bazalaridan erkin nusxa olish va ularning adaptatsiyasi

EHM uchun yaratilgan dastur yoki ma’lumotlar bazasining nusxasiga qonunan ega bo‘lgan shaxs huquq egasidan qo‘shimcha ravishda ruxsat olmagan holda EHM uchun yaratilgan dastur yoki ma’lumotlar bazasi o‘z vazifasiga monand ishlashi bilan bog‘liq har qanday harakatlarni amalga oshirishga, shu

jumladan EHMga yozib qo'yish va uning xotirasida saqlashga, shuningdek aniq ko'rinib turgan xatolarni tuzatishga haqlidir. EHMga yozib qo'yish va uning xotirasida saqlashga, bosharti, huquq egasi bilan tuzilgan shartnomada o'zgacha qoida nazarda tutilmagan bo'lsa, bitta EHM yoki shoxobchadagi bitta foydalanuvchiga nisbatan yo'l qo'yiladi.

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining nusxasiga qonunan ega bo'lgan shaxs huquq egasining roziligini olmay va unga qo'shimcha haq to'lamay turib (bosharti, shartnomada o'zgacha qoida nazarda tutilmagan bo'lsa), quyidagi harakatlarni amalga oshirishga haqlidir: EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini adaptatsiyalashga; EHM uchun yaratilgan dastur yoki ma'lumotlar bazasi nusxasini, ushbu ko'chirma nusxa arxiv maqsadlarigagina mo'ljallangan taqdirda va qonuniy tarzda olingan nusxani almashtirish uchun kerak bo'lib qolgan (EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining asl nusxasi yo'qolib qolgan, yo'q qilingan yoki yaroqsiz holga kelgan) taqdirda o'zlari tayyorlashga yoki tayyorlash uchun topshiriq berishga. Bunda EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining ko'chirma nusxasidan yuqorida aytib o'tilgan maqsadlardan bo'lak maqsadlarda foydalanilishi mumkin emas va EHM uchun yaratilgan ushbu dasturdan yoki ma'lumotlar bazasidan bundan buyon foydalanish qonuniy bo'lmay qolsa, ular yo'q qilinishi lozim.

EHM uchun yaratilgan dastur nusxasiga haqli ravishda egalik qilayotgan shaxs mazkur dasturning kodlanishi va tuzilishini o'rganish maqsadlarida uni muallifning yoki o'zga huquq egasining yozma roziligi bo'lgan taqdirda yoki quyidagi hollarda bunday rozilik bo'lmasa ham dekompilyatsiya qilishi mumkin, agar:

dekompilyatsiya qilish natijasida olingan hamda mazkur shaxs tomonidan ishlab chiqilgan dasturning EHM uchun yaratilgan boshqa dasturlar bilan o'zaro hamkor ishlashi uchun zarur axborotni boshqa manbalardan olish mumkin bo'lmasa;

EHM uchun yaratilgan dasturning faqat bunday hamkor ishlashini yo'lga qo'yish uchun zarur bo'lgan qismlarining o'zi dekompiyatsiya qilinayotgan bo'lsa;

dekompiyatsiya natijasida olingan axborotdan ifodasiga ko'ra EHM uchun yaratilgan, dekompiyatsiya qilinayotgan dasturga juda o'xshash bo'lgan EHM dasturi ishlab chiqish, ishlab chiqarish yoki tarqatish uchun foydalanilmasa yoxud bunday axborot mualliflik huquqini buzadigan boshqa har qanday harakatni amalga oshirish uchun ishlatilmasa.

(12-moddaning uchinchi qismi O'zbekiston Respublikasining 2002 yil 5 apreldagi 364-II-son qonuni tahririda — Oliy Majlis Axborotnomasi, 2002 y., 4-5-son, 74-modda)

13-modda. EHM uchun yaratilgan dastur yoki ma'lumotlar bazasi nusxasini erkin olib sotish

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasi nusxasiga bo'lgan egalik huquqi yoki o'zga mulkiy huquqlar ushbu nusxaga egalik huquqi birinchi marotaba sotilganidan keyin yoki boshqacha tarzda o'zgaga o'tkazilganidan keyin, huquq egasining roziligini olmay va unga qo'shimcha haq to'lamagan holda olib sotilishiga yoki boshqacha usulda o'zgalarga o'tkazilishiga yo'l qo'yiladi.

14-modda. Mualliflik huquqini muhofaza qilish

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasining muallifi va o'zga huquq egalari:

huquqlari tan olinishini;

huquq buzilishiga qadar mavjud bo'lgan holat tiklanishini va huquqni buzayotgan yoki uning buzilishi xavfini tug'dirayotgan hatti-harakatlar to'xtatilishini;

yetkazilgan zarar uning miqdoriga huquqbuzar tomonidan g'ayriqonuniy olingan daromad summasini qo'shgan holda qoplanishini;

foyda ko'rgan huquqbuzardan yetkazilgan zarar qoplanishi o'rniga eng kam oylik ish haqining tegishli sud qarori bilan belgilanadigan yigirma barobaridan ming barobarigacha bo'lgan miqdorida tovon to'lanishini;

ularning huquqlari muhofaza qilinishi bilan bog'liq qonunlarda nazarda tutilgan o'zga choralar ko'rilishini talab qilishga haqlidir.

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasi muallifi va o'zga huquq egalari o'z huquqlari muhofaza qilinishini so'rab tegishli sudga murojaat etishlari mumkin.

Sud EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalarining mualliflik huquqi buzilgan holda tayyorlangan nusxalarini musodara etish va ularni yo'q qilib yuborish to'g'risida qaror chiqarishi mumkin. EHM uchun yaratilgan dastur yoki ma'lumotlar bazasidan bunday nusxalar olishda foydalaniladigan materiallar va uskunalar sudning qarori bilan byudjet daromadiga o'tkazilishi yohud da'vogarning iltimosiga binoan zararlarni qoplash hisobiga berilishi mumkin.

15-modda. Mualliflik huquqining buzilishi

Huquq egalariining mutlaq huquqlariga taalluqli ushbu Qonun talablarining jismoniy yoki yuridik shaxs tomonidan bajarilmasligi mualliflik huquqining buzilishi hisoblanadi.

EHM uchun yaratilgan dastur yoki ma'lumotlar bazasini o'zganing nomi bilan chiqarish yohud undan g'ayriqonuniy ravishda nusxa olish yoki bunday asarlarni tarqatish qonun hujjatlarida belgilangan tartibda ma'muriy yohud jinoiy javobgarlikka sabab bo'ladi.

Tayyorlanishi yoki ulardan foydalanilishi mualliflik huquqi buzilishiga olib keladigan EHM uchun yaratilgan dasturlar yoki ma'lumotlar bazalarining nusxalari qonun hujjatlarida belgilangan tartibda olib qo'yilishi lozim.

16-modda. Chet ellik yuridik va jismoniy shaxslarning huquqlari

Chet ellik yuridik va jismoniy shaxslar ushbu qonunda nazarda tutilgan huquqlardan O'zbekiston Respublikasining yuridik va jismoniy shaxslari bilan teng ravishda yoki o'zarolik printsipi asosida foydalanadilar.

O'zbekiston Respublikasining Prezidenti

I. Karimov

Toshkent sh.,
1994 yil 6 may

O‘ZBEKISTON RESPUBLIKASINING QONUNI
AXBOROT ERKINLIGI PRINTSIPLARI VA KAFOLATLARI
TO‘G‘RISIDA

(O‘zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2003 y., 1-son, 2-
modda)

1-modda. Ushbu qonunning asosiy vazifalari

Ushbu qonunning asosiy vazifalari axborot erkinligi printsiplari va kafolatlariga rioya etilishini, har kimning axborotni erkin va moneliksiz izlash, olish, tekshirish, tarqatish, foydalanish va saqlash huquqlari ro‘yobga chiqarilishini, shuningdek axborotning muhofaza qilinishini hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta‘minlashdan iborat.

2-modda. Axborot erkinligi printsiplari va kafolatlari to‘g‘risidagi qonun hujjatlari

Axborot erkinligi printsiplari va kafolatlari to‘g‘risidagi qonun hujjatlari ushbu qonun va boshqa qonun hujjatlaridan iboratdir.

Agar O‘zbekiston Respublikasining xalqaro shartnomasida O‘zbekiston Respublikasining axborot erkinligi printsiplari va kafolatlari to‘g‘risidagi qonun hujjatlarida nazarda tutilganidan boshqacha qoidalar belgilangan bo‘lsa, xalqaro shartnoma qoidalari qo‘llaniladi.

3-modda. Asosiy tushunchalar

Ushbu qonunda quyidagi asosiy tushunchalar qo‘llaniladi:

axborot — manbalari va taqdim etilish shaklidan qat’i nazar shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to‘g‘risidagi ma’lumotlar;

axborot mulkdori — o‘z mablag‘iga yoki boshqa qonuniy yo‘l bilan olingan axborotga egalik qiluvchi, undan foydalanuvchi va uni tasarruf etuvchi yuridik yoki jismoniy shaxs;

axborotni muhofaza etish — axborot borasidagi xavfsizlikka tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish chora-tadbirlari;

axborot resurslari — alohida hujjatlar, hujjatlarning alohida to‘plamlari, axborot tizimlaridagi (kutubxonalardagi, arxivlardagi, fondlardagi, ma’lumotlar banklaridagi va boshqa axborot tizimlaridagi) hujjatlar va hujjatlarning to‘plamlari;

axborot sohasi — sub’ektlarning axborotni yaratish, qayta ishlash va undan foydalanish bilan bog‘liq faoliyati sohasi;

axborot borasidagi xavfsizlik — axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holati;

axborot egasi — qonunda yoki axborot mulkdori tomonidan belgilangan huquqlar doirasida axborotga egalik qiluvchi, undan foydalanuvchi va uni tasarruf etuvchi yuridik yoki jismoniy shaxs;

maxfiy axborot — foydalanilishi qonun hujjatlariga muvofiq cheklab qo‘yiladigan hujjatlashtirilgan axborot;

ommaviy axborot — cheklanmagan doiradagi shaxslar uchun mo‘ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar;

hujjatlashtirilgan axborot — identifikatsiya qilish imkonini beruvchi rekvizitlari qo‘yilgan holda moddiy jismda qayd etilgan axborot.

4-modda. Axborot erkinligi

O‘zbekiston Respublikasining Konstitutsiyasiga muvofiq har kim axborotni moneliksiz izlash, olish, tekshirish, tarqatish, undan foydalanish va uni saqlash huquqiga ega.

Axborot olish faqat qonunga muvofiq hamda inson huquq va erkinliklari, konstitutsiyaviy tuzum asoslari, jamiyatning axloqiy qadriyatlari, mamlakatning ma’naviy, madaniy va ilmiy salohiyatini muhofaza qilish, xavfsizligini ta’minlash maqsadida cheklanishi mumkin.

5-modda. Axborot erkinligining asosiy printsiplari

Ochiqlik va oshkoralik, hamma erkin foydalanishi mumkinligi va haqqoniylik axborot erkinligining asosiy printsiplaridir.

6-modda. Axborotning ochiqligi va oshkoraligi

Axborot ochiq va oshkora bo‘lishi kerak, maxfiy axborot bundan mustasno.

Maxfiy axborotga quyidagilar kirmaydi:

fuqarolarning huquq va erkinliklari, ularni ro'yobga chiqarish tartibi to'g'risidagi, shuningdek davlat hokimiyati va boshqaruv organlari, fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlarining huquqiy maqomini belgilovchi qonun hujjatlari;

ekologik, meteorologik, demografik, sanitariya-epidemiologik, favqulodda vaziyatlar to'g'risidagi ma'lumotlar hamda aholining, aholi punktlarining, ishlab chiqarish ob'ektlari va kommunikatsiyalarning xavfsizligini ta'minlash uchun zarur bo'lgan boshqa axborotlar;

kutubxonalarning, arxivlarning va O'zbekiston Respublikasi hududida faoliyat ko'rsatayotgan yuridik shaxslarga tegishli axborot tizimlarining ochiq fondlaridagi mavjud ma'lumotlar.

Davlat hokimiyati va boshqaruv organlari, fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlari jamiyat manfaatlariga taalluqli voqealar, faktlar, hodisalar va jarayonlar to'g'risida qonun hujjatlarida belgilangan tartibda ommaviy axborot vositalariga xabar berishi shart.

7-modda. Axborotdan hamma erkin foydalanishi mumkinligi va uning haqqoniyligi

Axborot undan hamma erkin foydalanishi mumkinligi ta'minlangan va haqqoniy bo'lishi kerak.

Axborotni buzib talqin etish va soxtalashtirish taqiqlanadi.

Ommaviy axborot vositalari o'zlari tarqatayotgan axborotning haqqoniyligi uchun axborot manbai va muallifi bilan birgalikda qonunda belgilangan tartibda javobgar bo'ladilar.

Axborot mulkdori, egasining axborot berishni rad etganligi ustidan sudga shikoyat qilinishi mumkin.

8-modda. Axborot erkinligi kafolatlari

Davlat har kimning axborotni izlash, olish, tekshirish, tarqatish, undan foydalanish va uni saqlash huquqini himoya qiladi. Jinsi, irqi, millati, tili, dini,

ijtimoiy kelib chiqishi, e'tiqodi, shaxsiy va ijtimoiy mavqeiga qarab axborot olish huquqi cheklanishiga yo'l qo'yilmaydi.

Davlat hokimiyati va boshqaruv organlari, fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlari hamda mansabdor shaxslar qonun hujjatlarida belgilangan tartibda har kimga o'zining huquqlari, erkinliklari va qonuniy manfaatlariga daxldor bo'lgan axborot bilan tanishib chiqish imkoniyatini ta'minlab berishga, maqbul axborot resurslari yaratishga, foydalanuvchilarni fuqarolarning huquqlari, erkinliklari va majburiyatlariga, ularning xavfsizligiga doir hamda jamiyat manfaatlariga taalluqli boshqa masalalar yuzasidan axborot bilan ommaviy tarzda ta'minlashga majburdirlar.

O'zbekiston Respublikasida senzuraga va axborotni monopollashtirishga yo'l qo'yilmaydi.

9-modda. Axborot olish tartibi

Har kim axborot olish uchun bevosita yoki vakillari orqali yozma yoxud og'zaki so'rov bilan murojaat etish huquqiga ega.

Yozma so'rovda murojaat etuvchining ismi, otasining ismi, familiyasi, manzili (yuridik shaxslarning esa rekvizitlari) hamda so'ralayotgan axborotning nomi yoki xususiyati ko'rsatilishi lozim. So'rovlar belgilangan tartibda ro'yxatdan o'tkazilishi kerak.

Yozma so'rovga imkon qadar qisqa muddatda, agar qonun hujjatlarida boshqacha qoida nazarda tutilgan bo'lmasa, so'rov olingan sanadan e'tiboran o'ttiz kundan kechiktirmay javob qaytarilishi lozim.

Og'zaki so'rovga, imkoniyatga qarab, darhol javob berilishi kerak.

So'ralayotgan axborotni ushbu moddaning uchinchi va to'rtinchi qismlarida nazarda tutilgan muddatda taqdim etishning iloji bo'lmagan taqdirda axborot olish uchun murojaat etgan shaxsga uni taqdim etish kechiktirilganligi to'g'risida xabar yuboriladi.

So'ralayotgan axborotni taqdim etishni kechiktirish so'rov berilgan sanadan e'tiboran ikki oydan ortib ketmasligi lozim. Taqdim etish kechiktirilganligi

to'g'risidagi xabar axborot so'rab murojaat etgan shaxsga so'rov olingan sanadan e'tiboran bir hafta muddat ichida yuboriladi.

Taqdim etish kechiktirilganligi to'g'risidagi xabarda quyidagilar ko'rsatilishi kerak:

so'ralayotgan axborotni vaqtida taqdim eta olmaslik sabablari;

so'ralayotgan axborot taqdim etiladigan sana.

Agar so'rov tushgan organ yoki mansabdor shaxs so'ralayotgan axborotga ega bo'lmasa, axborot so'rab murojaat etgan shaxsga so'rov olingan sanadan e'tiboran besh kundan kechiktirmay bu haqda ma'lum qilishi shart.

Axborot berganlik uchun belgilangan tartibda haq olinishi mumkin.

10-modda. Axborot berishni rad etish

Agar so'ralayotgan axborot maxfiy bo'lsa yoki uni oshkor etish natijasida shaxsning huquqlari va qonuniy manfaatlariga, jamiyat va davlat manfaatlariga zarar etishi mumkin bo'lsa, axborotni berish rad etilishi mumkin.

So'ralayotgan axborotni berish rad etilganligi to'g'risidagi xabar so'rov bilan murojaat etgan shaxsga so'rov olingan sanadan e'tiboran besh kunlik muddat ichida yuboriladi.

Rad etish to'g'risidagi xabarda so'ralayotgan axborotni berish mumkin emasligi sababi ko'rsatilishi kerak.

Maxfiy axborot mulkdori, egasi axborotni so'ralayotgan shaxslarni bu axborotni olishning amaldagi cheklavlari to'g'risida xabardor etishi shart.

Axborot berilishi qonunga xilof ravishda rad etilgan shaxslar, shuningdek o'z so'roviga haqqoniy bo'lmagan axborot olgan shaxslar o'zlariga yetkazilgan moddiy zararining o'rnini qonunda belgilangan tartibda qoplanishi yoki ma'naviy ziyon kompensatsiya qilinishi huquqiga ega.

11-modda. Axborotni muhofaza etish

Har qanday axborot, agar u bilan qonunga xilof ravishda muomalada bo'lish axborot mulkdori, egasi, axborotdan foydalanuvchi va boshqa shaxsga zarar yetkazishi mumkin bo'lsa, muhofaza etilmog'i kerak.

Axborotni muhofaza etish:

- shaxs, jamiyat va davlatning axborot sohasidagi xavfsizligiga tahdidlarning oldini olish;
- axborotning maxfiyligini ta'minlash, tarqalishi, o'g'irlanishi, yo'qotilishining oldini olish;
- axborotning buzib talqin etilishi va soxtalashtirilishining oldini olish maqsadida amalga oshiriladi.

12-modda. Axborot xavfsizligini ta'minlash sohasidagi davlat siyosati

Axborot xavfsizligini ta'minlash sohasidagi davlat siyosati axborot sohasidagi ijtimoiy munosabatlarni tartibga solishga qaratilgan bo'ladi hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta'minlash sohasida davlat hokimiyati va boshqaruv organlarining asosiy vazifalari hamda faoliyat yo'nalishlarini, shuningdek fuqarolarning o'zini o'zi boshqarish organlari, jamoat birlashmalari va boshqa nodavlat notijorat tashkilotlarining, fuqarolarning o'rni va ahamiyatini belgilaydi.

13-modda. Shaxsning axborot borasidagi xavfsizligi

Shaxsning axborot borasidagi xavfsizligi uning axborotdan erkin foydalanishi zarur sharoitlari va kafolatlarini yaratish, shaxsiy hayotiga taalluqli sirlarini saqlash, axborot vositasida qonunga xilof ravishda ruhiy ta'sir ko'rsatilishidan himoya qilish yo'li bilan ta'minlanadi.

Jismoniy shaxslarga taalluqli shaxsiy ma'lumotlar maxfiy axborot toifasiga kiradi.

Jismoniy shaxsning rozilgisiz uning shaxsiy hayotiga taalluqli axborotni, xuddi shuningdek shaxsiy hayotiga taalluqli sirini, yozishmalar, telefondagi so'zlashuvlar, pochta, telegraf va boshqa muloqot sirlarini buzuvchi axborotni to'plashga, saqlashga, qayta ishlashga, tarqatishga va undan foydalanishga yo'l qo'yilmaydi, qonun hujjatlarida belgilangan hollar bundan mustasno.

Jismoniy shaxslar to'g'risidagi axborotdan ularga moddiy zarar va ma'naviy ziyon yetkazish, shuningdek ularning huquqlari, erkinliklari va qonuniy manfaatlari ro'yobga chiqarilishiga to'sqinlik qilish maqsadida foydalanish taqiqlanadi.

Fuqarolar to'g'risida axborot oluvchi, bunday axborotga egalik qiluvchi hamda undan foydalanuvchi yuridik va jismoniy shaxslar bu axborotdan foydalanish tartibini buzganlik uchun qonunda nazarda tutilgan tarzda javobgar bo'ladilar.

Ommaviy axborot vositalari axborot manbaini yoki taxallusini qo'ygan muallifni ularning rozilgisiz oshkor etishga haqli emas. Axborot manbai yoki muallif nomi faqat sud qarori bilan oshkor etilishi mumkin.

14-modda. Jamiyatning axborot borasidagi xavfsizligi

Jamiyatning axborot borasidagi xavfsizligiga quyidagi yo'llar bilan erishiladi: demokratik fuqarolik jamiyati asoslari rivojlantirilishini, ommaviy axborot erkinligini ta'minlash;

qonunga xilof ravishda ijtimoiy ongga axborot vositasida ruhiy ta'sir ko'rsatishga, uni chalg'itishga yo'l qo'ymaslik;

jamiyatning ma'naviy, madaniy va tarixiy boyliklarini, mamlakatning ilmiy va ilmiy-texnikaviy salohiyatini asrash hamda rivojlantirish;

milliy o'zlikni anglashni izdan chiqarishga, jamiyatni tarixiy va milliy an'analar hamda urf-odatlardan uzoqlashtirishga, ijtimoiy-siyosiy vaziyatni beqarorlashtirishga, millatlararo va konfessiyalararo totuvlikni buzishga qaratilgan axborot ekspansiyasiga qarshi harakat tizimini barpo etish.

15-modda. Davlatning axborot borasidagi xavfsizligi

Davlatning axborot borasidagi xavfsizligi quyidagi yo'llar bilan ta'minlanadi: axborot sohasidagi xavfsizlikka tahdidlarga qarshi harakatlar yuzasidan iqtisodiy, siyosiy, tashkiliy va boshqa tUSDagi chora-tadbirlarni amalga oshirish;

davlat sirlarini saqlash va davlat axborot resurslarini ulardan ruxsatsiz tarzda foydalanilishidan muhofaza qilish;

O'zbekiston Respublikasining jahon axborot makoniga va zamonaviy telekommunikatsiyalar tizimlariga integratsiyalashuvi;

O'zbekiston Respublikasining konstitutsiyaviy tuzumini zo'rlik bilan o'zgartirishga, hududiy yaxlitligini, suverenitetini buzishga, hokimiyatni bosib olishga yoki qonuniy ravishda saylab qo'yilgan yoxud tayinlangan hokimiyat

vakillarini hokimiyatdan chetlatishga va davlat tuzumiga qarshi boshqacha tajovuz qilishga ochiqdan-ochiq da'vat etishni o'z ichiga olgan axborot tarqatilishidan himoya qilish;

urushni va zo'ravonlikni, shafqatsizlikni targ'ib qilishni, ijtimoiy, milliy, irqiy va diniy adovat uyg'otishga qaratilgan terrorizm va diniy ekstremizm g'oyalarini yoyishni o'z ichiga olgan axborot tarqatilishiga qarshi harakatlar qilish.

16-modda. Axborot erkinligi printsiplari va kafolatlari to'g'risidagi qonun hujjatlarini buzganlik uchun javobgarlik

Axborot erkinligi printsiplari va kafolatlari to'g'risidagi qonun hujjatlarini buzganlikda aybdor shaxslar belgilangan tartibda javobgar bo'ladilar.

O'zbekiston Respublikasining Prezidenti

I. KARIMOV

Toshkent sh.,
2002 yil 12 dekabr

O‘ZBEKISTON RESPUBLIKASINING QONUNI

AXBOROTLASHTIRISH TO‘G‘RISIDA

(O‘zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2004 y., 1-2-son, 10-
modda)

1-modda. Ushbu Qonunning maqsadi

Ushbu Qonunning maqsadi axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solishdan iborat.

2-modda. Axborotlashtirish to‘g‘risidagi qonun hujjatlari

Axborotlashtirish to‘g‘risidagi qonun hujjatlari ushbu Qonun va boshqa qonun hujjatlaridan iboratdir.

Agar O‘zbekiston Respublikasining xalqaro shartnomasida O‘zbekiston Respublikasining axborotlashtirish to‘g‘risidagi qonun hujjatlarida nazarda tutilganidan boshqacha qoidalar belgilangan bo‘lsa, xalqaro shartnoma qoidalari qo‘llaniladi.

3-modda. Asosiy tushunchalar

Ushbu Qonunda quyidagi asosiy tushunchalar qo‘llaniladi:

axborotlashtirish — yuridik va jismoniy shaxslarning axborotga bo‘lgan ehtiyojlarini qondirish uchun axborot resurslari, axborot texnologiyalari hamda axborot tizimlaridan foydalangan holda sharoit yaratishning tashkiliy ijtimoiy-iqtisodiy va ilmiy-texnikaviy jarayoni;

axborot resursi — axborot tizimi tarkibidagi elektron shakldagi axborot, ma’lumotlar banki, ma’lumotlar bazasi;

axborot resurslarining yoki axborot tizimlarining mulkdori — axborot resurslariga yoki axborot tizimlariga egalik qiluvchi, ulardan foydalanuvchi va ularni tasarruf etuvchi yuridik yoki jismoniy shaxs;

axborot resurslarining yoki axborot tizimlarining egasi — qonun bilan yoki axborot resurslarining, axborot tizimlarining mulkdori tomonidan belgilangan

huquqlar doirasida axborot resurslariga yoxud axborot tizimlariga egalik qiluvchi, ulardan foydalanuvchi va ularni tasarruf etuvchi yuridik yoki jismoniy shaxs;

axborot texnologiyasi — axborotni to‘plash, saqlash, izlash, unga ishlov berish va uni tarqatish uchun foydalaniladigan jami uslublar, qurilmalar, usullar va jarayonlar;

axborot tizimi — axborotni to‘plash, saqlash, izlash, unga ishlov berish hamda undan foydalanish imkonini beradigan, tashkiliy jihatdan tartibga solingan jami axborot resurslari, axborot texnologiyalari va aloqa vositalari.

4-modda. Axborotlashtirish sohasidagi davlat siyosati

Axborotlashtirish sohasidagi davlat siyosati axborot resurslari, axborot texnologiyalari va axborot tizimlarini rivojlantirish hamda takomillashtirishning zamonaviy jahon tamoyillarini hisobga olgan holda milliy axborot tizimini yaratishga qaratilgan.

Axborotlashtirish sohasidagi davlat siyosatining asosiy yo‘nalishlari quyidagilardan iborat:

har kimning axborotni erkin olish va tarqatishga doir konstitutsiyaviy huquqlarini amalga oshirish, axborot resurslaridan erkin foydalanilishini ta‘minlash;

davlat organlarining axborot tizimlari, tarmoq va hududiy axborot tizimlari, shuningdek yuridik hamda jismoniy shaxslarning axborot tizimlari asosida O‘zbekiston Respublikasining yagona axborot makonini yaratish;

xalqaro axborot tarmoqlari va Internet jahon axborot tarmog‘idan erkin foydalanish uchun sharoit yaratish;

davlat axborot resurslarini shakllantirish, axborot tizimlarini yaratish hamda rivojlantirish, ularning bir-biriga mosligini va o‘zaro aloqada ishlashini ta‘minlash;

axborot texnologiyalarining zamonaviy vositalari ishlab chiqarilishini tashkil etish;

axborot resurslari, xizmatlari va axborot texnologiyalari bozorini shakllantirishga ko‘maklashish;

dasturiy mahsulotlar ishlab chiqarish rivojlantirilishini rag‘batlantirish;

tadbirkorlikni qo‘llab-quvvatlash va rag‘batlantirish, investitsiyalarni jalb etish uchun qulay sharoit yaratish;

kadrlar tayyorlash va ularning malakasini oshirish, ilmiy tadqiqotlarni rag‘batlantirish.

5-modda. Axborotlashtirish sohasini davlat tomonidan tartibga solish

Axborotlashtirish sohasini davlat tomonidan tartibga solishni O‘zbekiston Respublikasi Vazirlar Mahkamasi va u maxsus vakolat bergan organ amalga oshiradi.

6-modda. Maxsus vakolatli organ

Maxsus vakolatli organ:

davlat axborot resurslarini shakllantirish ishlarini tashkil etadi va muvofiqlashtiradi;

axborotlashtirish va axborot texnologiyalarini rivojlantirish davlat dasturlarini ishlab chiqadi;

davlat organlarining axborot tizimlari, tarmoq va hududiy axborot tizimlari yaratilishiga ko‘maklashadi;

axborotlashtirish sohasidagi standartlar, normalar va qoidalarni ishlab chiqadi;

axborot tizimlari va axborot texnologiyalarining texnika vositalari hamda xizmatlarini sertifikatlashtirish ishlarini tashkil etadi;

yuridik va jismoniy shaxslarning o‘z axborot resurslari hamda axborot tizimlari muhofaza etilishini ta‘minlash borasidagi faoliyatini muvofiqlashtiradi;

axborot resurslari, xizmatlari va axborot texnologiyalari bozorini rivojlantirishga ko‘maklashadi;

axborotlashtirish sohasida marketing tadqiqotlari va monitoringni tashkil etadi;

axborot resurslaridan foydalanuvchilarning huquqlari va qonuniy manfaatlarini himoya qilish choralarini amalga oshiradi;

O‘zbekiston Respublikasining mudofaa qobiliyati va xavfsizligi manfaatlarini ko‘zlab axborot xavfsizligini hamda axborot tizimlaridan ustuvor foydalanilishini ta’minlaydi;

qonun hujjatlariga muvofiq boshqa vakolatlarni amalga oshiradi.

7-modda. Axborot resurslari va axborot tizimlarining huquqiy rejimi

Axborot resurslari va axborot tizimlarining huquqiy rejimi quyidagilarni belgilovchi normalar bilan aniqlanadi:

axborotni hujjatlashtirish, axborot resurslarini shakllantirish va axborot tizimlarini yaratish tartibini;

axborot resurslariga va axborot tizimlariga bo‘lgan mulk huquqini;

axborot resurslarining ulardan erkin foydalanish darajasi bo‘yicha toifasini;

axborot resurslari va axborot tizimlarini muhofaza qilish tartibini;

axborot tizimlarining tarmoqlararo ulanishi tartibini.

8-modda. Axborotni hujjatlashtirish

Axborotni hujjatlashtirish axborotni axborot resurslariga kiritishning majburiy shartidir. Axborotni hujjatlashtirish tartibi maxsus vakolatli organ tomonidan belgilanadi.

Axborot resurslarida saqlanadigan va ishlov beriladigan, elektron raqamli imzo bilan tasdiqlangan axborot elektron hujjat bo‘lib, qog‘oz hujjat bilan bir xil yuridik kuchga ega.

Elektron hujjatni va elektron raqamli imzoni shakllantirish hamda ulardan foydalanish bilan bog‘liq munosabatlar qonun bilan tartibga solinadi.

9-modda. Axborot resurslari va axborot tizimlariga bo‘lgan mulk huquqi

O‘zbekiston Respublikasida axborot resurslari va axborot tizimlari ommaviy hamda xususiy mulk bo‘lishi mumkin.

Axborot resurslari va axborot tizimlariga bo‘lgan mulk huquqining vujudga kelishiga quyidagilar asos bo‘ladi:

axborot resurslari hamda axborot tizimlarining davlat byudjeti mablag‘lari, yuridik va jismoniy shaxslarning o‘z mablag‘lari yoki qonun hujjatlari bilan taqiqlanmagan boshqa manbalar hisobidan yaratilishi;

axborot resurslari va axborot tizimlariga bo'lgan mulk huquqining o'zga shaxsga o'tishi shartlarini o'z ichiga olgan oldi-sotdi shartnomasi yoki boshqa bitim;

meros olish.

Qonunda axborot resurslari va axborot tizimlariga bo'lgan mulk huquqi vujudga kelishining boshqa asoslari ham nazarda tutilishi mumkin.

10-modda. Davlat axborot resurslari

Davlat axborot resurslari quyidagilardan shakllantiriladi:

davlat organlarining axborot resurslaridan;

yuridik va jismoniy shaxslarning davlat byudjeti mablag'lari hisobidan yaratilgan axborot resurslaridan;

yuridik va jismoniy shaxslarning davlat sirlari hamda maxfiy axborotni o'z ichiga olgan axborot resurslaridan;

yuridik va jismoniy shaxslarning belgilangan tartibda taqdim etiladigan hujjatlashtirilgan axborotidan.

Yuridik va jismoniy shaxslar hujjatlashtirilgan axborotni davlat axborot resurslarini shakllantirish uchun tegishli davlat organlariga belgilangan tartibda taqdim etishi shart.

Yuridik va jismoniy shaxslarning hujjatlashtirilgan axborotni majburiy taqdim etishi tartibi, davlat axborot resurslarini shakllantirish hamda ulardan foydalanish uchun mas'ul davlat organlarining ro'yxati O'zbekiston Respublikasi Vazirlar Mahkamasi tomonidan belgilanadi.

Davlat sirlari va maxfiy axborot jumlasiga kiritilgan axborotni taqdim etish tartibi qonun hujjatlari bilan belgilanadi.

11-modda. Axborot resurslaridan erkin foydalanish toifalari

Axborot resurslari ulardan erkin foydalanish toifalari bo'yicha hamma erkin foydalanishi mumkin bo'lgan axborot resurslariga va erkin foydalanilishi cheklab qo'yilgan axborot resurslariga bo'linadi.

Cheklanmagan doiradagi foydalanuvchilar uchun mo'ljallangan axborot resurslari hamma erkin foydalanishi mumkin bo'lgan axborot resurslaridir.

Davlat sirlari to'g'risidagi axborotni va maxfiy axborotni yoki erkin foydalanilishi axborot resurslarining mulkdorlari tomonidan cheklab qo'yilgan axborotni o'z ichiga olgan axborot resurslari erkin foydalanilishi cheklab qo'yilgan axborot resurslariga kiradi.

Axborot resurslarining mulkdorlari va egalari hamma erkin foydalanishi mumkin bo'lgan axborot resurslaridan yuridik hamda jismoniy shaxslarning teng huquq asosida erkin tarzda foydalanishini ta'minlashi kerak.

Axborot resurslarini erkin foydalanish toifalariga kiritish qonun hujjatlarida belgilangan tartibda axborot resurslarining mulkdori tomonidan aniqlanadi.

12-modda. Axborot resurslaridan foydalanish

Axborot resurslaridan foydalanuvchilar axborot resurslaridan erkin foydalanishda teng huquqlarga ega, erkin foydalanilishi cheklab qo'yilgan axborot resurslari bundan mustasno.

Axborot resurslaridan foydalanganlik uchun belgilangan tartibda haq olinishi mumkin.

Axborot bilan ta'minlashga doir axborot va xizmatlar ro'yxatlarini, axborot resurslaridan erkin foydalanish tartibi hamda shartlari haqidagi ma'lumotlarni axborot resurslarining mulkdorlari va egalari foydalanuvchilarga bepul taqdim etadi.

Yuridik va jismoniy shaxslar qonuniy asoslarda axborot resurslaridan o'zlari olgan axborotdan axborot manbaini albatta havola etgan holda hosila axborot yaratish uchun foydalanishlari mumkin.

Axborot resurslaridan axborot olish tartibini axborot resurslarining mulkdori yoki egasi qonun hujjatlarida belgilangan talablarga rioya etgan holda aniqlaydi.

13-modda. Jismoniy shaxslarning shaxsiga taalluqli ma'lumotlar to'g'risidagi axborotni o'z ichiga olgan axborot resurslari

Jismoniy shaxslarning shaxsiga taalluqli ma'lumotlar to'g'risidagi axborotni o'z ichiga olgan axborot resurslarini shakllantirish va ulardan foydalanish tartibi qonun hujjatlari bilan belgilanadi.

Jismoniy shaxslarning shaxsiga taalluqli ma'lumotlar to'g'risidagi axborot maxfiy axborot toifasiga kiradi.

14-modda. O'zlari to'g'risidagi ma'lumotlarni ichiga olgan axborot resurslaridan yuridik va jismoniy shaxslarning erkin foydalanishi

Yuridik va jismoniy shaxslar o'zlari to'g'risidagi ma'lumotlarni ichiga olgan axborot resurslaridan erkin foydalanish, mazkur ma'lumotlarning to'liqligi hamda to'g'riligini ta'minlash maqsadida ularga aniqliklar kiritish huquqiga ega.

O'zlari to'g'risidagi ma'lumotlarni ichiga olgan axborot resurslaridan yuridik va jismoniy shaxslarning erkin foydalanishi qonun bilan cheklanishi mumkin.

Yuridik va jismoniy shaxslarga o'zlari to'g'risidagi ma'lumotlarni ichiga olgan axborot resurslaridan erkin foydalanishni axborot resurslarining mulkdori yoki egasi rad etganligi ustidan sudga shikoyat qilinishi mumkin.

15-modda. Milliy axborot tizimi

Milliy axborot tizimiga davlat organlarining axborot tizimlari, tarmoq va hududiy axborot tizimlari, shuningdek yuridik hamda jismoniy shaxslarning axborot tizimlari kiradi.

Milliy axborot tizimi davlat byudjeti mablag'lari, shuningdek yuridik va jismoniy shaxslarning o'z mablag'lari hamda qonun hujjatlarida taqiqlanmagan boshqa manbalar hisobidan yaratiladi.

Milliy axborot tizimi uning tarkibiga kiruvchi axborot tizimlarining xalqaro axborot tizimlari bilan bir-biriga mosligini hisobga olgan holda yaratiladi.

Milliy axborot tizimidan foydalangan holda axborot almashish shartnoma asosida amalga oshiriladi, qonun hujjatlarida nazarda tutilgan hollar bundan mustasno.

16-modda. Axborot tizimlaridan bitimlar tuzishda foydalanish

Yuridik va jismoniy shaxslar o'rtasida bitimlar tuzishda axborot tizimlaridan foydalanish qonun hujjatlari bilan tartibga solinadi.

17-modda. Axborot tizimlarining texnika vositalarini sertifikatlashtirish

Axborot tizimlarini tashkil qiluvchi texnika vositalari qonun hujjatlarida belgilangan tartibda sertifikatlashtirilishi kerak.

Davlat organlari axborot tizimlarining, tarmoq va hududiy axborot tizimlarining, yuridik hamda jismoniy shaxslar axborot tizimlarining davlat sirlari yoki maxfiy axborotni o'z ichiga olgan axborotni ishlovdan o'tkazish uchun mo'ljallangan texnika vositalari, shuningdek mazkur tizimlarni muhofaza qilish vositalari majburiy sertifikatlashtirilishi lozim.

18-modda. Axborot tizimlarining tarmoqlararo bog'lanishi

Axborot tizimlarining tarmoqlararo bog'lanishi turli axborot tizimlari o'rtasida axborot almashish uchun amalga oshiriladi.

Belgilangan normalar va qoidalarga muvofiq o'zaro tarmoqlararo bog'lanish imkoniyatini axborot tizimlarining mulkdorlari, egalari ta'minlaydi.

Turli axborot tizimlarining tarmoqlararo bog'lanishi axborot tizimlarining mulkdorlari, egalari o'rtasidagi shartnoma asosida amalga oshiriladi.

Tarmoqlararo bog'lanishni amalga oshirish hamda turli axborot tizimlarining o'zaro aloqada bo'lish tartibi va shartlari maxsus vakolatli organ tomonidan belgilanadi.

19-modda. Axborot resurslari va axborot tizimlarini muhofaza qilish

Axborot resurslari va axborot tizimlarini muhofaza qilish quyidagi maqsadlarda amalga oshiriladi:

shaxs, jamiyat va davlatning axborot xavfsizligini ta'minlash;

axborot resurslarining tarqalib ketishi, o'g'irlanishi, yo'qotilishi, buzib talqin etilishi, to'sib qo'yilishi, qalbakilashtirilishi va ulardan boshqacha tarzda ruxsatsiz erkin foydalanilishining oldini olish;

axborotni yo'q qilish, to'sib qo'yish, undan nusxa olish, uni buzib talqin etishga doir ruxsatsiz harakatlarning hamda axborot resurslari va axborot tizimlariga boshqa shakldagi aralashishlarning oldini olish;

axborot resurslaridagi mavjud davlat sirlari va maxfiy axborotni saqlash.

20-modda. Axborot resurslari va axborot tizimlari muhofaza qilinishini tashkil etish

Axborot resurslari va axborot tizimlari, agar ular bilan g'ayriqonuniy munosabatda bo'lish natijasida axborot resurslarining yoki axborot tizimlarining

mulkdorlariga, egalariga yoxud boshqa yuridik hamda jismoniy shaxslarga zarar yetkazilishi mumkin bo'lsa, muhofaza qilinishi kerak.

Davlat organlari, yuridik va jismoniy shaxslar davlat sirlari hamda maxfiy sirlar to'g'risidagi axborotni o'z ichiga olgan axborot resurslari va axborot tizimlarining muhofaza qilinishini ta'minlashi shart.

Axborot resurslari va axborot tizimlari muhofaza qilinishini tashkil etish tartibi ularning mulkdorlari, egalari tomonidan mustaqil belgilanadi.

Davlat sirlari hamda maxfiy sirlar to'g'risidagi axborotni o'z ichiga olgan axborot resurslari va axborot tizimlarining muhofaza qilinishini tashkil etish tartibi O'zbekiston Respublikasi Vazirlar Mahkamasi tomonidan belgilanadi.

21-modda. Xalqaro axborot tarmoqlariga ulanish

Davlat organlari, yuridik va jismoniy shaxslar o'z axborot tizimlarini xalqaro axborot tarmoqlariga hamda Internet jahon axborot tarmog'iga qonun hujjatlarida belgilangan tartibda ulashi mumkin.

Erkin foydalanilishi cheklab qo'yilgan axborot resurslarini o'z ichiga olgan axborot tizimlarining xalqaro axborot tarmoqlariga hamda Internet jahon axborot tarmog'iga ulanishi faqat zarur muhofaza choralari ko'rilganidan keyin amalga oshiriladi.

22-modda. Nizolarni hal etish

Axborotlashtirish sohasidagi nizolar qonun hujjatlarida belgilangan tartibda hal etiladi.

23-modda. Axborotlashtirish to'g'risidagi qonun hujjatlarini buzganlik uchun javobgarlik

Axborotlashtirish to'g'risidagi qonun hujjatlarini buzganlikda aybdor shaxslar belgilangan tartibda javobgar bo'ladilar.

O'zbekiston Respublikasining Prezidenti

I. KARIMOV

Toshkent sh.,
2003 yil 11 dekabr

MUNDARIJA

KIRISH.....	4
1. Axborot texnologiyalari sohasidagi jinoyatlarning jinoiy-huquqiy tavsifi.....	7
2. Axborotlashtirish qoidalarini buzish (JK 278 ¹ -moddasi).....	22
3. Kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish (JK 278 ² -moddasi).....	26
4. Kompyuter tizimidan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o'tkazish maqsadini ko'zlab tayyorlash yoxud o'tkazish va tarqatish (JK 278 ³ -moddasi).....	33
5. Kompyuter axborotini modifikatsiyalashtirish (JK 278 ⁴ -moddasi).....	38
6. Kompyuter sabotaji (JK 278 ⁵ -moddasi).....	41
7. Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish (JK 278 ⁶ -moddasi).....	45
8. Kompyuter texnologiyalari sohasidagi jinoyatlarning oldini olish.....	51
XULOSA.....	65
ILOVA.....	73