***O.H.YIGITALIYEV*[1]**

AXBOROT XAVFSIZLIGIGA OID XALQARO HUQUQIY HUJJATLAR VA ULARNING TAHLILI

Axborot xavfsizligi *(Information Security)* tashkilotlarga raqamli huquq va analog huquqlarni, axborotni himoya qilish imkonini beradi. Xalqaro tashkilotlarning axborot xavfsizligi siyosati qisqacha *"InfoSec"* [286] [287] deb nomlanadi va kriptografiya, mobil hisoblash, ijtimoiy media, shuningdek, xususiy, moliyaviy va korporativ ma'lumotlarni o'z ichiga olgan infratuzilma va tarmoqlarni qamrab oladi. Boshqa tomondan, kiberxavfsizlik ma'lumotlarni himoya qiladi, lekin faqat internetga asoslangan tahdidlardangina himoya qiladi. Tashkilotlar turli sabablarga ko'ra axborot xavfsizligini amalga oshiradilar. Axborot xavfsizligining asosiy maqsadlari odatda, kompaniya ma'lumotlarining maxfiyligi, yaxlitligi va mavjudligini ta'minlash bilan bog'liq hisoblanadi. Bu soha ko'plab sohalarni qamrab olganligi sababli, u ko'pincha dastur xavfsizligi, infratuzilma xavfsizligi, kriptografiya, hodisalarga javob berish, zaifliklarni boshqarish va ofatlarni tiklash kabi turli xil xavfsizlik choralarini amalga oshirishni o'z ichiga oladi. Axborot xavfsizligi siyosati quyidagi umumiy xavflarining oldini olish uchun tashkilotlarda axborot xavfsizligi siyosati amalga oshiriladi: ijtimoiy muhandislik hujumlari, kengaytirilgan doimiy tahdidlar *(APT),* ichki tahdidlar, tashqi taxdidlar, cryptojackinglar, to'lov dasturlari, man-in-the-middle *(MitM)* hujumlari, bank operatsiyalariga hurujlar, shaxsiy ma'lumotlarni og'irlash va boshqalar [288].

Xalqaro tashkilotlarda axborot xavfsizligi chora-tadbirlari quyidagi tashkiliy jarayonlar orqali amalga oshiriladi: xavfsizlik hodisalari va hodisalarni boshqarish *(SIEM),* ma'lumotlar yo'qolishining oldini olish *(DLP),* intrusionlarni aniqlash tizimi *(IPS),* foydalanuvchi xatti-harakatlari tahlili *(UBA),* blokcheyn kiber xavfsizligi, yakuniy nuqtani aniqlash va javob berish *(EDR),* xavfsizlik holatini boshqarish *(CSPM)* va boshqalar. Axborot xavfsizligini ta'minlash infratuzilma va tarmoq

---

[286] Toshkent davlat yuridik universiteti "Ommaviy axborot vositalari huquqi" yo'nalishi magistranti

[287] McCullagh K. Protecting "privacy" through control of "personal" data processing: A flawed approach. International Review of Law, Computers & Technology. 2009. V. 23. N 1-2

1 Hunter J. An Information Security Handbook. London: Springer Verlag London Limited; 2001

2 Understanding Cybersecurity Law and Digital Privacy A Common Law Perspective 226

xavfsizligi, audit va kibertestni o‘z ichiga olgan bir qator IT domenlarini qamrab oladi. Bunda, ruxsatsiz foydalanuvchilarning shaxsiy ma'lumotlarga kirishini cheklash uchun autentifikatsiya va ruxsatlar kabi vositalardan foydalanadi. Ushbu chora-tadbirlar ma'lumotni o‘g‘irlash, o‘zgartirish yoki yo‘qotish bilan bog‘liq zararlarning oldini olishga yordam beradi. Tashkilotlarda axborot xavfsizligi maqsadlari axborot xavfsizligi bilan himoyalangan uchta asosiy maqsad mavjud, ular birgalikda *CIA* deb nomlanadi [1]. Demak, axborotning maxfiyligi bu - ma'lumotlar mazmunining maxfiyligini himoya qilish uchun ruxsatsiz foydalanuvchilarning ma'lumotlarga kirishini oldini oladi. Tashkilotlarda ma’lumotlar maxfiyligi kirish cheklovlari orqali saqlanadi. Maxfiylikning buzilishi inson xatosi, qasddan almashish yoki zararli kirish tufayli sodir bo‘lishi mumkin. Ma’lumotlar butunligi esa - ma'lumotlarning haqiqiyligi va to‘g‘riligini ta'minlaydi. Butunlik ma'lumotni tahrirlash yoki o‘zgartirish imkoniyatini cheklash orqali ta'minlanadi. Butunlikni yo‘qotish analog ma'lumotlar atrof-muhit sharoitlaridan himoyalanmagan, raqamli ma'lumotlar to‘g‘ri uzatilmagan yoki foydalanuvchilar tasdiqlanmagan o‘zgarishlarni amalga oshirganda sodir bo‘lishi mumkin. Axborotning mavjudligini ta’minlash - avtorizatsiya qilingan foydalanuvchilarning ma'lumotlarga ishonchli kirishini ta'minlaydi. Mavjudlik kirish tartib-qoidalarining uzluksizligi, ma'lumotlarni zaxiralash yoki takrorlash, apparat va tarmoq ulanishlarini saqlash orqali ta'minlanadi. Mavjudlikni yo‘qotish tabiiy ofatlar tufayli tarmoqlarga hujum qilinganda yoki mijoz qurilmalari ishlamay qolganda sodir bo‘lishi mumkin.

Axborot xavfsizligini xalqaro huquqiy jihatdan tahlil etishdan ko‘zlangan maqsad esa, global va mintaqaviy darajada xalqaro axborot xavfsizligi kontsepsiyasini ko‘rib chiqish va uni amalga oshirishning huquqiy vositalarini tahlil qilish, global axborot jamiyatida munosabatlarni tartibga solish muammolarini tahlil qilish hisoblanadi [2]. Bunda biz mantiqiy, qiyosiy-huquqiy, rasmiy-huquqiy, tizimli-tuzilmaviy va muammoli-nazariy usullar orqali tadqiq etamiz. Bugungacha olib borilgan ilmiy tadqiqot ishlari shuni ko‘rsatadiki, tadqiqotlar natijasida global va mintaqaviy miqyosda xalqaro axborot xavfsizligini ta'minlashning yagona konsepsiyasi ishlab chiqish kerakligini, uni global miqyosda amalga oshirish uchun xalqaro huquqiy hujjatlarga ehtiyoj borligi aniqlandi. Jahon miqyosida xalqaro shartnomalar va hujjatlar loyihasini ishlab chiqish va qabul qilishda Yevropa Kengashining kiberjinoyatchilik va shaxsiy hayotni himoya qilish tajribasidan

foydalanish kerak [1]. Xalqaro tashkilotlar faoliyatida ularning axborot xavfsizligi qonunchiligini birlashtirish va uyg‘unlashtirish funksiyalarini amalga oshirish hamda milliy telekommunikatsiya operatorlari tomonidan xalqaro va tashqi bozorlarga chiqish jarayonida o‘zaro hamkorlik qilish mumkin. Jadal tarzda o‘sib borayotgan texnologik taraqqiyot zamonaviy dunyoda tub o‘zgarishlarga olib keldi. Xalqaro munosabatlarda davlatlar o‘rtasidagi aloqa tizimi o‘zgardi. Axborot- kommunikatsiya texnologiyalarining *(AKT)* rivojlanishi jamiyat hayotining barcha sohalariga, jumladan, iqtisodiyot, siyosat, ijtimoiy muammolar va madaniyatga ta'sir ko‘rsatib, ularni axborot jamiyatini barpo etish doirasida birlashtirdi [2].

Hozirgi vaqtda axborotlashgan jamiyat va axborot xavfsizligi kontseptsiyasi bir qator xalqaro hujjatlarda o‘z ifodasini topgan bo‘lib, ular orasida “Axborot jamiyatini qurish: Yangi ming yillikda global muammo” deb nomlangan Prinsiplar deklaratsiyasida (keyingi o‘rinlarda 2003-yil Deklaratsiyasi deb yuritiladi) va 2003-yil 12-dekabrdagi “Axborot jamiyati bo‘yicha Butunjahon sammitining harakat rejasi”ni aytib o‘tishimiz mumkin. Axborot jamiyati global axborot jamiyatiga nisbatan umumiyroq tushuncha hisoblanadi. U bir davlat ichida yoki mintaqaviy yoki global darajada tashkil etilishi mumkin. Global miqyosda u global axborot jamiyati deb nomlanadi. 2003-yilda qabul qilingan “Axborot jamiyatini qurish: Yangi ming yillikda global muammo” deb nomlangan prinsiplar deklaratsiyasida *"kiberxavfsizlik" atamasi* faqat kiberjinoyatlardan himoya qilishdan ko‘ra kengroq ma'noga ega degan fikr berib o‘tilgan. Xususan, deklaratsiyada qayd etilishicha, sammit ishtirokchilari Birlashgan Millatlar Tashkilotining axborot komunikatsiya texnologiyalaridan xalqaro barqarorlik va xavfsizlikni saqlash maqsadlariga zid bo‘lgan hamda davlatlar ichidagi infratuzilma yaxlitligiga salbiy ta’sir ko‘rsatishi mumkin bo‘lgan maqsadlarda potentsial foydalanishning oldini olish bo‘yicha faoliyatini qo‘llab-quvvatlaydi va xalqaro hamkorlikni amalga oshiradi. Ushbu qoidalar xalqaro axborot huquqining rivojlanayotgan tamoyilining amaldagi tamoyillar bilan, ya'ni fikr, so‘z va axborot erkinligini amalga oshirish, tinchlik va xalqaro xavfsizlikni mustahkamlashning muhim omili ekanligi tamoyili bilan bog‘liqligini anglatadi [1].

2000-yil avgust oyida Stenford universitetining bir guruh tadqiqotchilari tomonidan kiberjinoyat va terrorizmdan himoyalanishni kuchaytirish bo‘yicha xalqaro konvensiya loyihasini taqdim etdilar

(Stenford loyihasi) [289] [290]. Braun qurolli mojarolarda axborot tizimlaridan foydalanishni tartibga soluvchi konvensiya loyihasini ishlab chiqdi. 2009-yil 6-noyabrda Ma'lumotlarni himoya qilish va shaxsiy daxlsizlik bo'yicha komissarlarning xalqaro konferensiyasi "Maxfiylik va shaxsiy ma'lumotlar standartlari" rezolyutsiyasini qabul qildi. Buning uchun u global shartnoma loyihasini ishlab chiqish bo'yicha ishchi guruh tuzdi va uni ishlab chiqish me'zonlarini sanab o'tdi. Shartnomaning ishlab chiqilgan bo'limlarini BMT ga taqdim etish rejalashtirilgan. Shunday qilib, tadqiqotchilar va xalqaro forumlar aniq loyihalarni taklif qilmoqdalar, ammo BMT, Xalqaro elektraloqa ittifoqi *(XEI)* yoki YUNESKO doirasida bu sohada bugungi kunda tizimli ishlar olib borilmayapti. Shu bilan birga, xalqaro axborot xavfsizligining umumiy kontseptsiyasining mintaqaviy va global darajalarni qamrab oladigan monografik tadqiqotlari va uning huquqiy asoslarini rivojlantirish muammolari mavjud emas.

Axborot komunikatsiya texnologiyalarining rivojlanishi bilan yuzaga kelgan xalqaro xavfsizlik muammolarini hal etish maqsadida Birlashgan Millatlar Tashkiloti Bosh Assambleyasi 1998-yildan boshlab, o'zining har bir sessiyasida "Xalqaro xavfsizlik konteksida axborot va kommunikatsiyalar sohasidagi rivojlanish" rezolyutsiyalarini qabul qildi. Mazkur qarorlarning asosiy g'oyasi shundan iboratki, eng yangi axborot texnologiyalari va telekommunikatsiyalarini rivojlantirish va joriy etish borasida erishilayotgan salmoqli yutuqlar ijobiy bilan bir qatorda, salbiy oqibatlarni ham keltirib chiqardi. Shu bilan birga, ijobiy natijalar, ya'ni butun insoniyat uchun yangi imkoniyatlar paydo bo'lishi yaqqol ko'zga tashlanadi. Biroq, BMT Bosh Assambleyasi ushbu texnologiyalar va vositalar xalqaro barqarorlik va xavfsizlikni saqlash maqsadlariga zid bo'lgan maqsadlarda ishlatilishi mumkin bo'lgan yangi texnologiyalar va obyektlardan xavotirda ekanligini bildirdi va davlatlar infratuzilmasi yaxlitligiga salbiy ta'sir ko'rsatishi mumkinligini ta'kidlab o'tdi va fuqarolik va harbiy sohada ularning xavfsizligiga zarar etkazish ehtimolining katta ekanligiga alohida urg'u berib o'tdi. BMT Bosh Assambleyasi 2003-yil 23-dekabrda "Kiberxavfsizlikning global madaniyatini yaratish va muhim axborot tuzilmalarini himoya qilish to'g'risida"gi 58/199-sonli rezolyutsiyasini qabul qildi. Unda muhim axborot infratuzilmalarini himoya qilish elementlari, xususan, kiber

---

[289] Rowland D, Macdonald E. Information Technology Law. Abingdon: Cavendish Publishing Ltd; 2005

[290] Reed C, Angel J, editors. Computer Law: Law and Regulation of Information Technology. Oxford: Oxford University Press; 2007

zaifliklar, tahdidlar va hodisalar haqida favqulodda ogohlantirish tarmoqlariga ega bo‘lish, manfaatdor tomonlarning muhim axborot infratuzilmalarining tabiati va ko‘lamini hamda ularni himoya qilishda har birining o‘ynashi kerak bo‘lgan rolini tushunishlarini osonlashtirish uchun xabardorlikni oshirish, infratuzilmalarni o‘rganish va ular o‘rtasidagi o‘zaro bog‘liqlikni aniqlash, shu orqali bunday infratuzilmalarni himoya qilishni kuchaytirish va bunday infratuzilmalarga etkazilgan zarar yoki hujumlarning oldini olish, tekshirish va ularga javob berish maqsadida muhim infratuzilma ma'lumotlarini almashish va tahlil qilish uchun davlat va xususiy manfaatdor tomonlar o‘rtasida hamkorlikni rivojlantirish va hokazo. Eng muhim axborot tuzilmalarini himoya qilish elementlarining tabiati shundan iboratki, agar ular ko‘rsatilgan bo‘lsa, ular xalqaro shartnomaga kiritilishi mumkin [1]. Hozirgi vaqtda, BMT doirasida xalqaro axborot xavfsizligini ta'minlashning institutsional mexanizmi va tizimi yaratilgan. Davlatlar axborot xavfsizligi holatiga o‘z baholarini muntazam ravishda taqdim etadilar, ular esa Bosh kotibning ma'ruzalariga kiritiladi va xalqaro axborot xavfsizligi muammolari va ular bilan bog‘liq tushunchalarning mohiyatini yaxshiroq tushunishga yordam beradi. Bu axborot xavfsizligi bo‘yicha BMT ning ishlash mexanizmi hisoblanadi.

Yuqoridagi axborot xavfsizligini ta’minlashga oid xalqaro huquqiy hujjatlarga nazar soladigan bo‘lsak, axborot xavfsizligini ta’minlash nechog‘lik ustuvor ahamiyatga ega bo‘lgan masala ekanligiga guvoh bo‘lamiz. Shundan kelib chiqib ilg‘or horij tajribasining ayrim jihatlarini milliy qonunchilikka joriy qilish, bu sohaga oid ham huquqiy, ham amaliy-tashkiliy chora tadbirlarni ko‘rish, mavjud huquqiy asoslarni takomillashtirish, axborot telekomunikatsiya sohasida xalqaro hamkorlikni yo‘lga qo‘yish darkor. Bugun har bir davlat global axborot makonida o‘z xavfsizligini ta’minlashda ,avvalo ichki qonunchilik mexanizmini yaratishi, mavjud huquqiy bo‘shliq va kamchiliklarni esa

[1] Black SK. Telecommunications Law in the Internet Age. San Francisco: Morgan Kaufmann Publishers; 2002 228

xalqaro huquqiy normalarning tavsiyaviy harakterdagi hujjatlari va normalarini tahlil etgan holda to‘ldirib borishi maqsadga muvofiqdir.

Foydalanilgan adabiyotlar:

1. Неъматов, Жасур, and Бектурсун Муродкосимов. "Судлар фаолиятини рақамлаштириш–Ўзбекистоннинг халқаро рейтинглардаги ўрнини яхшилашга хизмат қилади." Актуальные вопросы и перспективы цифровизации судебно-правовой деятельности 1.01 (2022): 131-138.

А.Ф.АВАЗНИЯЗОВ[CCXCI]

ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ ИСПОЛНЕНИЯ

Согласно статье 44 закона Республики Узбекистан № 258-II «Об исполнении судебных актов и актов иных органов» от 29 августа 2001 г.:

«Меры принудительного исполнения применяются при предъявлении в установленном законом порядке надлежаще оформленного исполнительного документа и принятии государственным исполнителем постановления о возбуждении исполнительного производства за исключением случаев исполнения исполнительных документов в порядке упрощенного исполнительного производства».

Значит, порядок применения мер принудительного исполнения очень прост - это наличие исполнительного листа и принятия исполнителем данного листа, то есть возбуждения исполнительного производства. А основанием применения мер принудительного исполнения выступает истечение 15 дневного срока добровольного исполнения.

А видами мер принудительного исполнения являются следующие:

«Мерами принудительного исполнения являются:

1) обращение взыскания на денежные средства и иное имущество должника;

2) обращение взыскания на денежные средства и иное

[CCXCI] Магистрант Ташкентского государственного юридического университета