

KIBERXAVFSIZLIKNING HUQUQIY ASOSLARI VA XALQARO
STANDARTLAR

Mamadaliyev Javohir Tursunboy o‘g‘li

O‘ZBEKISTON RESPUBLIKASI IIV AKADEMIYASI KURSANTI

Iminov Abdurasul Abdulatipovich

IIV AKADEMIYASI KIBERXAVFSIZLIK KAFEDRASI BOSHLOG‘I

Kalit so‘zlar: kiberxavfsizlik, huquqiy asoslar, xalqaro standartlar, ISO, NIST, COBIT, axborot tizimlari, himoya, kiberhujumlar.

Annotatsiya: Ushbu maqolada kiberxavfsizlik sohasining huquqiy asoslari va xalqaro standartlari tahlil qilinadi. Maqolada avvalo kiberxavfsizlik tushunchasi, uning zamonaviy axborot texnologiyalari rivojida tutgan o‘rni va muhimligi yoritiladi. So‘ngra, mamlakatimiz va xalqaro miqyosda kiberxavfsizlikni tartibga soluvchi normativ-huquqiy hujjatlar, shuningdek, ISO, NIST, COBIT kabi xalqaro standartlar batafsil tahlil qilinadi. Maqolada kiberhujumlardan himoyalaniish, shaxsiy ma’lumotlarni saqlash, korporativ va davlat axborot tizimlarini himoya qilish bo‘yicha amaliy chora-tadbirlar, shuningdek, ular bilan bog‘liq huquqiy mas’uliyat tahlil qilinadi. Shuningdek, maqolada xalqaro hamkorlikning ahamiyati, kiberxavfsizlik bo‘yicha ekspertlar va davlatlar o‘rtasidagi tajriba almashinuvi, kiberhujumlarga qarshi kurashda umumiy standartlar va protokollarning roli ham ko‘rsatiladi. Maqola nafaqat kiberxavfsizlikni huquqiy nuqtai nazardan yoritadi, balki global standartlarga rioya qilish va ularni amaliyotga tadbiiq etish zarurligini ta’kidlaydi. Shu bilan birga, kiberxavfsizlikni mustahkamlashning samarali mexanizmlari, xavfsizlik siyosatini shakllantirish va uning qonuniy asoslarini kuchaytirish bo‘yicha tavsiyalar ham berilgan.

Ключевые слова: кибербезопасность, правовые основы, международные стандарты, ISO, NIST, COBIT, информационные системы, защита, кибератаки.

Аннотация: В статье проводится анализ правовых основ и международных стандартов кибербезопасности. Вначале раскрывается понятие кибербезопасности, подчеркивается её значение в развитии современных информационных технологий. Далее рассматриваются национальные и международные нормативно-правовые акты, а также ключевые международные стандарты, такие как ISO, NIST и COBIT. Исследование охватывает практические меры защиты от кибератак, обеспечение сохранности персональных данных, защиту корпоративных и государственных информационных систем, а также правовую ответственность, связанную с этими вопросами. Кроме того, статья акцентирует внимание на важности международного сотрудничества, обмене опытом между экспертами и странами, роли единых стандартов и протоколов в противодействии киберугрозам. Статья не только освещает вопросы кибербезопасности с юридической точки зрения, но и подчёркивает необходимость соблюдения глобальных стандартов и их внедрения на практике. Приводятся рекомендации по укреплению механизмов кибербезопасности, разработке политики безопасности и совершенствованию её правовых основ.

Keywords: cybersecurity, legal foundations, international standards, ISO, NIST, COBIT, information systems, protection, cyberattacks.

Annotation: *This article analyzes the legal foundations and international standards of cybersecurity. It begins by defining cybersecurity, highlighting its importance in the development of modern information technologies. The article further examines national and international regulatory frameworks, as well as key international standards such as ISO, NIST, and COBIT. The study addresses practical measures for protecting against cyberattacks, safeguarding personal data, and securing corporate and governmental information systems. It also considers the related legal responsibilities and liabilities. Additionally, the article emphasizes the significance of international cooperation, experience sharing among experts and countries, and the role of common standards and protocols in combating cyber threats. The article not only presents a legal perspective on cybersecurity but also underscores the necessity of adhering to global standards and implementing them in practice. Recommendations are provided for strengthening cybersecurity mechanisms, developing security policies, and enhancing their legal foundations.*

KIRISH

Hozirgi zamonda axborot texnologiyalari va raqamli tizimlar hayotimizning barcha sohalariga chuqur kirib bormoqda. Moliyaviy xizmatlar, sog'liqni saqlash, davlat boshqaruvi, ta'lim va tijorat kabi sohalarda internet va tarmoqlar orqali amalga oshiriladigan operatsiyalar soni ortib bormoqda. Shu bilan birga, kiberxavfsizlikning ahamiyati tobora ortib bormoqda, chunki har qanday raqamli tizimda xavfsizlikning yetarli darajada ta'minlanmasligi shaxsiy ma'lumotlar, korporativ sirlar va davlat sirlariga tahdid solishi mumkin. Kiberhujumlar nafaqat moddiy zarar keltiradi, balki obro' va ijtimoiy ishonchning pasayishiga, iqtisodiy jarayonlarning izdan chiqishiga ham sabab bo'lishi mumkin. Shu bois, kiberxavfsizlik sohasida qonuniy va normativ asoslarni shakllantirish hamda xalqaro standartlarga rioya qilish dolzarb vazifalardan biri sifatida namoyon bo'lmoqda. Kiberxavfsizlikning huquqiy asoslari – bu nafaqat kiberhujumlardan himoyalaniшни, balki shaxsiy ma'lumotlarni himoya qilish, korporativ va davlat axborot tizimlarini himoyalash, xakerlik faoliyatiga qarshi chora-tadbirlarni belgilovchi normativ-huquqiy hujjatlar majmuasidir. Shu nuqtai nazardan, mamlakatimizda qabul qilingan qonunlar, qarorlar va farmonlar kiberxavfsizlikni tartibga solishda muhim rol o'ynaydi. Masalan, shaxsiy ma'lumotlarni himoya qilish, elektron tijorat xavfsizligi, davlat axborot resurslarini himoya qilish bo'yicha normativ-huquqiy bazalar mavjud bo'lib, ular kiberxavfsizlik sohasidagi qonuniy mexanizmlarni shakllantiradi. Bundan tashqari, kiberxavfsizlikni ta'minlashda xalqaro standartlarning roli beqiyosdir. ISO/IEC 27001, NIST Cybersecurity Framework, COBIT va boshqa xalqaro standartlar raqamli tizimlarning xavfsizlik darajasini baholash, nazorat mexanizmlarini joriy etish va xavflarni aniqlash bo'yicha umumiy me'yorlar va tavsiyalarni beradi. Ushbu standartlar nafaqat texnik jihatlarni, balki boshqaruv, audit va jarayonlarni ham qamrab oladi. Shu sababli, kiberxavfsizlik bo'yicha xalqaro standartlarga rioya qilish korporativ va davlat tizimlarining ishonchliligini oshirish, kiberxavfsizlik

risklarini minimallashtirish, shuningdek, global hamkorlikni mustahkamlashga xizmat qiladi. Kiberxavfsizlikning huquqiy asoslari va xalqaro standartlar mavzusini o'rganishning yana bir muhim jihati – bu kiberhujumlarga qarshi kurashishning kompleksligi va ko'p qirrali yondashuvni talab qilishi. Kiberhujumlar doimo yangi shakl va uslublarda sodir etiladi, shuning uchun qonunchilik va standartlar doimo yangilanib borishi kerak. Shu bois, maqolada kiberxavfsizlik bo'yicha mavjud huquqiy bazalar va xalqaro standartlar tahlil qilinadi, ularning afzalliklari, kamchiliklari va zamonaviy talablar bilan uyg'unligi baholanadi. Shuningdek, kiberxavfsizlikni huquqiy nuqtai nazardan o'rganish jamiyatning barcha qatlamlariga ta'sir ko'rsatadi. Davlat organlari uchun bu normativ-huquqiy mexanizmlar ularning axborot tizimlarini himoya qilish va kiberhujumlarga qarshi strategiyalarni ishlab chiqish imkonini beradi. Korporativ sektorda esa bu yondashuv kompaniyalar faoliyatining barqarorligini ta'minlash, mijozlar ma'lumotlarini himoya qilish va moliyaviy xavflardan saqlanish imkonini yaratadi. Shu bilan birga, shaxsiy foydalanuvchilar va fuqarolar uchun ham kiberxavfsizlikning huquqiy asoslarini bilish va ularga amal qilish, shaxsiy ma'lumotlar xavfsizligini ta'minlash va raqamli muhitda xavfsiz faoliyat yuritish uchun muhimdir. Bugungi kunda global miqyosda kiberxavfsizlik masalalari xalqaro hamkorlik va tajriba almashinuvini talab qiladi. Davlatlar, nodavlat tashkilotlar va xalqaro kompaniyalar birgalikda kiberhujumlarga qarshi kurashish, xavfsizlik siyosatini shakllantirish va global standartlarni tatbiq etish bo'yicha faol ish olib bormoqdalar. Shu sababli, maqola nafaqat milliy qonunchilik va standartlarni, balki ularni xalqaro talablar bilan solishtirib, eng yaxshi amaliyotlarni aniqlashga ham qaratilgan. Mazkur tadqiqotning maqsadi – kiberxavfsizlikning huquqiy asoslarini tahlil qilish, xalqaro standartlar bilan solishtirish, ularning amaliy tatbiqini ko'rsatish va kiberxavfsizlik siyosatini rivojlantirish bo'yicha tavsiyalar ishlab chiqishdir. Tadqiqot jarayonida qonunchilik hujjatlari, xalqaro standartlar, ekspertlar fikrlari va ilg'or tajribalar o'rganilgan. Shu bilan birga, maqolada kiberxavfsizlikni samarali boshqarish mexanizmlari, xavflarni aniqlash va oldini olish choralari, shuningdek, xalqaro standartlarga mos keladigan monitoring va audit tizimlari ham yoritiladi. Natijada, ushbu maqola kiberxavfsizlikning huquqiy va normativ jihatlarini tizimli tarzda o'rganish, zamonaviy talablar bilan uyg'unligini baholash va amaliy tavsiyalar ishlab chiqish orqali mamlakatimiz va global miqyosda kiberxavfsizlikni mustahkamlashga xizmat qiladi.

ASOSIY QISM

Kiberxavfsizlik bugungi kunda har bir davlat, korporatsiya va shaxs uchun ustuvor vazifa sifatida qaraladi. Axborot tizimlari, internet platformalari va raqamli xizmatlarning kengayishi bilan birga kiberhujumlar soni ham oshib bormoqda. Shu sababli, kiberxavfsizlikni ta'minlashning huquqiy asoslari va xalqaro standartlarga rioya qilishning ahamiyati tobora oshmoqda.

Birinchidan, kiberxavfsizlikning huquqiy asoslari milliy va xalqaro huquqiy tizimlarda shakllanadi. Milliy darajada, ko'plab davlatlarda kiberxavfsizlikni tartibga soluvchi qonunlar qabul qilingan. Masalan, shaxsiy ma'lumotlarni himoya qilish, elektron tijorat xavfsizligi, davlat axborot tizimlarini himoya qilish, moliyaviy operatsiyalar xavfsizligi kabi yo'nalishlar bo'yicha normativ-huquqiy bazalar mavjud. Bu hujjatlar kiberxavfsizlik

siyosatini ishlab chiqishda, xavfsizlik mexanizmlarini tatbiq etishda va kiberhujumlarga qarshi chora-tadbirlarni belgilashda asos bo‘lib xizmat qiladi.

Shaxsiy ma’lumotlarni himoya qilish qonunlari, masalan, GDPR (Evropa Ittifoqi), Amerika Qo‘shma Shtatlaridagi CCPA va boshqa milliy qonunlar foydalanuvchilarning shaxsiy ma’lumotlarini himoya qilishni nazarda tutadi. Ular tashkilotlarni ma’lumotlarni yig‘ish, saqlash, qayta ishlash va uzatishda belgilangan talablarni bajarishga majbur qiladi. Shu bilan birga, bu qonunlar kiberhujumlardan kelib chiqadigan moliyaviy va huquqiy mas’uliyatni aniqlaydi va huquqbuzarliklarni tartibga soladi.

Ikkinchidan, xalqaro standartlar kiberxavfsizlikni ta’minlashda muhim vosita hisoblanadi. ISO/IEC 27001 standarti axborot xavfsizligi boshqaruv tizimini yaratish, xavf tahlilini amalga oshirish va xavfsizlik jarayonlarini nazorat qilish bo‘yicha umumiy me’yorlarni beradi. Shu bilan birga, NIST Cybersecurity Framework (AQSh Milliy Standartlar va Texnologiyalar Instituti tomonidan ishlab chiqilgan) xavflarni aniqlash, ularni baholash, nazorat qilish va ularni oldini olish bo‘yicha tizimli yondashuvni taklif qiladi. COBIT (Control Objectives for Information and Related Technologies) esa korporativ va davlat axborot tizimlarining boshqaruv va audit jarayonlarini yaxshilashga qaratilgan xalqaro standart sifatida ishlatiladi.

Uchinchi jihat – kiberhujumlarga qarshi amaliy choralar. Kiberxavfsizlik faqat qonunchilik va standartlar bilan cheklanib qolmaydi, balki texnik va tashkiliy choralarni ham o‘z ichiga oladi. Masalan, xavfsizlik devorlari (firewalls), kirish nazorati (access control), shifrlash (encryption), antivirus va antimalware dasturlari, tarmoqlarni monitoring qilish va kiberhujumlarni aniqlash tizimlari kiberxavfsizlikni ta’minlashning asosiy vositalari hisoblanadi. Shu bilan birga, tashkilotlarda xodimlarni kiberxavfsizlik bo‘yicha o‘qitish, ichki siyosat va tartiblarni belgilash ham muhim ahamiyatga ega.

To‘rtinchidan, xalqaro hamkorlik va standartlarga rioya qilish. Kiberxavfsizlikning samarali mexanizmi milliy chegaralardan oshib, global miqyosda hamkorlikni talab qiladi. Davlatlararo kelishuvlar, xalqaro tashkilotlar (masalan, INTERPOL, ITU, Europol) va xalqaro ekspertlar tarmoqlari kiberhujumlarga qarshi kurashish, tajriba almashish va birgalikda standartlar ishlab chiqish bo‘yicha faol ish olib boradi. Bu xalqaro standartlar va protokollar milliy qonunchilik bilan uyg‘unlashganda kiberxavfsizlikning samaradorligini oshiradi. Beshinchidan, huquqiy mas’uliyat va monitoring tizimi. Kiberxavfsizlik bo‘yicha qonunchilik va standartlar kiberhujumlardan himoyalaniшни belgilasa-da, ularning ijrosi nazorat qilinmasa, samaradorlik pasayadi. Shu sababli, davlat va korporativ tizimlarda monitoring, audit va nazorat mexanizmlari muhim ahamiyatga ega. Masalan, xavf tahlili natijalari bo‘yicha xodimlar va rahbarlar javobgarlikka tortilishi, ma’lumotlar buzilgan holatlarda ogohlantirish tizimlari va jarimalar belgilanishi kiberxavfsizlikni mustahkamlashga xizmat qiladi. Shuningdek, kiberxavfsizlikni ta’minlashda strategik yondashuv zarur. Bu yondashuv milliy xavfsizlik siyosati, iqtisodiy barqarorlik va ijtimoiy ishonchni mustahkamlashga xizmat qiladi. Masalan, davlat darajasida kiberxavfsizlik siyosati ishlab chiqish, xavfsizlik protokollarini joriy etish va ularni muntazam yangilab borish zarur. Korporativ darajada esa xavfsizlik siyosati, xodimlarni tayyorlash va texnik vositalarni muntazam yangilab borish talab qilinadi. Natijada, kiberxavfsizlikning huquqiy

asoslari va xalqaro standartlarga rioya qilish bir-biri bilan uzviy bog‘liq bo‘lib, zamonaviy axborot jamiyatida xavfsiz va barqaror faoliyat yuritish uchun zarur shart-sharoitlarni yaratadi. Shu bilan birga, global standartlar va normativ-huquqiy baza birgalikda ishlatilsa, ular kiberxavfsizlikni mustahkamlash, kiberhujumlarga qarshi kurashish va shaxsiy, korporativ hamda davlat ma’lumotlarini himoya qilishda samarali mexanizmlarga aylanadi. Ushbu asosiy qism kiberxavfsizlikning huquqiy va normativ jihatlarini chuqur tahlil qilib, xalqaro standartlar bilan uyg‘unligini ko‘rsatadi, shuningdek, kiberxavfsizlik siyosatini rivojlantirish va amaliy tavsiyalar ishlab chiqish bo‘yicha ilmiy asos yaratadi. Shu nuqtai nazardan, maqola kiberxavfsizlikning nafaqat texnik, balki huquqiy, tashkiliy va strategik jihatlarini ham qamrab olgan kompleks tahlil bo‘lib xizmat qiladi.

XULOSA

Kiberxavfsizlikning huquqiy asoslari va xalqaro standartlar zamonaviy axborot jamiyatida muhim ahamiyatga ega. Tadqiqot davomida aniqlanishicha, milliy va xalqaro qonunchilik hamda standartlar kiberxavfsizlikni ta’minlashda bir-birini to‘ldiruvchi asosiy vositalardir. Milliy qonunchilik kiberhujumlardan himoya qilish, shaxsiy va korporativ ma’lumotlarni saqlash, davlat axborot tizimlarini himoya qilish va moliyaviy operatsiyalar xavfsizligini ta’minlash bo‘yicha aniq talablar va mexanizmlarni belgilaydi. Shu bilan birga, xalqaro standartlar, jumladan ISO/IEC 27001, NIST Cybersecurity Framework va COBIT korporativ va davlat axborot tizimlarida xavfsizlikni boshqarish, xavflarni aniqlash va ularni oldini olish bo‘yicha tizimli yondashuvlarni taklif qiladi. Maqolada kiberhujumlarga qarshi amaliy choralar ham batafsil tahlil qilindi. Texnik va tashkiliy chora-tadbirlar, jumladan xavfsizlik devorlari, kirish nazorati, shifrlash vositalari, antivirus dasturlari, tarmoqlarni monitoring qilish tizimlari, shuningdek, xodimlarni kiberxavfsizlik bo‘yicha tayyorlash va ichki siyosatlarni joriy etish muhimligi ta’kidlandi. Bu choralar nafaqat huquqiy talablarga javob beradi, balki real xavflarni kamaytirish va tizimlarning ishonchliligini oshirishga xizmat qiladi. Shuningdek, kiberxavfsizlik sohasida xalqaro hamkorlik va standartlarga rioya qilish dolzarb ahamiyatga ega. Davlatlar, xalqaro tashkilotlar va ekspertlar tarmoqlari o‘rtasidagi tajriba almashinuvi, birgalikda standartlar va protokollar ishlab chiqish kiberhujumlarga qarshi samarali mexanizm yaratadi. Milliy qonunchilik va xalqaro standartlarning uyg‘un ishlashi kiberxavfsizlikni mustahkamlash, kiberhujumlardan kelib chiqadigan xavflarni kamaytirish va axborot tizimlarining barqarorligini ta’minlashga xizmat qiladi. Maqolada shuningdek, huquqiy mas’uliyat, monitoring va audit tizimlarining ahamiyati yoritildi. Kiberxavfsizlik bo‘yicha normativ-huquqiy mexanizmlarni tatbiq etish va ularning ijrosini nazorat qilish xavfsizlikning samaradorligini oshiradi, kiberhujumlarga qarshi chora-tadbirlarni mustahkamlashga yordam beradi. Shu bilan birga, strategik yondashuvning zarurligi ta’kidlandi. Davlat va korporativ darajada xavfsizlik siyosatini ishlab chiqish, protokollarni joriy etish va ularni muntazam yangilab borish kiberxavfsizlikning barqarorligini ta’minlash uchun muhim shartdir. Natijada, kiberxavfsizlikning huquqiy asoslari va xalqaro standartlar bir-birini to‘ldiruvchi, zamonaviy raqamli jamiyatda xavfsiz va barqaror faoliyat yuritish uchun asosiy vositalardir. Milliy qonunchilik kiberhujumlarga qarshi chora-tadbirlarni belgilasa, xalqaro standartlar tizimli yondashuvni, monitoringni va boshqaruvni ta’minlaydi. Shu bilan birga, texnik va

tashkiliy chora-tadbirlar, xodimlarni tayyorlash va xalqaro hamkorlikning uyg'unligi kiberxavfsizlikni yanada mustahkamlaydi. Kiberxavfsizlikni huquqiy va xalqaro standartlar doirasida rivojlantirish nafaqat texnik, balki strategik va tashkiliy jihatdan ham jamiyatning barcha qatlamlariga foyda keltiradi. Bu nafaqat davlat, balki korporativ sektor va shaxsiy foydalanuvchilar uchun ham xavfsiz raqamli muhitni ta'minlaydi. Shu nuqtai nazardan, maqola kiberxavfsizlikni huquqiy asoslar va xalqaro standartlar nuqtai nazaridan tizimli o'rganish, ularning amaliy tatbiqini tahlil qilish va tavsiyalar ishlab chiqish orqali ushbu sohaga ilmiy hissa qo'shadi. Xulosa qilib aytganda, milliy qonunchilik, xalqaro standartlar, texnik va tashkiliy chora-tadbirlar, monitoring va strategik yondashuvning uyg'un ishlashi kiberxavfsizlikni mustahkamlash, kiberhujumlarga qarshi kurashish va raqamli tizimlarda barqarorlikni ta'minlashning asosiy shartlaridan biridir. Shu sababli, mamlakatimiz va global miqyosda kiberxavfsizlik siyosatini takomillashtirish, normativ-huquqiy bazani mustahkamlash va xalqaro standartlarga moslash dolzarb vazifa sifatida qaraladi.

FOYDALANILGAN ADABIYOTLAR:

1. Shackelford, Scott J. "Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace." Cambridge University Press, 2014.
2. Kshetri, Nir. "The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns." Big Data & Society, 2014.
3. Whitman, Michael E., Mattord, Herbert J. "Principles of Information Security." 6th Edition. Cengage Learning, 2018.
4. Bada, A., Sasse, M.A. "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?" arXiv preprint arXiv:1505.02055, 2015.