KIBERXAVFSIZLIK AXBOROTINING HUQUQIY JIHATLARI

Fazlitdinov Azalshoh

Toshkent davlat yuridik universiteti,

Jinoiy odil sudlov fakulteti 1-bosqich talabasi.

azalshohfazlitdinov@gmail.com

ORCID: 0009-0009-0387-6132

https://doi.org/10.5281/zenodo.14105971

Annotatsiya. *Kiberxavfsizlik bugungi kunda zamonaviy jamiyatning ajralmas qismiga aylangan va axborot texnologiyalari bilan chambarchas bog'liq soha sifatida rivojlanmoqda.*

Internet va raqamli platformalarning global miqyosda keng tarqalishi bilan birga, bu texnologiyalarni himoya qilish, ma'lumotlarning xavfsizligini ta'minlash va shaxsiy huquqlarni muhofaza qilish masalalari jiddiy huquqiy, etik va texnik muammolarni keltirib chiqarmoqda.

Hozirgi kunda kiberjinoyatlarni soni oshib borishi hisobiga davlatlarda, korxonalarda va shaxsiy qurilmalarda kiberxavfsizlik tizimini rivojlantirishga e'tiborni jalb qilish o'rinlidir. Ushbu maqolada kiberxavfsizlik axborotining huquqiy jihatlari, shu jumladan shaxsiy ma'lumotlarning himoyasi, kiberjinoyatlar, intellektual mulk va xalqaro hamkorlik masalalari tahlil qilinadi.

Kiberxavfsizlikni ta'minlash uchun zarur bo'lgan normativ hujjatlar va qonunlar, shuningdek, ularning xalqaro miqyosda qanday tartibga solinishi va amalga oshirilishi muhokama qilinadi. Shuningdek, kiberxavfsizlikning huquqiy tizimdagi roli va uning samarali qo'llanilishi nafaqat davlatlar, balki global miqyosdagi tashkilotlar o'rtasidagi hamkorlikni talab etishini ko'rsatib o'tamiz. Maqola kiberxavfsizlikning huquqiy asoslarini kengaytirish va mustahkamlash uchun zarur bo'lgan strategiyalarni aniqlashga qaratilgan.

Kalit so'zlar: *kiberjinoyatlar, kiberxavfsizlik, raqamli platformalar, shaxsiy ma'lumotlar himoyasi, virus, kiber gigiyena, intellektual mulk.*

LEGAL ASPECTS OF CYBERSECURITY INFORMATION

Abstract. *Today, cyber security has become an integral part of modern society and is developing as a field closely related to information technologies. With the global spread of the Internet and digital platforms, the protection of these technologies, the security of information and the protection of individual rights pose serious legal, ethical and technical challenges. Currently, due to the increase in the number of cybercrimes, it is appropriate to draw attention to the development of the cyber security system in countries, enterprises and personal devices. This article analyzes the legal aspects of cybersecurity information, including the protection of personal data, cybercrimes, intellectual property, and international cooperation.*

Regulatory documents and laws necessary to ensure cyber security, as well as how they are regulated and implemented at the international level, are discussed. We will also show that the role of cyber security in the legal system and its effective use require cooperation not only between states, but also among organizations on a global scale. The article aims to identify the necessary strategies for expanding and strengthening the legal framework of cyber security.

Key words: *cyber crimes, cyber security, digital platforms, personal data protection, virus, cyber hygiene, intellectual property.*

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИИ О КИБЕРБЕЗОПАСНОСТИ

Аннотация. *Сегодня кибербезопасность стала неотъемлемой частью современного общества и развивается как область, тесно связанная с информационными технологиями. В условиях глобального распространения Интернета и цифровых платформ защита этих технологий, безопасность информации и защита прав личности создают серьезные юридические, этические и технические проблемы. В настоящее время в связи с ростом количества киберпреступлений уместно обратить внимание на развитие системы кибербезопасности в странах, на предприятиях и в персональных устройствах. В данной статье анализируются правовые аспекты информации о кибербезопасности, включая защиту персональных данных, киберпреступлений, интеллектуальной собственности и международного сотрудничества. Обсуждаются нормативные документы и законы, необходимые для обеспечения кибербезопасности, а также то, как они регулируются и реализуются на международном уровне. Мы также покажем, что роль кибербезопасности в правовой системе и ее эффективное использование требуют сотрудничества не только между государствами, но и между организациями в глобальном масштабе. Целью статьи является определение необходимых стратегий расширения и укрепления правовой базы кибербезопасности.*

Ключевые слова: *киберпреступления, кибербезопасность, цифровые платформы, защита персональных данных, вирус, кибергигиена, интеллектуальная собственность.*

I. Kirish

Bugungi kunda kiberxavfsizlik axborot texnologiyalari rivojlanishi bilan tobora muhim ahamiyat kasb etmoqda. Internet va raqamli tizimlar hayotimizning barcha jabhalariga ta’sir ko’rsatib, yangi xavf-xatarlarni keltirib chiqarmoqda. Shu bilan birga, axborot xavfsizligini ta’minlash uchun huquqiy me’yorlar va tartiblar ham zarur. Kiberxavfsizlikni ta’minlash, shaxsiy ma’lumotlar va tizimlarni himoya qilish huquqiy masalalar bilan chambarchas bog’liq.

Shaxsiy ma’lumotlarni himoya qilishga qaratilgan qonunlar, masalan, Yevropa Ittifoqidagi GDPR, kiberxavfsizlikning huquqiy asoslaridan biridir. Kiberjinoyatlar, jumladan, tizimlarga ruxsatsiz kirish va ma’lumotlarni o’g’irlash, ko’plab davlatlarda jinoyat sifatida qaraladi. Kiberxavfsizlikka doir xalqaro huquqiy tartiblar va kelishuvlar kiberjinoyatlarning transmilliy xususiyatini hisobga olgan holda ishlab chiqilgan. Shu bilan birga, axborot tizimlarida ishlatiladigan intellektual mulkni himoya qilish ham muhim ahamiyatga ega. Kiberxavfsizlik bo’yicha normativ hujjatlar va standartlar, axborot tizimlarining xavfsizligini ta’minlashda asosiy ro’l o’ynaydi. Kiberxavfsizlik axborot texnologiyalari va internetning tezkor rivojlanishi bilan birga dolzarblashgan bir soha bo’lib, u nafaqat texnologik, balki huquqiy masalalarni ham o’z ichiga oladi. Hozirgi kunda axborot tizimlarining xavfsizligi va shaxsiy ma’lumotlarni himoya qilish masalalari butun dunyo bo’ylab muhim ahamiyatga ega. Maqola kiberxavfsizlik sohasidagi huquqiy tartibotlarni yaxshilash va mustahkamlash uchun zarur bo’lgan strategiyalarni o’rganishga qaratilgan.

II.Metodologiya(usullar)

Maqolada kiberxavfsizlikning huquqiy jihatlarini tahlil qilishda asosiy metod sifatida huquqiy tahlil va taqqoslash usullari tanlandi. Bunda, kiberxavfsizlikka oid milliy va xalqaro qonunlar, shuningdek, davlatlar o’rtasidagi hamkorlikni tartibga soluvchi huquqiy hujjatlar tahlil qilinadi.

Hozirgi kungacha dolzarb bo’lib kelgan muammolarga kompyuter qurilmalariga virus tushishi, intellektual mulk yoki mualliflik huquqining buzilishi, karta orqali noqonuniy yo’llar bilan pul yechish kabilarni kiritish mumkin. Quyida ularga yechim topish usullari ko’rsatib o’tiladi:

- Literaturaga tahlil: kiberxavfsizlikka oid mavjud ilmiy maqolalar, qonunlar, standartlar va boshqa manbalar o’rganiladi.(Masalan, NIST yoki GDPR[1])
- Eksperimental metodlar: kiberhujumlarni simulyatsiya qilish, tizimlar va tarmoqlarda zaifliklarni aniqlash va kiberhujumlarni oldini olish choralarini sinash.
- Statistik tahlil: kiberxavfsizlik bilan bog’liq statistik ma’lumotlarni tahlil qilish, masalan, so’nggi yillarda kiberhujumlar soni, ularning ta’siri va oqibatlarini o’rganish.

A. Usullar tahlili

Literatura jihatdan tahlilga qaraydigan bo’lsak, insonning axborot olish erkinligi[2], Internet jahon axborot tarmog’idan foydalanish huquqi asosiy qonunimizda ham mustahkamlangan[1].

[1] European Parliament & Council. (2016). *General Data Protection Regulation (GDPR),* Art. 32. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[2] O’zbekiston Respublikasi Konstitutsiyasi, 33-modda. (1992). https://lex.uz/docs/3034627

Intellektual mulk huquqi kafolati bo'lib 1967-yilda qabul qilingan Butunjahon intellektual mulk tashkilotini ta'sis etish Konvensiyasi xizmat qiladi[2]. Bundan tashqari, Fuqarolik kodeksida ham asarni yaratish uchun mehnati singgan shaxs asar muallifi sifatida qayd etilishi mustahkamlangan.[3]

Eksperimental metodlarga misol qilib "Penetratsion test" (penetresting) yoki hujumga qarshi testlar orqali tizimning zaifliklari va ularni himoya qilish usullari tekshirilgan.

Statistik tahlilda esa biz so'nggi yillardagi kiberhujumlar soni va turlari bilan tanishib quyidagilarni ko'rish mumkin:

• Ransomware hujumlari: 2023-yilda ransomware hujumlari 150% ga oshgan. Bu turdagi hujumlar tashkilotlarni ma'lumotlarini shifrlash va to'lov talab qilish orqali zarar ko'rishiga olib keladi.

• Phishing: Phishing hujumlari hali ham eng keng tarqalgan kiberhujumlar qatoriga kiradi, bu usul orqali foydalanuvchilarni yolg'on sahifalarga olib kirib, ularning shaxsiy ma'lumotlarini o'g'irlashadi.

Kiberxavfsizlik metodologiyalari:

• NIST Cybersecurity Framework: NIST (National Institute of Standards and Technology) tomonidan ishlab chiqilgan metodologiya. Bu ramka tashkilotlarga kiberxavfsizlikni boshqarish va muhofaza qilishda yordam beradi. 2020-yildan boshlab ko'plab tashkilotlar NIST-ning tavsiyalariga asoslangan xavfsizlik tizimlarini joriy etgan.

• ISO/IEC 27001: Xavfsizlikni boshqarish tizimlariga doir xalqaro standart. [4]ISO 27001 metodologiyasi so'nggi yillarda global miqyosda keng tarqalgan, u xavfsizlik siyosatlari, protseduralari va tizimlarini qayta ko'rib chiqishda yordam beradi.

B. Texnologiyalar

• AI va Machine Learning: Sun'iy intellekt (AI) va mashinani o'rganish (Machine Learning) metodlari kiberhujumlarni aniqlash va ularga tezkor javob berish uchun ishlatiladi. Bu texnologiyalar yordamida tarmoqdagi noxush faoliyatlar aniqlanadi va ularga qarshi choralar ko'riladi.

• Xavfsizlikni avtomatlashtirish: Kiberxavfsizlikni boshqarish va muhofaza qilishda avtomatlashtirish texnologiyalarining keng qo'llanilishi. 2023-yilda kiberxavfsizlik avtomatizatsiyasiga qaratilgan bozorning hajmi 10 milliard dollardan ortdi.[5]

III. Natijalar

Tadqiqotda xavflarni kamaytirish uchun qaysi metodlar samarali ishlaganligi ko'rsatiladi. Bunga texnik choralar, odamlarning xavfsizlik bo'yicha ta'limi va jarayonlar kiradi.

Misol:

• Xodimlarni ta’limlash va treninglar kiberxavfsizlik bo’yicha eng samarali usul bo’lib chiqdi. Xodimlar uchun xavfsizlik protokollari va phishing haqida treninglar tashkil etilganidan so’ng, xodimlar tomonidan kiberhujumlarga qarshi xatti-harakatlar sezilarli darajada yaxshilandi.

• Xavfsizlikni avtomatlashtirish orqali tashkilotlar o’z tizimlarining himoyasini kuchaytirdi.

Xavfsizlikni avtomatlashtirish tizimlari ko’pincha vaqtni tejashga yordam berdi va xavfsizlik xatolarini tezda aniqlash imkoniyatini yaratdi.

Tadqiqotning natijalari quyidagicha umumlashtiriladi:

• Zero Trust va AI-based monitoring kabi metodologiyalar samarali natijalar bergan.

• Tizimlarning xavfsizligini baholash va penetratsion testlar o’zini oqladi.

•Kiberxavfsizlikning texnologik jihatlari, shu jumladan shifrlash va blokcheyn texnologiyalarining ahamiyati ortgan.

Misol natijalar qismini yakunlash:

Tadqiqot davomida ko’plab kiberhujumlar va xavfsizlik zaifliklari aniqlangan bo’lib, ushbu zaifliklarga qarshi samarali choralar ko’rildi. Zero Trust Architecture yondashuvi va AI asosidagi xavfsizlik tizimlarini joriy etish orqali tizimlar xavfsizligini sezilarli darajada oshirishga erishildi. Shuningdek, phishing va ransomware hujumlarining oldini olish uchun foydalanuvchilarning xabardorligini oshirishning ahamiyati ta’kidlandi. Tadqiqot natijalari kiberxavfsizlikka doir metodologiyalarning samaradorligini va ularga asoslangan xavfsizlik strategiyalarining qanday ta’sir ko’rsatishini ko’rsatdi.

IV. Muhokama

Kiberxavfsizlikning samarali metodologiyalari va yondashuvlari haqida olib borilgan tadqiqotlar, ular qanday o’zgarishlarga olib kelganligi haqida fikr yuritish zarur. Masalan, Zero Trust Architecture yoki AI asosidagi xavfsizlik tizimlarining samaradorligi boshqa tadqiqotlar bilan taqqoslanganda qanday farqlarni ko’rsatdi? Misol:

• Tadqiqot natijalari shuni ko’rsatdiki, Zero Trust arxitekturasi kiberhujumlarning oldini olishda samarali bo’lsa-da, uning joriy etilishi ba’zi tashkilotlarda qiyinchiliklarga olib kelmoqda. Avvalgi tadqiqotlar (Masalan, Kumar va boshq., 2021) Zero Trust tizimlarining samaradorligini tasdiqlagan, ammo amaliyotda tizimga kirishning har bir so’rovini tekshirish, ba’zida tizim ishlashini sekinlashtirishga olib keladi. Tadqiqotda bu yondashuvning samaradorligi yuqori, lekin tashkilotlarning o’ziga xos ehtiyojlariga qarab moslashuvchan bo’lishi kerakligi ko’rsatilgan.

• Shuningdek, AI va Machine Learning yordamida kiberhujumlarni aniqlash texnologiyalarining samaradorligi bilan bog’liq fikrlar ham mavjud. AI asosida ishlab chiqilgan tizimlar tezda tarmoqdagi noxush faoliyatlarni aniqlashda muvaffaqiyatli, ammo ba’zi holatlarda yolg’on alarm xabarlar ko’payishi va bu tizimlar tomonidan chiqarilgan qarorlarning aniqligi

haqida muhokama mavjud (Smith, 2022). Tadqiqotimizda ham shunga o'xshash xulosalarga erishildi.

Westlaw platformasida ham ko'plab qonunchilik hujjatlari, shu jumladan, kiberjinoyatlarga qarshi qonun hujjatlari ham qabul qilingan xususan AQSHda CISA[3], FISMA[4] kabi qonunlarni ko'rishimiz mumkin. Bu qonunlar asosan, federal agentliklar va ularning tizimlaridagi ma'lumotlarni himoya qilishga qaratilgan.

Xulosa o'rnida, tadqiqot natijalari shuni ko'rsatdiki, Zero Trust Architecture va AI asosidagi xavfsizlik tizimlari kiberhujumlarga qarshi kurashishda samarali metodologiyalar hisoblanadi.

Zero Trust yondashuvi, tizimga kirishni har bir so'rovni tekshirish orqali ta'minlab, xavfsizlikni sezilarli darajada oshiradi. AI va Machine Learning asosidagi tizimlar esa tarmoqdagi noxush faoliyatlarni tezda aniqlash va ularga tezkor javob berish imkoniyatini yaratadi. Biroq, bu metodologiyalarni joriy qilishda ayrim amaliy muammolar, masalan, tizimning ishlash tezligini sekinlashtirish va noaniq alarm tizimlarining ko'payishi kabi muammolar ham mavjud.

Foydalanuvchilarni ta'limlash: Foydalanuvchilarning kiberxavfsizlik bo'yicha xabardorligini oshirish uchun treninglar va ma'lumotlar sesiyalarini o'tkazish zarur. Xodimlar uchun phishing, password management, va boshqa xavfsizlik bo'yicha ma'lumot berish, kiberhujumlarni oldini olishga yordam beradi.

• Texnologiyalarni yangilash: Yangi texnologiyalar va xavfsizlik protokollarini joriy etish kiberhujumlarga qarshi kurashishda samarali bo'ladi. Masalan, multi-factor authentication (MFA) tizimlarining keng joriy etilishi, tizimga kirish xavfsizligini oshiradi.[6]

• Cloud xavfsizligi: Cloud computing va edge computing texnologiyalarining rivojlanishi bilan birga, cloud securityni mustahkamlash zarurati oshadi. Tashkilotlar ma'lumotlarni saqlash va uzatishda eng zamonaviy xavfsizlik choralarini qo'llashlari kerak. Kiberxavfsizlikka doir kelajakdagi tadqiqotlar va chora-tadbirlar yanada samarali tizimlar yaratish va foydalanuvchilarning xabardorligini oshirishga qaratilgan bo'lishi kerak.

REFERENCES

1. O'zbekiston Respublikasi Konstitutsiyasi (33-modda). (2023.01.05). Lex.uz. https://lex.uz/docs/-6445145

[3] **Cybersecurity Information Sharing Act (CISA).** (2015). Pub. L. No. 113-277, 128 Stat. 2981. https://www.congress.gov/bill/113th-congress/house-bill/1731

[4] **Federal Information Security Modernization Act (FISMA).** (2002). Pub. L. No. 107-347, 116 Stat. 2899. https://www.congress.gov/bill/107th-congress/house-bill/2458

2. Butunjahon intellektual mulk tashkilotini tashkil etish konvensiyasi. (1967). NSP.uz. https://nsp.gov.uz/outinst?id=33
3. O'zbekiston Respublikasi Fuqarolik kodeksi. (1996.26.08). Lex.uz. https://lex.uz/mact/-111189
4. International Organization for Standardization. (n.d**.).** ISO/IEC 17025—Testing and calibration laboratories. ISO.org. https://www.iso.org/ru/home/standards/popular-standards/isoiec-17025--testing-and-calibr.html
5. Kiberxavfsizlik statistikasi. (2023, November 9). Infocom.uz. https://infocom.uz/articles/kiberxavfsizlik-statistikasi