ISSN 2181-3187

DAVLAT ORGANLARINING KIBERXAVFSIZLIGI.

Harbiy ta'lim fakulteti
maxsus tayorgarlik sikli dotsenti
Niyazov Erkin SHamsiyevich
BuxDPI Harbiy ta'lim
fakulteti 1 bosqich talabasi
Komilov Mehriddin Malikovich

Annotatsiya: Kiberxavfsizlik davlat organlari uchun ustuvor yo'nalishga aylangan, chunki ular milliy xavfsizlik, davlat xizmatlari va maxfiy ma'lumotlarni buzishga olib keluvchi kiberhujumlarga tobora ko'proq duch kelmoqda. Ushbu maqolada davlat muassasalarida kiberxavfsizlikning holati, mavjud muammolar, qo'llanilayotgan usullar va yaxshilash strategiyalari tahlil qilinadi. Raqamli infratuzilmani himoya qilish uchun kuchli siyosat, ilg'or texnologiyalar va xalqaro hamkorlikning ahamiyati alohida ta'kidlanadi.

Kalit so'zlar: kiberxavfsizlik, davlat organlari, davlat muassasalari, kiber tahdidlar, raqamli infratuzilma, axborot xavfsizligi, milliy xavfsizlik.

Dunyo bo'ylab davlat organlari muhim operatsiyalarni boshqarish va davlat xizmatlarini taqdim etishda raqamli texnologiyalarga tobora ko'proq tayanmoqda. Ammo bu bog'liqlik ularni ransomware, fishing va davlat tomonidan homiylik qilinadigan xakerlik kabi jiddiy kiber tahdidlarga duchor qiladi. Ushbu tahdidlarning oqibatlari xizmatlarning buzilishidan tortib maxfiy ma'lumotlarning buzilishigacha jiddiy bo'lishi mumkin. Mazkur maqolada davlat organlarida kiberxavfsizlikning ko'p qirrali mohiyati o'rganilib, xavflarni kamaytirish uchun keng qamrovli strategiyalarga ehtiyoj ta'kidlanadi.

Davlat organlarida kiberxavfsizlik choralarini tahlil qilish uchun ushbu tadqiqotda quyidagi aralash usullar qo'llanildi:

ISSN 2181-3187

Kvantitativ tahlil: So'nggi besh yilda davlat muassasalariga qaratilgan kiberhujumlar bo'yicha ma'lumotlar to'planib, tendensiyalar va naqshlar aniqlangan.

Sifatli intervyular: Kiberxavfsizlik bo'yicha mutaxassislar, davlat organlarining IT xodimlari va siyosatshunoslar bilan intervyular o'tkazilib, amaldagi amaliyotlar va muammolar haqida tushunchalar olindi.

Case study: SolarWinds hujumi kabi aniq kiberhodisalar batafsil o'rganilib, javob strategiyalari va natijalar baholandi.

Davlat organlarining kiberxavfsizligi bugungi kunning eng dolzarb masalalaridan biridir, chunki davlatning ichki va tashqi xavfsizligi ko'pincha axborot texnologiyalariga bog'liq. Quyida davlat organlarining kiberxavfsizligi haqida qisqacha tahlil beriladi:

Davlat organlarining kiberxavfsizligi nima uchun muhim?

Milliy xavfsizlik: Davlat organlari davlatning strategik, harbiy, iqtisodiy va ijtimoiy ma'lumotlarini saqlaydi. Kiberhujumlar orqali ushbu ma'lumotlar oshkor bo'lishi yoki o'g'irlanishi milliy xavfsizlikka tahdid soladi.

Jamoatchilik ishonchi: Fuqarolar davlat xizmatlarining xavfsiz va uzluksiz ishlashiga ishonadi. Kiberhujumlar davlat tizimlariga bo'lgan ishonchni zaiflashtirishi mumkin.

Iqtisodiy ta'sir: Davlat tizimlariga hujumlar iqtisodiy yo'qotishlarga olib kelishi mumkin, chunki davlat xizmatlarining uzilishi yoki ma'lumotlarning yo'qotilishi ko'plab xarajatlarni talab qiladi.

Asosiy tahdidlar

Ransomware hujumlari: Davlat organlarining ma'lumotlari shifrlanib, qaytarib olish uchun to'lov talab qilinadi.

Fishing (Phishing): Davlat xodimlarining shaxsiy ma'lumotlarini o'g'irlash orqali tizimga kirishga urinish.

DDoS hujumlari: Davlat veb-saytlarini vaqtinchalik ishdan chiqarish orqali faoliyatni izdan chiqarish.

ISSN 2181-3187

Tashqi davlatlar tomonidan olib boriladigan kiberjosuslik: Davlat sirlarini o'g'irlash va noto'g'ri ma'lumot tarqatish.

Ichki tahdidlar: Davlat xodimlari tomonidan xato yoki qasddan ma'lumotlarning oshkor qilinishi.

Kiberxavfsizlikni mustahkamlash choralar

Kiberxavfsizlik siyosatini ishlab chiqish: Davlat darajasida axborot xavfsizligi bo'yicha qat'iy qonun va reglamentlarni ishlab chiqish.

Xodimlarni o'qitish: Davlat xizmatchilariga kiberxavfsizlik qoidalarini o'rgatish va ularda xavfsizlikka oid mas'uliyatni oshirish.

Texnik chora-tadbirlar:

- Ma'lumotlar shifrlash.
- Kuchli parol siyosatini qo'llash.
- Foydalanuvchilarni autentifikatsiya qilish (masalan, ikki bosqichli tekshirish).
- Zararli dasturlarga qarshi vositalarni doimiy yangilab turish.

Monitoring tizimlari: Doimiy ravishda tizimlarni nazorat qilish, xususan, shubhali faoliyatni aniqlash uchun sun'iy intellekt va tahliliy vositalarni qo'llash.

Favqulodda vaziyatlar uchun reja: Kiberhujumlardan so'ng tiklanish rejalarini ishlab chiqish va sinovdan o'tkazish.

Xalqaro hamkorlik

- Davlatlararo kiberxavfsizlik bo'yicha hamkorlik shartnomalari tuzish.
- Kiberjinoyatchilikka qarshi xalqaro tashkilotlar bilan ishlash (Interpol, Europol va boshqalar).
- Texnologiya gigantlari bilan hamkorlik qilish (Microsoft, Google va boshqalar).

Davlat organlarining kiberxavfsizligi davlat boshqaruvining muhim bir bo'lagi bo'lib, uni mustahkamlash uchun texnik, huquqiy va ma'naviy choralarni birgalikda amalga oshirish zarur. Bu nafaqat davlatning o'ziga, balki fuqarolar xavfsizligiga ham bevosita ta'sir ko'rsatadi.

Natijalar davlat organlarining kiberxavfsizlikni ustuvor vazifa sifatida belgilash zarurligini ko'rsatadi. Byudjet cheklovlari, kadrlar yetishmasligi va agentliklararo

ISSN 2181-3187

hamkorlikning yo'qligi samarali himoyaga to'sqinlik qiladi. Hukumatlar sun'iy intellekt, mashinani o'rganish va "zero-trust" arxitekturalarini qo'llash orqali himoyani kuchaytiruvchi faol yondashuvni qabul qilishlari kerak. Bundan tashqari, xalqaro hamkorlik umumiy razvedka va resurslardan foydalanishga imkon beradi, bu esa global tahdidlarga qarshi chidamlilikni oshiradi.

Xulosa

Davlat organlari milliy xavfsizlikni ta'minlashda old qatorlarda turadi, shuning uchun ularni kiber tahdidlardan himoya qilish muhimdir. Aniqlangan muammolarni hal qilish uchun quyidagi tavsiyalar beriladi:

Zamonaviy infratuzilmaga sarmoya: Eskirgan IT tizimlarini xavfsiz va kengaytiriladigan texnologiyalarga almashtirish.

To'liq trening dasturlari: Xodimlarning xabardorligini oshirish va insoniy xatolarni kamaytirish uchun muntazam kiberxavfsizlik bo'yicha treninglar o'tkazish.

Siyosat ishlab chiqish: Davlat organlari ehtiyojlariga mos aniq va bajarilishi mumkin bo'lgan kiberxavfsizlik siyosatini amalga oshirish.

Hamkorlikni kuchaytirish: Yangi tahdidlardan xabardor bo'lish uchun xususiy sektor mutaxassislari va xalqaro tashkilotlar bilan hamkorlikni rivojlantirish.

Doimiy monitoring: Real vaqt monitoring vositalarini qo'llash va muntazam penetratsion testlar o'tkazish orqali zaifliklarni aniqlash va darhol bartaraf etish.

Ushbu choralarni qabul qilish orqali davlat organlari kuchli kiberxavfsizlik infratuzilmasini yaratib, muhim infratuzilmalarni himoya qilish va davlat faoliyatiga bo'lgan ishonchni ta'minlay oladi.

Adabiyotlar.

1. O’zbekiston Respublikasi prezidentining “2017 —2021 yillarda O’zbekiston respublikasini rivojlantirishning beshta ustuvor yo’nalishi bo’yicha harakatlar strategiyasini «Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili»da amalga oshirishga oid davlat dasturi to’g’risida”gi Farmoni, 2020 yil 2 mart, PF-5953-son

ISSN 2181-3187

2. O’zbekiston Respublikasi prezidentining “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to’g’risida”gi Farmoni, 2018 yil 19 fevral, PF-5349-son

3. O’zbekiston Respublikasi prezidentining “«Raqamli O’zbekiston -2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to’g’risida”gi Farmoniga 1-ilova “Raqamli O’zbekiston –2030” strategiyasi. 2020 yil 5 oktyabr, PF-6079-son.

4. Mulaydinov, F., & Nishonqulov, S. (2021). The role of information technologies in the development of the digital economy. The role of information technologies in the development of the digital economy.

5. Abdullajonov, D. (2022). Корхонада ходимларнинг меҳнат мотивациясини кучайтиришнинг ижтимоий-иқтисодий механизмларини такомиллаштириш: меҳнат мотивациясини, хориж тажрибаси, самарадорлиги, корпоратив тизимлар, инновацион иқтисодиёт. Qo'qon universitetining ilmiy materiallar bazasi, 1(000005)

6. G.Q. Qosimova, F.M. Mulaydinov. Iqtisodiyot va biznesda innovatsion rivojlanish muammolari. Ilm va madaniyat yosh olim va yetakchilar nigohida: xalqaro ilmiy-amaliy onlayn konferentsiyasi, 26 iyun 2020 y. –Qo‘qon. 172-174 betlar.

7. Добродеев Александр Юрьевич, кандидат технических наук, старший научный сотрудник, советник генерального директора ФГУП «Центральный научно-исследовательский институт связи», г. Москва, Россия. E-mail: a.dobrodeev@zniis.ru

8. Konvenciya OON ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (koncepciya). 2011. http://www.scrf.gov.rU/documents/6/112.html