ISSN 3060-4567

KIBERXAVFSIZLIK: ZAMONAVIY TAHDIDLAR VA HIMOYA STRATEGIYALARI

КИБЕРБЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ УГРОЗЫ И СТРАТЕГИИ ЗАЩИТЫ

CYBERSECURITY: MODERN THREATS AND PROTECTION STRATEGIES

Toshboltayev Faxriddin O'rinboyevich

Farg'ona Davlat Universiteti, Axborot Texnologiyalari kafedrasi katta o'qituvchisi (PhD)

Muhammadova Oydinoy Imomali qizi

Farg'ona davlat universiteti,Chet tillari fakulteti, 1-bosqich, 24.111-guruh talabasi

Annotatsiya: *Ushbu maqolada zamonaviy kiberxavfsizlik tahdidlari, ularni aniqlash va bartaraf etish usullari, shuningdek, O'zbekiston va dunyo miqyosida qo'llanilayotgan samarali strategiyalar, zamonaviy kiberxavfsizlik tahdidlari va ularni bartaraf etish choralari o'rganiladi. Dastlab zararli dasturlar, ijtimoiy muhandislik, tarmoq hujumlari kabi tahdidlar tahlil qilinadi. Keyin esa zamonaviy himoya texnologiyalari va xalqaro hamkorlik masalalariga e'tibor qaratiladi. Tadqiqot natijasida kiberxavfsizlikni ta'minlashda kompleks yondashuv zarurligi xulosa qilindi.*

Аннотация: *В данной статье рассматриваются современные угрозы кибербезопасности, методы их выявления и устранения, а также эффективные стратегии, применяемые в Узбекистане и во всем мире, современные угрозы кибербезопасности и меры по их устранению. Первоначально анализируются такие угрозы, как вредоносное ПО, социальная инженерия и сетевые атаки. Затем внимание будет уделено современным оборонным технологиям и международному сотрудничеству. Исследование пришло к выводу, что необхдим комплексный подход к обеспечению кибербезопасности.*

ISSN 3060-4567

Abstract: *This article examines modern cybersecurity threats, methods for identifying and eliminating them, as well as effective strategies used in Uzbekistan and the world, modern cybersecurity threats and measures to eliminate them. First, threats such as malicious programs, social engineering, network attacks are analyzed. Then, attention is paid to modern protective technologies and international cooperation. The study concluded that an integrated approach to ensuring cybersecurity is necessary.*

Kalit so‘zlar: *Kiberxavfsizlik, tahdidlar, zararli dasturlar, phishing, DDoS hujumlar, axborot himoyasi, kiberhujum, firewall, kriptografiya, autentifikatsiya, O‘zbekiston, xalqaro hamkorlik.*

Ключевые слова: *Кибербезопасность, угрозы, вредоносные программы, фишинг, DDoS-атаки, информационная безопасность, кибератака, межсетевой экран, криптография, аутентификация, Узбекистан, международное сотрудничество.*

Keywords: *Cybersecurity, threats, malware, phishing, DDoS attacks, information security, cyber attack, firewall, cryptography, authentication, Uzbekistan, international cooperation.*

KIRISH

Bugungi tez sur’atlar bilan rivojlanayotgan raqamli dunyoda kiberxavfsizlik muammosi tobora dolzarb tus olmoqda. Jamiyatning barcha qatlamlari – davlat idoralari, xususiy sektor, ta’lim va sog‘liqni saqlash muassasalari, hatto oddiy foydalanuvchilargacha – axborot texnologiyalaridan faol foydalanmoqda. Shu bilan birga, kiberhujumlar sonining keskin ortib borayotgani, ma’lumotlar o‘g‘irlanishi, firibgarliklar va tarmoqlarni izdan chiqarish kabi xavf-xatarlar yangi himoya mexanizmlarini ishlab chiqishni taqozo qilmoqda. Axborot va kommunikatsiya texnologiyalaridan keng foydalanish jamiyatning barcha sohalarida raqamli himoya tizimlarini mukammallashtirish zaruratini yuzaga keltirdi.

ADABIYOTLAR TAHLILI VA METODLAR

Kiberxavfsizlik sohasida olib borilgan tadqiqotlar shuni ko‘rsatadiki, so‘nggi o‘n yillikda raqamli texnologiyalarning rivojlanishi bilan bir qatorda axborot xavfsizligi tahdidlari ham sezilarli darajada ortgan.

- J. Blyth (2013) o‘zining "Cybersecurity: Protecting Critical Infrastructures" nomli asarida kiberxavfsizlikni davlat va strategik infratuzilmalarning barqarorligini ta’minlash uchun zarur omil sifatida ko‘rsatgan.
- W. Stallings (2018) esa "Computer Security: Principles and Practice" kitobida zamonaviy tahdid turlari, zararli dasturlar, phishing hujumlar, DDoS hujumlar va ijtimoiy muhandislik usullarini batafsil tasniflab bergan. Unga ko‘ra, zamonaviy himoya usullari ko‘p bosqichli (multi-layered) yondashuv asosida tuzilishi kerak.

O‘zbekiston Respublikasida ham "Kiberxavfsizlik to‘g‘risida"gi Qonun va "Raqamli O‘zbekiston – 2030" strategiyasi orqali axborot resurslari va infratuzilmalarning himoyasini ta’minlash choralari ko‘rilmoqda.

Xalqaro Telekommunikatsiya Ittifoqining (ITU) "Global Cybersecurity Index" hisobotlariga ko‘ra, muvaffaqiyatga erishgan davlatlar kompleks siyosat ishlab chiqqan: qonunchilik, texnik himoya va foydalanuvchi xabardorligini oshirish asosiy omillar sifatida ko‘rsatilgan.

Tadqiqot metodologiyasi quyidagilarga asoslanadi:

- Adabiy manbalarni o‘rganish va tahlil qilish;
- Jahon va O‘zbekiston statistik ma’lumotlarini tahlil qilish;
- Tahdidlar va himoya strategiyalarini tizimli taqqoslash;
- Kompleks tahlil orqali umumiy xulosalar chiqarish.

NATIJALAR VA MUHOKAMA

Olingan natijalar zamonaviy tahdidlar orasida zararli dasturlar va phishing hujumlari eng keng tarqalganini ko‘rsatdi. Xususan:

- Zararli dasturlar (malware), ya'ni viruslar, trojanlar, ransomware dasturlari orqali korxonalar va shaxsiy foydalanuvchilarning ma'lumotlariga ruxsatsiz kirish va ularni shikastlash holatlari ko‘paymoqda. Ransomware tahdidlarida hujumchilarning maqsadi – foydalanuvchi ma’lumotlarini bloklab, pul to‘lovini talab qilishdir.
- Phishing hujumlari foydalanuvchilarning ishonchini qozonish orqali ularning login, parol, bank kartasi ma’lumotlarini o‘g‘irlashga qaratilgan. Soxta veb-saytlar, e-mail va SMS xabarlar orqali amalga oshiriladi.

- DDoS (Distributed Denial of Service) hujumlari orqali serverlar va xizmatlar ish faoliyati izdan chiqariladi, bu esa kompaniyalarga katta moliyaviy va imijiy zarar yetkazadi.

Tahlillar ko‘rsatmoqdaki, har yili kiberhujumlarning soni o‘rtacha 20–25% ga oshib bormoqda. ITU tomonidan chop etilgan Global Cybersecurity Index’ga ko‘ra, rivojlangan davlatlar (masalan, AQSh, Buyuk Britaniya, Singapur) har yili kiberxavfsizlik uchun umumiy byudjetining 8–10% qismini ajratmoqda.

O‘zbekiston tajribasi:

– 2020-yilda qabul qilingan "Kiberxavfsizlik to‘g‘risida"gi Qonun va "Raqamli O‘zbekiston – 2030" dasturi doirasida maxsus Kiberxavfsizlik markazlari tashkil etildi.

– Davlat organlari va yirik kompaniyalar o‘z axborot tizimlariga zamonaviy antivirus va firewall tizimlarini joriy etmoqda.

– E'tiborli jihati shuki, foydalanuvchilar o‘rtasida raqamli savodxonlik darajasi pastligi hali ham asosiy muammolardan biri bo‘lib qolmoqda.

Himoya strategiyalarining samaradorligi:

– Antivirus va firewall tizimlari zararli dasturlarni aniqlash va bloklashda asosiy vosita hisoblanadi.

– Kriptografik himoya (ma’lumotlarni shifrlash) axborot maxfiyligini ta’minlashda samarali vosita bo‘lib, ayniqsa bank sohasida keng qo‘llaniladi.

– Ko‘p bosqichli autentifikatsiya (2FA) — foydalanuvchi hisoblarini himoya qilishda eng oddiy va samarali usullardan biridir.

– Cyber hygiene — foydalanuvchilarni muntazam o‘qitish, ularga phishing va zararli havolalardan ehtiyot bo‘lishni o‘rgatish kiberxavfsizlik siyosatining ajralmas qismiga aylangan.

Faqat texnik himoya choralari bilan cheklanib qolish yetarli emas. Kiberxavfsizlikni ta’minlash uchun:

- Texnologik vositalar (antivirus, firewall, shifrlash tizimlari);

Ijtimoiy omillar (foydalanuvchilarning axborot xabardorligini oshirish);

- Huquqiy bazani kuchaytirish (kiberjinoyatlarga qarshi qat’iy choralar) uyg‘unlashgan holda qo‘llanilishi kerak.

Shuningdek, xalqaro hamkorlikni rivojlantirish, tajriba almashish va global kiberxavfsizlik standartlariga rioya qilish ham kiber tahdidlarga qarshi kurashda muhim ahamiyat kasb etadi.

XULOSA

Tadqiqot natijalariga ko‘ra, kiberxavfsizlikni ta’minlashda kompleks yondashuv muhim ahamiyatga ega. Texnologik himoya choralarini joriy etish, foydalanuvchilarning raqamli savodxonligini oshirish va huquqiy bazani mustahkamlash birgalikda tahdidlarni sezilarli darajada kamaytirishi mumkin. Kelgusida xalqaro tajribani o‘rganish va ilmiy-tadqiqot ishlarini kuchaytirish zarur.

ADABIYOTLAR RO‘YXATI

1. Blyth, J. (2013). Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Wiley.
2. Stallings, W. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.
3. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. (2021). Kiberxavfsizlik asoslari.
4. International Telecommunication Union (ITU). (2022). Global Cybersecurity Index Reports.