KIBERXAVFSIZLIK

Muhammadiyeva Jasmina Akbar qizi
Shahrisabz Davlat Pedagogika instituti
Xorijiy til va adabiyot ingliz tili 1.24 – guruh talabasi.
jasminamukhammadiyevaa14@gmail.com
+998971290415

Annotatsiya : *Kiberxavfsizlik – bu tizimlar, tarmoqlar va dasturlarning raqamli hujumlardan himoya qilish uchun texnologiyalar, jarayonlar va amaliyotlardan foydalanish usuli. Kiberhujumlar ko’pincha nozik ma’lumotlar va ma’lumotlarni nishonga oladi va bu ma’lumotlarga kirish orqali kiberjinoyatchilar, foydalanuvchilar va kompaniyalardan pul undiradilar, odddiy jarayonlarni to’xtatadilar va butun saytlarni o’chirib tashlaydilar. Samarali kiberxavfsizlik har qanday biznes uchun muhim tarkibiy qism bo’lib, kichik va o’rta tashkilotlar uchun undan ham ko’proq narsa xavf ostida, chunki ular ko’pincha bunday hujumlardan xalos bo’lish uchun resurslarga ega emaslar. Ma’lumotlarga asoslangan zamonaviy dunyomizda mavjud bo’lgan ma’lumotlar va qurilmalar soni ortib borayotgani sababli kinerhujumlardan himoyalanish tobora qiyinlashib bormoqda. Bu maqolada kiberhujum, kiberxavfislik, kiberxavfsizlikni rivojlantirish uchun qanday choratadbirlar ko’rilayotganligi haqida ma’lumotlar berilgan.*

Kalit so’zlar : *Korporativ josuslik, intellektual mulk, xakerlar, Pandemiya, iqtisodiy bo’htonlar, bank sektori, vaksina, Estee Lauder kompaniyasi, AV-test kompaniyasi, kriptojeking, Xalqaro Tinchlik uchun Karnegi Jamg’armasi, Global Cybersecurity Index, kriptomayner, troyanlar, Bangladesh, Xitoy, Tojikiston;*

Аннотация : *Кибербезопасность — это способ, которым системы, сети и приложения используют технологии, процессы и методы для защиты от цифровых атак. Кибератаки часто нацелены на конфиденциальные данные и информацию, и, получая доступ к этим данным, киберпреступники вымогают деньги у пользователей и компаний, нарушают нормальные процессы и блокируют целые сайты. Эффективная кибербезопасность является важнейшим компонентом для любого бизнеса, и она еще более актуальна для малых и средних организаций, поскольку им часто не хватает ресурсов для защиты от таких атак. По мере того, как количество устройств и данных, доступных в нашем современном мире, управляемом данными, становится все труднее защититься от кибератак. В этой статье представлена*

информация о кибератаках, кибербезопасности и о том, какие меры принимаются для развития кибербезопасности.

Ключевие слова : *Корпоративный шпионаж, интеллектуальная собственность, хакеры, Пандемия, экономическая клевета, банковский сектор, вакцина, компания Estee Lauder, компания AV-test, криптоджекинг, Фонд Карнеги за международный мир, Глобальный индекс кибербезопасности, криптомайнер, трояны, Бангладеш, Китай, Таджикистан;*

Abstract : *Cybersecurity is the use of technologies, processes, and practices to protect systems, networks, and applications from digital attacks. Cyberattacks often target sensitive data and information, and by accessing this data, cybercriminals extort money from users and companies, disrupt routine operations, and take down entire websites. Effective cybersecurity is a critical component for any business, and is even more at risk for small and medium-sized organizations, which often lack the resources to fend off such attacks. In our modern, data-driven world, protecting against cyberattacks is becoming increasingly difficult due to the increasing amount of data and devices available. This article provides information about cyberattacks, cybersecurity, and measure being taken to develop cybersecurity.*

Key words : *Corporate espionage, intellectual property, hackers, Pandemic, economic fraud, banking sector, vaccine, Estee Lauder Company, AV-test company, cryptojacking, Carnegie Endowment for International Peace, Global Cybersecurity Index, cryptominer, Trojans, Bangladesh, China, Tajikistan;*

Kiberhujum tarmoqqa, kompyuter tizimiga yoki raqamli qurilmaga ruxsatsiz kirish orqali ma’lumotlar, ilovalar yoki boshqa aktivlarni o‘g‘irlash, fosh qilish, o‘zgartirish, o‘chirish yoki yo‘q qilishga qaratilgan har qanday qasddan harakatdir.Tahdid qiluvchilar har xil sabablarga ko'ra kiberhujumlarni boshlaydilar, kichik o'g'irlikdan tortib urush harakatlarigacha. Ular maqsadli tizimlariga ruxsatsiz kirish uchun zararli dasturlarga hujumlar , ijtimoiy muhandislik firibgarliklari va parol o'g'irlash kabi turli xil taktikalardan foydalanadilar .Kiberhujumlar biznesni buzishi, zarar etkazishi va hatto yo'q qilishi mumkin.Ma'lumotlar buzilishining dunyo bo‘ylab o'rtacha qiymati 4,88 million dollarni tashkil qiladi . Ushbu narx yorlig'iga qoidabuzarliklarni aniqlash va ularga javob berish, ishlamay qolish va yo'qolgan daromadlar hamda biznes va uning brendiga uzoq muddatli obro'siga putur yetkazish xarajatlari kiradi.Kamroq tarqalgan kiberhujum motivlariga korporativ josuslik kiradi, bunda xakerlar raqobatchilardan nohaq ustunlikka erishish uchun intellektual mulkni o'g'irlashadi va boshqalarni ular haqida ogohlantirish uchun tizim

zaifliklaridan foydalanadigan hushyor xakerlar. Ba'zi xakerlar intellektual qiyinchiliklardan zavqlanib, sport uchun xakerlik qilishadi.

2020-yil kiberxavfsizlik nuqtayi nazaridan eng yomon yillardan biri boldi. Pandemiya va ogir iqtisodiy bohronlar sharoitida kishilarning shaxsiy malumotlarining maxfiyligini taminlash bilan bogliq vazifalar asosiy ustuvorlikdan chetlashib qoldi. 2020-yil mobaynida tadqiqotchilar bank sektoriga qilingan juda katta kolamdagi xakerlik hujumlarini qayd etishdi. Shuningdek, vaksina ustida ish boshlagan tibbiyot kompaniyalari ham xakerlik guruhlari nishoniga aylandi.Shaxsiy malumotlar chiqib ketishi bilan bogliq holatlarga toxtaladigan bolsak, 2020-yil mobaynida 737 millionta fayl ogirlangan. Eng katta ogrilik Estee Lauder kosmetika kompaniyasi bilan sodir boldi. Xakerlar uning bazasidan 440 million nafar shaxsga oid maxfiy malumotlarni omarishgan.Zararkunanda dasturlarning yangi turlarini aniqlash bilan shugullanuvchi AV-test kompaniyasi yil davomida butunlay yangi turdagi zararli dasturlar sonining jadal osganini qayd etgan. Avvalgi yilga nisbatan 2020-yilda fishing hujumlari, tamagir dasturlar va kriptojeking vositasi orqali qilinadigan hujumlar soni 252 foizga kopaygan.

Kiberxujumning xavfi ortib borganiligi sababli davlatlar bu hujumga qarshi choralarni kuchaytirishmoqda.Kiberxavfsizlik uchun turli tadqiqotlar olib borishmoqda .Misol uchun :Global moliyaviy tizimni kibertahdidlardan samaraliroq himoya qilishga erishish uchun Xalqaro Tinchlik uchun Karnegi Jamgarmasi 2020yil noyabr oyida Global moliyaviy tizimni kibertahdidlardan yaxshiroq himoya qilish boyicha xalqaro strategiya ” nomli hisobotini e’lon qildi .Yana «Comparitech» har yili Global Cybersecurity Index metodologiyasi asosida «eng kiberxavfsiz» davlatni aniqlash yuzasidan mustaqil tadqiqot o‘tkazib, davlatlar reytingini e’lon qiladi.Unga ko‘ra oxirgi ikki yil davomida Daniya 3,56 ball bilan eng kiberxavfsiz mamlakat hisoblanadi. U 15 ta mezondan 10 tasida kuchli uchlikka kirdi, ayniqsa, tovlamachi-troyanlar tomonidan hujumga uchragan foydalanuvchilar (0,02 foiz) va kriptomaynerlar tomonidan qilingan hujumlar foizi (0,11 foiz) kabi mezonlarda yaxshi ball topladi. Shuningdek, mobil tovlamachi-troyanlar va mobil bank tovlamachi-troyanlari tomonidan hujumga uchragan bitta ham foydalanuvchi yoq. Boshqa tomondan esa,kiberxavfsizlik boyicha Tojikiston dunyodagi eng kam himoyalangan mamlakat bolib, undan keyin Bangladesh va Xitoy orin olgan. Tojikiston bank zararli dasturlari hujumiga uchragan foydalanuvchilar (4,7 foiz), mahalliy zararli dasturlardan kamida bitta hujumga uchragan kompyuterlar (41,16 foiz) va kriptomaynerlarning hujumlari (5,7 foiz) boyicha eng yomon korsatkichlarga ega mamlakat boldi. Xulosa qilib aytganda kibermakondagi tahdidlardan himoyalanishning majburiy asosiy usullari ham shaxsiy, ham korporativ darajada,

birinchi navbatda, dasturiy ta'minot yangilanishlarini muntazam ravishda o'rnatishni o'z ichiga oladi. Shuningdek, antivirus himoyasi, xavfsizlik devori va boshqa axborot xavfsizligi vositalaridan, jumladan DDoS hujumlaridan himoya qilish xizmatlaridan foydalanish tavsiya etiladi .Tahdidlarning oldini olish uchun tashkilotda zaifliklar va axborot xavfsizligi hodisalarini boshqarish jarayonini o'rnatish kerak : qoidalarni yaratish, mas'ul shaxslarni aniqlash, ta'lim tadbirlarini o'tkazish va vaqti-vaqti bilan xodimlarning kompyuterlari xavfsizligini tekshirish. Shu bilan birga, to'lov dasturini shifrlashdan qochish uchun muhim tizimlar va ma'lumotlarni muntazam ravishda zaxiralash va zaxira nusxalarini tizimlarning o'zidan alohida saqlash kerak .Turli xil xizmatlarga kirish uchun bir xil parollardan foydalanmaslik, oddiy va buzilgan parollardan foydalanmaslik, parol menejerlaridan foydalanish va ikki faktorli autentifikatsiyadan foydalanishdan iborat bo'lgan parol siyosatiga alohida e'tibor qaratish lozim .

Foydalanilgan adabiyotlar

1. G’aniyev S.K. , Karimov M.M. , Tashaev K.A. AXBOROT XAVFSIZLIGI Toshkent 07.
2. S.S. Qosimov Axborot texnologiyalari haqida o’quv qo’llanma. Toshkent 07.
3. G’aniyeV S.K. , Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi. TDTU 03.
4. R.Y. Mamajanov, T.J. Rajabov, E.I. Saidaxmedov, I.U. Xushboqov. Kiber xavfsizlik 2024.
5. Shohruh Farhodjon O’g’li Nishonqulov, Rajabboyev.B. , Mamasoliyev.J. Iqtisodiyot sohasiga raqamli texnologiyalarni olib kirish. 2022.
6. Xoldorbayev.R. , Abduvaxobova.R. Kiberxavfsizlik 2022.
7. Akbarova.M. Kiberxavfsizlik – raqamli iqtosodiyotni rivojlantirishning muhim omili.
8. Omonkeldiyev.J. Yangi O’zbekiston raqamli iqtisodiyatining fundamental omili.
9. Nial Adams, Nicholas Herad, “ Data Analysis for network cyber – security ” ,
10. G’aniyev.S.K. “ Kiberxavfsizlik asoslari “ O’quv qo’llanma.