ISSN 3060-4567

KIBERXAVFSIZLIK VA SHAXSIY MA'LUMOTLARNI HIMOYA QILISH

Mo'minova Munisaxon Ulug'bek qizi

Farg'ona Davlat Universiteti

Chet tillari fakulteti, Filologiya va tillarni o'qitish: ingliz tili

1-kurs talabasi

Ilmiy rahbar: ***Toshboltayev Faxriddin O'rinboyevich***

Annotatsiya: *Ushbu maqolada kiberxavsizlikning elementlari va uning kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va ma'lumotlarni zararli hujumlardan himoya qilish usullari haqida ma'lumotlar berilgan. Mazkur maqola xavfsizlik prinsiplari, muhim xavfsizlik nazorati va kiberxavfsizlikning eng yaxshi amaliyotlarini o'z ichiga olgan xavfsizlik asoslarini tushuntirib beradi. Xavfsizlik dasturlari potensial zararli dasturlarni foydalanuvchining xatti- harakatlarini tahlil qilish va yangi infeksiyalarni qanday yaxshiroq aniqlashni o'rganish uchun yo'l yo'riqlar ko'rsatilgan.*

Kalit so'zlar*: Elektron, xavfsizlik, protokollar, virus, mobil, axborot, kiberxavfsizlik, pochta, texnologiya, biznes, kiberjinoyat.*

Аннотация: *В данной статье представлены элементы кибербезопасности и способы защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак. Эта статья объясняет основы безопасности, включая принципы безопасности, ключевые элементы контроля и лучшие практики в области кибербезопасности. В программах безопасности даны рекомендации по анализу поведения пользователя для выявления потенциально вредоносных программ и улучшения способов обнаружения новых угроз.*

Ключевые слова*: Электронный, безопасность, протоколы, вирус, мобильный, информация, кибербезопасность, почта, технологии, бизнес, киберпреступность.*

ISSN 3060-4567

Hozirgi kunda tez sur’atlarda rivojlanayotgan raqamli dunyoda kiberxavfsizlik muhim sohalardan biri sifatida ajralib turadi. Internet va axborot texnologiyalari hayotimizning deyarli barcha jabhalariga chuqur kirib borgan davrda, shaxsiy ma’lumotlarni, moliyaviy ma’lumotlarni va boshqa muhim axborotlarni himoya qilish ehtiyoji yanada dolzarb muammo bo‘lib qoldi. Kiberxavfsizlik deganda, kompyuter tizimlari, serverlar, mobil qurilmalar, tarmoqlar va ma’lumotlarni zararli hujumlardan, firibgarlikdan, ma’lumot o‘g‘irlanishidan yoki buzilishidan himoya qilishga qaratilgan chora-tadbirlar tushuniladi.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo’lib, unga berilgan turlicha ta’riflar mavjud. Kiberxavfsizlikning asosiy maqsadi ma’lumotlarning maxfiyligini saqlash, ularning yaxlitligini va mavjudligini ta’minlash hisoblanadi. Bu uchta asosiy tamoyil "CIA" modeli deb nomlanadi: Confidentiality (Maxfiylik), Integrity (Butunlik), va Availability (Mavjudlik). Maxfiylik ma’lumotlarga faqat ruxsat etilgan foydalanuvchilar kira olishini ta’minlaydi. Butunlik esa ma’lumotlarning to‘g‘riligini saqlashga qaratilgan bo‘lib, ma’lumotlarni ruxsatsiz o‘zgartirish, o‘chirish yoki buzilishdan himoya qiladi. Mavjudlik esa tizimning yoki ma’lumotlarning kerakli vaqtda mavjudligini ta’minlaydi, ya’ni hujum yoki nosozlik bo‘lsa ham, foydalanuvchilar o‘z ma’lumotlariga kira olishlari lozim.

Hozirgi kunda kiberjinoyatchilar tomonidan amalga oshirilayotgan hujum turlari ko‘payib bormoqda. Ular orasida fishing, viruslar, zararli dasturlar, DDoS hujumlari, ma’lumotlarni o‘g‘irlash va firibgarlik kabi usullar mavjud. Fishing bu firibgarlarning yolg‘on elektron pochta yoki xabarlar yuborib, foydalanuvchilardan shaxsiy ma’lumotlarni (login, parol, karta raqami va boshqalar) olishga qaratilgan hujumdir. Zararli dasturlar esa kompyuterga yoki tarmoqqa kirib, ma’lumotlarni o‘g‘irlash, buzish yoki qurilmani ishlamas holga keltirishga mo‘ljallangan bo‘ladi.

Kiberxavfsizlikni ta’minlash uchun ko‘plab usullar mavjud. Birinchidan, kuchli parollar yaratish va ularni muntazam ravishda o‘zgartirish muhim sanaladi. Ikkinchidan, ikki bosqichli autentifikatsiyadan foydalanish zarur. Bu foydalanuvchi tizimga kirishda faqat parolni emas, balki qo‘shimcha tasdiqlash usulini (masalan,

SMS kod yoki biometrik tasdiqlash) ishlatadi. Bundan tashqari, zamonaviy antivirus va xavfsizlik devorlaridan (firewall) foydalanish, dasturlarni muntazam yangilab borish ham muhim himoya choralaridan biri bo‘lib kelmoqda.

Kiberxavfsizlikni ta’minlashda nafaqat texnologik chora-tadbirlar, balki foydalanuvchilarning o‘zlari ham muhim rol o‘ynaydi. Chunki ko‘plab hujumlar insoniy omilga tayanadi: foydalanuvchilarning chalg‘ishi, ehtiyotsizligi yoki bilimsizligi sababli ma’lumotlar qo‘ldan ketadi. Shu sababli, kompaniyalar va tashkilotlar xodimlarini muntazam ravishda kiberxavfsizlik bo‘yicha o‘qitishlari, ularga xavfsizlik qoidalarini tushuntirishlari kerak.

Davlatlar darajasida ham kiberxavfsizlikni ta’minlash uchun maxsus qonunlar, qoidalar va standartlar ishlab chiqilmoqda. Masalan, Yevropa Ittifoqida GDPR (General Data Protection Regulation) deb nomlangan umumiy ma’lumotlarni himoya qilish reglamenti mavjud bo‘lib, bu hujjat shaxsiy ma’lumotlarni qanday yig‘ish, saqlash hamda himoya qilish kerakligini belgilab beradi. Ko‘plab davlatlarda maxsus kiberxavfsizlik markazlari tashkil etilgan bo‘lib, ular milliy darajada kibersohadagi tahdidlarni aniqlash va oldini olish bo‘yicha ishlaydi.

Biznes sohasida kiberxavfsizlik alohida o‘rin tutadi. Kompaniyalar uchun mijozlarning shaxsiy ma’lumotlarini himoya qilish nafaqat qonuniy majburiyat, balki ularning obro‘si va ishonchliligi uchun ham muhimdir. Agar kompaniyada ma’lumotlar sizdirilsa, bu nafaqat moliyaviy yo‘qotishlarga olib keladi, balki mijozlarning ishonchini yo‘qotishga ham sabab bo‘ladi. Raqamli texnologiyalar rivojlanishi insoniyat taraqqiyotining ajralmas qismiga aylangani sababli, kiberxavfsizlik masalasi global miqyosda strategik ahamiyat kasb etmoqda. Zamonaviy texnologik muhitda shaxsiy, korporativ va davlat darajasidagi axborot resurslarini himoya qilish, axborot xavfsizligini ta’minlash va kiberjinoyatlarga qarshi tizimli chora-tadbirlarni ishlab chiqish dolzarb vazifadir. Tahlillar shuni ko‘rsatmoqdaki, kiberxavfsizlik infratuzilmasini yaratishda texnik vositalar va algoritmlarni takomillashtirish bilan bir qatorda, inson omili, ya’ni foydalanuvchilarning raqamli savodxonligini oshirish muhim rol o‘ynaydi.

Raqamli texnologiyalar rivojlanishi insoniyat taraqqiyotining ajralmas qismiga aylangani sababli, kiberxavfsizlik masalasi global miqyosda strategik ahamiyat kasb etmoqda. Zamonaviy texnologik muhitda shaxsiy, korporativ va davlat darajasidagi axborot resurslarini himoya qilish, axborot xavfsizligini ta'minlash va kiberjinoyatlarga qarshi tizimli chora-tadbirlarni ishlab chiqish dolzarb vazifadir. Tahlillar shuni ko'rsatmoqdaki, kiberxavfsizlik infratuzilmasini yaratishda texnik vositalar va algoritmlarni takomillashtirish bilan bir qatorda, inson omili, ya'ni foydalanuvchilarning raqamli savodxonligini oshirish muhim rol o'ynaydi.

Amaliy jihatdan, zamonaviy antivirus tizimlari, kriptografik algoritmlar, tarmoqlarni segmentatsiya qilish, xavfsizlik devorlari (firewall), hamda sun'iy intellekt asosida ishlovchi tahliliy vositalar yordamida kiberxavfsizlikni ta'minlash imkoniyati kengaymoqda. Shu bilan birga, xalqaro tajriba ko'rsatadiki, kiberxavfsizlikni ta'minlash yakkama-yakka harakatlardan ko'ra, ko'p tomonlama hamkorlikni va xalqaro standartlarga asoslangan yondashuvni talab qiladi. Masalan, ISO/IEC 27001 kabi standartlar tashkilotlarga axborot xavfsizligini tizimli tarzda boshqarishda yordam beradi. Shunday qilib, axborot xavfsizligi va kiberxavfsizlikni ta'minlash bugungi va kelajakdagi raqamli transformatsiyaning poydevori sifatida maydonga chiqmoqda. Ilmiy tadqiqotlar va texnologik yutuqlar, huquqiy va institutsional choralar bilan uyg'unlashganda, jamiyatni kiberxavflardan himoya qilishning mustahkam mexanizmlari vujudga keladi. Bu esa, o'z navbatida, raqamli iqtisodiyotning barqaror rivojlanishini va global axborot makonining xavfsizligini ta'minlashda muhim omil bo'lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Andress, J., & Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier.

2. Stallings, W. (2019). Network Security Essentials: Applications and Standards. Pearson Education.

3. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

ISSN 3060-4567

4. Kaspersky Lab. (2023). Cybersecurity trends and predictions. Retrieved from: www.kaspersky.com.

5. Symantec Corporation. (2022). Internet Security Threat Report. Retrieved from: www.broadcom.com/company/newsroom/press-releases.

6. Касперский Лаборатория. (2023). Основы кибербезопасности для бизнеса. URL: www.kaspersky.ru.

7. Печников, С.А. (2020). Информационная безопасность в цифровую эпоху. Москва: Научный мир.

8. Cybersecurity & Infrastructure Security Agency (CISA). (2024). Cyber Essentials. Retrieved from: www.cisa.gov.

9. Агентство кибербезопасности Республики Узбекистан (2023). Киберугрозы и защита персональных данных. Ташкент.

10. Termiz davlat universiteti o‘quv qo‘llanmasi. (2024). Axborot xavfsizligi asoslari. Termiz.