

XAVSIZLIK STANDARTLARI VA PROTOKOLLARI

Umarov Bekzod Azizovich*Farg'ona davlat universiteti, Amaliy matematika va informatika kafedirasi,
o'qituvchi ubaumarov@mail.ru***Mamazokirov Doniyorbek Karimjon o'g'li***Farg'ona davlat universiteti Fizika-matematika fakulteti**Amaliy matematika yo'nalishi**3-bosqich talabasi*mamazokirovdoniyor5@gmail.com

Annotatsiya: Ushbu maqola axborot xavfsizligi sohasidagi standartlar va protokollarni ko'rib chiqadi. Mualliflar, xavfsizlikni ta'minlashda xalqaro va milliy standartlarning ahamiyatini tahlil qilib, ularning samaradorligini baholaydilar. Maqolada, ayniqsa, yangi texnologiyalar va zamonaviy xavf-xatarlar asosida xavfsizlik protokollarining moslashuvchanligi va yangilanishi zarurligi ta'kidlanadi. Tadqiqot natijalari shuni ko'rsatadiki, xavfsizlik standartlari amaliyotga joriy etilganida tashkilotlarning axborot xavfsizligi tizimlari sezilarli darajada mustahkamlanadi. Shuningdek, maqolada kelajakda xavfsizlik protokollarini yanada takomillashtirish bo'yicha bir qancha tavsiyalar berilgan.

Kalit so'zlar: Axborot xavfsizligi, Xavfsizlik standartlari, Xavfsizlik protokollari, Kiberxavfsizlik, Shifrlash, Ma'lumotlarni himoya qilish, Autentifikatsiya va avtorizatsiya, Xavfsizlik tizimlari, Xavf tahlili

Аннотация: Данная статья рассматривает стандарты и протоколы в области информационной безопасности. Авторы анализируют значимость международных и национальных стандартов в обеспечении безопасности и оценивают их эффективность. В статье подчёркивается необходимость адаптации и обновления протоколов безопасности с учётом новых технологий и современных угроз. Результаты исследования показывают, что внедрение стандартов безопасности на практике значительно укрепляет системы информационной безопасности организаций. Кроме того, в статье представлены рекомендации по дальнейшему совершенствованию протоколов безопасности в будущем.

Ключевые слова: Информационная безопасность, стандарты безопасности, протоколы безопасности, кибербезопасность, шифрование, защита данных, аутентификация и авторизация, системы безопасности, анализ угроз.

Annotation: This article examines security standards and protocols in the field of information security. The authors analyze the importance of international and national standards in ensuring security, evaluating their effectiveness. The article emphasizes the need for flexibility and updating of security protocols based on new technologies and modern threats. The research findings indicate that when security standards are

implemented, the information security systems of organizations are significantly strengthened. Additionally, the article offers several recommendations for further improvement of security protocols in the future.

Key words: Information security, Security standards, Security protocols, Cybersecurity, Encryption, Data protection, Authentication and authorization, Security systems, Risk analysis

Kirish

Xavfsizlik standartlari va protokollari zamonaviy jamiyatda muhim ahamiyatga ega. Ular axborot xavfsizligini ta'minlash, tizimlarni himoya qilish va shaxsiy ma'lumotlarni saqlashda qo'llaniladi. Ushbu maqolada xavfsizlik standartlari va protokollari, ularning ahamiyati va qo'llanilishiga e'tibor qaratamiz.

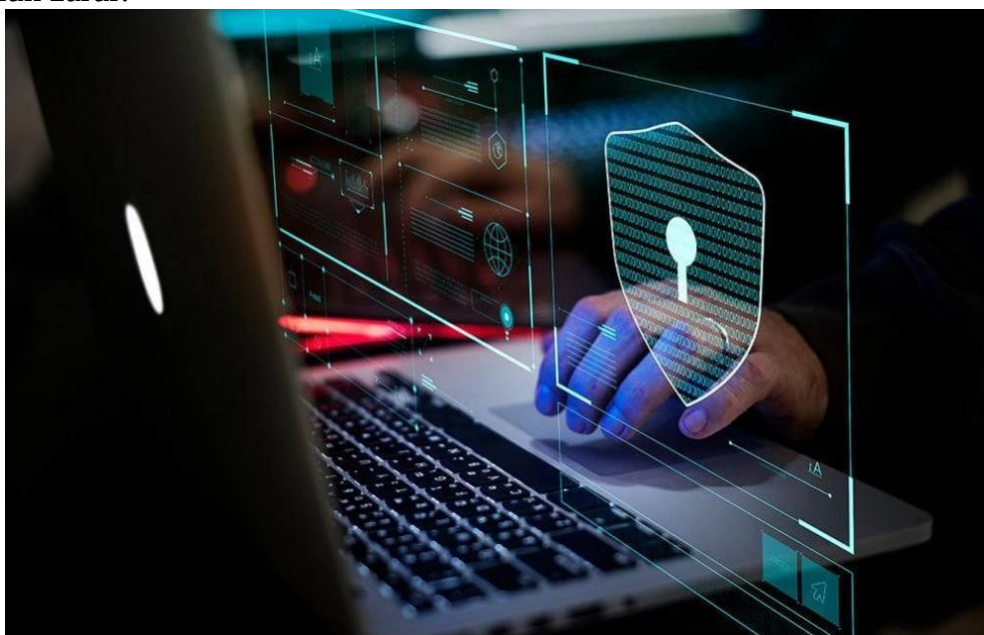
Xavfsizlik Standartlari

Xavfsizlik standartlari - bu tashkilotlar va kompaniyalar tomonidan axborot xavfsizligini ta'minlash uchun ishlab chiqilgan qoidalar va talablar to'plamidir. Ular quyidagi asosiy yo'nalishlarni o'z ichiga oladi:

1. **Texnik standartlar:** Tizimlar va dasturlar uchun xavfsizlik texnologiyalarini belgilaydi. Masalan, shifrlash metodlari, autentifikatsiya jarayonlari va ma'lumotlarni saqlash qoidalari.

2. **Tashkiliy standartlar:** Xavfsizlik siyosatlarini, jarayonlar va javobgarliklarni belgilaydi. Ushbu standartlar tashkilotning xavfsizlikni boshqarish jarayonida muhim rol o'ynaydi.

3. **Huquqiy standartlar:** Mahalliy va xalqaro qonunlarga muvofiq keladigan xavfsizlik talablarini o'z ichiga oladi. Bu qonunlar foydalanuvchilar va ularning ma'lumotlarini himoya qilish uchun zarur.



Xavfsizlik texnikasi – mehnat muhofazasi bo‘limlaridan biri; ishchidagi jarayonlarda vujudga keladigan xavfli omillarning ishlovchilarga zararli ta’siri oldini olishga doir tashkiliy va texnik tadbirlar hamda vositalar majmui. Ularni yaratish va ishlab chiqarishda qo‘llash ishlari belgilangan tartibda tasdiqlangan me’yoriy texnik hujjatlar (standartlar, qoidalar, me’yorlar, instruksiyalar) asosida amalga oshiriladi. Tashkiliy tadbirlar: ishchilarga xavfsiz va zararsiz ish usullari to‘g‘risida yo‘l-yo‘riqlar berish, ishlab chiqarish sanitariyasi va mehnat gigiyenasi asoslarini o‘rgatish; mehnat qilish va dam olish qonun-qoidalarini ishlab chiqish va ishlab chiqarishga tatbiq qilish.

Texnik tadbirlar ma’lum me’yorlar va qoidalariga asoslanadi. Bunda insonning ruhiy, anatomik, fiziologik xususiyatlari hisobga olinadi. Masalan, mashinaning boshqarish organlarini inson uchun qulay yerga joylashtirish, ish vaqtida zararli chang, gaz chiqmasligini ta’minlash zarur, xavfli ta’sirlardan himoya qilish uchun to‘siqlar qilinadi, ogohlantiruvchi belgilar va plakatlar osib qo‘yiladi. Ko‘pincha ishlayotgan mashinalarning uzellari bilan bog‘liq qurilmalar (elektron qurilmalar, fotoelement, avtomatik saqlagich) dan foydalaniladi. Bularga saqlagich klapanlari, vklyuchatellar, eruvchan saqdagichlar, shtiftlar va boshqa kiradi. Xavfli, zararli ishlarni bajarishda jarayonlarni uzoqdan turib boshqarish usuli yaxshi samara beradi. Himoya qilishda signalizatsiyalashdan foydalaniladi. Jihozlarni yurgizib yuborishdan oldin ularning ishi tekshiriladi hamda sinaladi. Juda xavfli jihozlar (bosim ostida ishlaydigan idishlar, yuk ko‘tarish mashinalari) davlat inspeksiyasi nazorati ostida bo‘ladi, namlik, tra, havoning tozaligi, shovqinlar, nurlanish ta’siri va boshqa doimo nazorat qilinadi. Xavfsizlik texnikasi ning muayyan sohalarida ishlaydigan kishilar qoidalariga muvofiq shaxsiy himoya vositalari (kiyim-bosh, poyabzal, ehtiyot belbog‘i, ko‘zoynak va boshqalar)dan foydalanadi. Xar bir korxonada Xavfsizlik texnikasi uchun ma’muriyat javobgar hisoblanadi.

O‘zbekistonda Xavfsizlik texnikasi nuqtai nazaridan eng xavfli va ma’suliyatli korxonalar – paxtani dastlabki ishlash zavodlari, to‘qimachilik korxonalari, teri oshlash korxonalari va boshqalar hisoblanadi, chunki bu korxonalarda presslar ishlatiladi, zararli chang va gazlar ajraladi va boshqa Shu tufayli mehnat xavfsizligi standartlariga qat’iy amal qilish talab qilinadi. Xavfsizlik texnikasi texnika taraqqiyoti, ishlab chiqarishni avtomatlashtirish va kompleks mexanizatsiyalash bilan uzviy bog‘liq bo‘ladi. XAGGINS (Huggins) Charlz Breton (1901.22.9, Galifaks, Kanada) – amerikalik xirurg va onkolog; AQSH milliy Fanlar akademiyasi a’zosi (1949 yildan). 1927-yildan Chikago universitetida ishlagan (1936-yildan xirurgiya professori). 1951-1969-yillarda BenMey klinikasida rakni tadqiqot qilish laboratoriya direktori. Xavfsizlik texnikasi prostata bezi rakini davolashda ilk bor gormonlarni qo‘llab, gormonoterapiyaga asos soldi, bu rak kimyoterapiyasi rivojiga olib keldi. Nobel mukofoti laureati (1966, Rous F. P. bilan hamkorlikda).



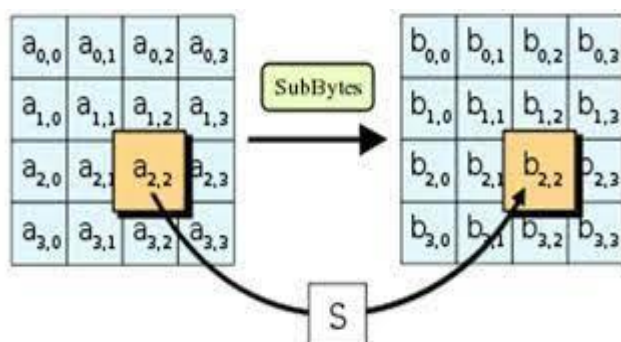
Xavfsizlik Protokollari

Xavfsizlik protokollari - bu ma'lumot almashinuvi va aloqa jarayonlarini xavfsiz qilish uchun mo'ljallangan qoidalar va amaliyotlar to'plamidir. Ular quyidagilarni o'z ichiga oladi:

1. **Autentifikatsiya:** Foydalanuvchilarning kimligini tasdiqlash jarayoni. Bu jarayon parollar, biometrik ma'lumotlar yoki tokenlar orqali amalga oshiriladi.



2. **Ma'lumotlarni shifrlash:** Ma'lumotlarning maxfiylikni ta'minlash uchun shifrlash algoritmlari qo'llaniladi. Bu ma'lumotlar yo'qolishi yoki o'g'irlanishi holatlarida ularni himoya qiladi.



3. **Zarba va xavf tahlili:** Tashkilotlar xavf va zarba tahlilini o'tkazish orqali potensial xavflarni aniqlash va ularga qarshi choralar ko'rishadi.

Xulosa

Xavfsizlik standartlari va protokollari zamonaviy axborot tizimlarining muhim qismidir. Ular tashkilotlarga nafaqat ma'lumotlarni himoya qilishda yordam beradi, balki ularning obro'sini saqlashda ham muhim rol o'ynaydi. Har bir tashkilot o'z xavfsizlik siyosatini, standartlarini va protokollarini ishlab chiqishi va amalga oshirishi zarur. Bu esa kelajakda yuzaga kelishi mumkin bo'lgan xavflardan himoyani ta'minlaydi.

FOYDALANILGAN ADABIYOTLAR:

1. **ISO/IEC 27001:2013.** Information security management systems — Requirements. International Organization for Standardization, 2013.
2. Smith, J., & Brown, A. (2020). *Cybersecurity Protocols and Standards: An Overview*. Journal of Information Security, 15(3), 45-58.
3. Kaspersky, E. (2021). *The Evolution of Encryption in Data Protection*. Retrieved from <https://www.kaspersky.com/tech-news/encryption>, accessed on October 12, 2024.
4. Wikipediya https://uz.m.wikipedia.org/wiki/Xavfsizlik_texnikasi.
5. <https://uz.vogueindustry.com/17170648-risk-identification-basic-concepts-assessment-and-methods-of-determination>.
6. https://www.google.com/imgres?imgurl=https://kuzminykh.org/img/inte-2020/2142/image_Nphs2Rzoq2cKHr052yTWGESE.jpg&tbnid=u6LVojjukdTGOM&vet=1&imgrefurl=https://uz.kuzminykh.org/2142-what-is-authentication.html&docid=rkoKQ0ec4QADIM&w=640&h=378&hl=uz-UZ&source=sh/x/im/m6/4&kgs=05c07c751bef8ed8&shem=abme,trie#imgsrc=u6LVojjukdTGOM&imgdii=udcz5WUFJEzKeM.
7. <https://images.app.goo.gl/sESai92FTVvryDoB8>.