KIBERXAVFSIZLIKDA MA'LUMOTLARNI HIMOYA QILISH VA KIBERXAVFSIZLIKDA INSON OMILI

Rahmonaliyeva Muhabbat Abdimalik qizi
Namangan shahar 2-son Politexnikumi maxsus fan o'qituvchisi
Tojiboyeva Shahloxon Olimovna
Namangan shahar 2-son Politexnikumi informatika fan o'qituvchisi
Tursunov Bekzod Axrorovich
Namangan shahar 2-son Politexnikumi maxsus fan o'qituvchisi
https://doi.org/10.5281/zenodo.17855160

Annotatsiya Maqolada kiberxavfsizlik sohasida ma'lumotlarni himoya qilishning asosiy usullari va prinsiplariga e'tibor qaratilgan. Shuningdek, inson omilining axborot xavfsizligidagi roli, uning kiberxavfsizlik tizimlariga ta'siri va kiber tahdidlarga qarshi kurashishdagi ahamiyati tahlil qilingan. Maqolada nazariy asoslar, amaliy misollar va zamonaviy tadqiqotlar ko'rib chiqilgan.

Kalit so'zlar: kiberxavfsizlik, axborot xavfsizligi, ma'lumotlarni himoya qilish, inson omili, kiberjinoyatchilik, kiber etika.

Raqamli transformatsiya va axborot-kommunikatsiya texnologiyalarining keng joriy etilishi bilan birga, axborot xavfsizligini ta'minlash masalasi dolzarb ahamiyat kasb qilmoqda. Ma'lumotlarning yo'qolishi, buzilishi yoki ruxsatsiz oshkor etilishi foydalanuvchilar, korxonalar va davlat organlari faoliyatiga jiddiy tahdid tug'diradi. Shu sababli, kiberxavfsizlik tizimlarida ma'lumotlarni himoya qilishning samarali mexanizmlari va strategiyalarini ishlab chiqish zarur.

Axborot tizimlarida inson omilining roli katta ahamiyatga ega. Ko'plab kiberhujumlar va axborot xavfsizligi buzilishlari texnik tizimlardagi zaifliklardan ko'ra, ko'proq inson xatolari yoki noto'g'ri qarorlar tufayli sodir bo'ladi. Shu bois, kiberxavfsizlikda texnologik vositalar bilan bir qatorda inson omilini boshqarish jarayoni muhim ahamiyatga ega.

Ma'lumotlarni himoya qilishning asosiy tushunchalari

Ma'lumotlarni himoya qilish (information security) — bu axborotning maxfiyligi, yaxlitligi va mavjudligini ta'minlash jarayonidir. Ushbu jarayon quyidagi asosiy elementlarni o'z ichiga oladi:

Maxfiylik (Confidentiality) – ma'lumotlarga ruxsatsiz kirishni oldini olish.

Yaxlitlik (Integrity) – ma'lumotlarning o'zgartirilmasligi va ishonchliligi.

Mavjudlik (Availability) – ma'lumotlarga kerak bo'lgan vaqtda yetib borish imkoniyati.

Ma'lumotlarni himoya qilish usullari quyidagilarni o'z ichiga oladi: shifrlash (encryption), autentifikatsiya, kirishni nazorat qilish (access control), xavfsizlik monitoringi va zaxira tizimlari (backup systems).

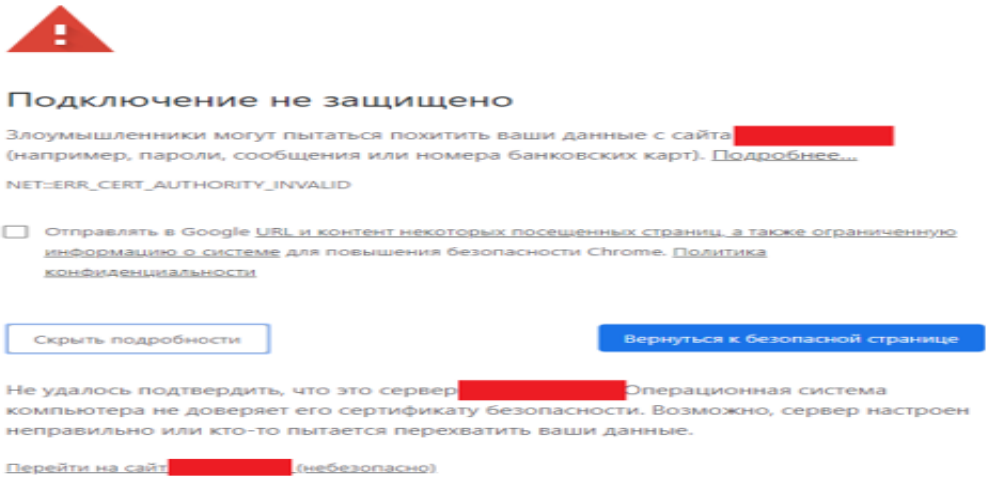
O‘zbekiston kontekstida, 2020-yilda ishlab chiqilgan milliy kiberxavfsizlik strategiyasida axborot tizimlarida ma’lumotlarni himoya qilish va monitoring qilish bo‘yicha aniq vazifalar belgilangan (CSEC, 2020).

Kiberxavfsizlikda inson omili

Foydalanuvchilar tomonidan har qanday yuqori darajadagi xavfsizlik ham buzilishi mumkin. Masalan, Bob amazon.com onlayn do‘konidan biror narsani sotib olmoqchi, deylik. Buning uchun Bob turli kriptografik usullarga tayanadigan SSL (Secure Sockets Layer) protokoli yordamida Amazon bilan ishonchli bog‘lanish uchun veb-brauzerdan foydalanishi mumkin. Ushbu protokol barcha zarur amallar to‘g‘ri bajarilganida kafolatli xavfsizlikni ta’minlaydi. Biroq, ushbu protokolga qaratilgan ba’zi hujum turlari (O‘rtada turgan odam hujumi, Man-in-the-middle attack) mavjudki, ularni amalga oshishi uchun foydalanuvchi “ishtirok”i talab etiladi (1-rasm). Agar foydalanuvchi xavfsiz holatni tanlasa (Вернуться к безопасной странице) hujum amalga oshmaydi. Biroq, foydalanuvchi tomonidan xavfsiz bo‘lmagan tanlov (Перейти на сайт .... (небезопасно)) amalga oshirilganida hujum muvaffaqiyatli tugaydi. Boshqacha

aytganda, yuqori xavfsizlik darajasiga ega protokoldan foydalanilganda ham foydalanuvchining noto‘g‘ri harakati sababli xavfsizlik buzilishi mumkin.

1.Inson omili sababli yuzaga keladigan tahdidlar Parol va autentifikatsiya xavfsizligi: foydalanuvchilar kuchsiz yoki bir xil parollarni ishlatishi.



1-rasm. SSL protokolidagi xavfsizlik ogohlantirishi

- **Ijtimoiy muhandislik (social engineering)**: xodimlar ma’lumotlarni nohaq shaxslarga oshkor qilishi.
- **Noto‘g‘ri** konfiguratsiya va xavfsizlik protokollari: tizimlarni noto‘g‘ri sozlash.
- **Bilim va tajriba yetishmovchiligi**: xodimlar kiberxavfsizlik qoidalarini bilmasligi.

2. Inson omilini boshqarish strategiyalari:

- Doimiy kiberxavfsizlik bo‘yicha trening va o‘quv dasturlari.
- Xodimlar faoliyatini monitoring qilish va tahlil qilish.
- Axborot xavfsizligi siyosati va standartlarini ishlab chiqish va amalda qo‘llash.
- Kiberetika va mas’uliyatni oshirish bo‘yicha kampaniyalar.

Ilmiy tadqiqotlar shuni ko‘rsatadiki, inson omilining samarali boshqarilishi orqali 60–70% kiberxavfsizlik hodisalarining oldini olish mumkin (Stallings, 2021; Khraisat et al., 2023).

4. Zamonaviy kiber tahdidlar va inson omili

Zamonaviy kiberhujumlar ko‘pincha texnologik tizimlar bilan birga inson xatolarini ham hisobga oladi. Misol uchun:

- **Faylni shifrlash viruslari (ransomware)** ko‘pincha xodimlar tomonidan noto‘g‘ri ochilgan elektron pochta ilovalari tufayli tarqaladi.
- **Phishing va social engineering** hujumlari xodimlarning e’tiborsizligi tufayli muvaffaqiyatli bo‘ladi.
- **Ichki xakerlar (insider threats)** — xodimlar tomonidan ma’lumotlarning ruxsatsiz oshkor qilinishi.

Shu sababli, kiberxavfsizlik tizimlarida texnologiya va inson omili bir-birini to‘ldiruvchi element sifatida qaraladi.Odatda foydalanuvchilar esda saqlash oson bo‘lgan parollardan foydalanishga harakat qiladilar. Biroq, bunday yo‘l tutish buzg‘unchi uchun parollarni taxminlab topish imkoniyatini oshiradi. Boshqa tomondan esa, murakkab parollardan foydalanish va ularni turli eltuvchilarda saqlash (masalan, qog‘ozda qayd etish) esa, ushbu muammoni yanada oshirib yuboradi. Bu misollar inson omil tufayli turli joylar va holatlarda xavfsizlik muammolari kelib chiqishi mumkinligini ko’rsatadi. Inson omili tufayli yuzaga keladigan xavfsizlik muammolariga ko‘plab misollar keltirish mumkin. Biroq, keltirilgan holatlardagi eng muhim jixat shundaki, xavfsizlik nuqtai nazaridan “tenglamadan” inson omilini olib tashlash zarur. Boshqacha aytganda, inson omili ishtirok etmagan tizimlar ishtirok etgan tizimlarga nisbatan xavfsizroq bo‘ladi.

Inson omili sababli yuzaga keladigan kiber tahdidlar va ularni oldini olish choralari

1-Jadval

Kiber tahdid turi	**Sababi (inson omili)**	**Oldini olish choralari**	**Amaliy misol**
Parol va utentifikatsiya xavfsizligi	Kuchsiz parollar, bir xil parollardan foydalanish	Kuchli parol siyosati, ikki faktorli autentifikatsiya	Xodimning paroli buzilib, tizimga ruxsatsiz kirish
Ijtimoiy muhandislik (Phishing)	Elektron pochta xabarlarini aniqlay olmaslik, xabardorlik yetishmasligi	Treninglar, phishing testlar, xodimlar xabardorligi	Xodim nohaq linkni bosib, ma'lumot oshkor qilinadi
Noto‘g‘ri tizim konfiguratsiyasi	Texnik bilim yetishmasligi, e'tiborsizlik	Tizimlarni tekshirish, xavfsizlik standartlarini qo‘llash	Firewall noto‘g‘ri sozlangan, tizimga kirish osonlashadi
Ichki xakerlar (insider threats)	Xodimning nojo‘ya niyati yoki qobiliyatsizligi	Monitoring, ruxsatlarni cheklash, ichki audit	Xodim ma'lumotlarni ruxsatsiz ko‘chiradi yoki yo‘q qiladi
Shaxsiy qurilmalar orqali tahdidlar	Xodim qurilmalari xavfsiz emas	BYOD siyosati, antivirusva shifrlash, ma'lumotlarni himoya qilish	*Xodimning telefonidan tizimga virus tushadi*

Ma'lumotlarni himoya qilishning asosiy tamoyillari

2-Jadval

Tamoyil	Tansifi	Amaliy usullar
Maxfiylik (Confidentiality)	Ma'lumotlarga ruxsatsiz kirishni oldini olish	Shifrlash, foydalanuvchi autentifikatsiyasi, kirishni nazorat qilish
Yaxlitlik (Integrity)	Ma'lumotlar o'zgarmasligi va ishonchliligi	Raqamli imzolar, log yozuvlari, checksum tekshiruvlari
Mavjudlik (Availability)	Ma'lumotlarga kerak bo'lgan vaqtda yetib borish imkoniyati	Zaxira nusxalari, serverlarning uzluksiz ishlashi, DRP (Disaster Recovery Plan)

Xulosa: Kiberxavfsizlikda ma'lumotlarni himoya qilish va inson omilini boshqarish bir-birini to'ldiruvchi asosiy tarkibiy qismlardir. Faqat texnologik vositalardan foydalanish yetarli emas; xodimlar bilimli, ehtiyotkor va mas'uliyatli bo'lishi, shuningdek muntazam trening va monitoringlar tashkil etilishi zarur.

O'zbekiston kontekstida milliy kiberxavfsizlik strategiyasi va qonuniy hujjatlar bu yo'nalishdagi faoliyatni tartibga soladi. Kiberhujumlardan samarali himoya qilish va axborot tizimlarining barqaror ishlashini ta'minlash uchun inson omilini e'tiborsiz qoldirmaslik kerak.

Adabiyotlar ro'yxati:

1. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria (1991) Luxembourg: Office for Official Publications of the European Communities, 1991 ISBN 92-826-3004-8, Catalogue Number: CD-71-91-502-EN-C © ECSC-EEC-EAEC, Brussels • Luxembourg.
2. National Information Systems Security (InfoSec) Glossary (2000) National Security Telecommunications and Information Systems Security Committee. National Security Agency US.
3. Pfleeger, C.P. (1997) Security in Computing. Second Edition, Prentice Hall, Upper Saddle River.
4. Guttman, B. and Roback, E. (1995) An Introduction to Computer security: The NIST Handbook. DIANE Publishing. http://dx.doi.org/10.6028/NIST.SP.800-12
5. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
6. Purdy G. ISO 31000: 2009—setting a new standard for risk management //Risk Analysis: An International Journal. – 2010. – T. 30. – №. 6. – C.

7. https://csec.uz/uz/company/staff/
8.https://infocom.uz/articles/kiberxavfsizlik-va-shaxsiy-malumotlarni-himoyalash.
9. https://www.opencloud.uz/uz/services/security/soc
10. https://www.fake.cyber102.uz/