KIBERXAVFSIZLIK ASOSLARI : SHAXSIY MA'LUMOTLARNI HIMOYA QILISH.

SAMINJONOVA SARVINOZXON JAHONGIR QIZI
XORIJIY FILOLOGIYA FAKULTETINING -KURS TALABASI
*MUALLIM:**JAMOLIDDIN XUDOYBERDIYEV***

Annotatsiya. Bu maqolada telekommunikatsiya tarmoqlari va aloqa kanallaridagi tezkor-qidiruv tadbirlaritizimining kiberxavfsizligini ta'minlash alohida qonunchilik hujjatlarida belgilangan tartibda amalga oshirilishi ,kiberxavfsizlik sohasini tartibga solishga nisbatan yondashuvlar, shaxsiy ma'lumotlarni buzilishi, o'g'irlanishi va boshqa zararli harakarlarga qarshi choralar yoritib berilgan . Turli xil ko'rsatmalar , eslatmalar, to'g'ri va aniq ma'lumotlar orqali shaxsiy ma'lumotlarni himoya qilish ko'rsatilgan.

Kalit so'zlar.Kiberxavfsizlik, kiberjinoyatcgilik, kibermakon, kibertahdid, kiberhujum, shaxsiy ma'lumot, NIST Privacy Framework

Kirish.Kiberxavfsizlik tizimlarida shaxsiy ma'lumotlarni himoya qilish bugungi raqamli davrning eng muhim masalalaridan biridir. Axborotning qiymati oshgani sayin uni noqonuniy qo'lga kiritish, o'zgartirish yoki tarqatishga qaratilgan tahdidlar ham kuchaymoqda. Bu jarayonda xalqaro standardlar va ilmiy manbalar shaxsiy ma'lumotlarni to'g'ri boshqarish himoya qilish hamda risklarni baholashda muhim o'rin tutadi.

Mavzuga oid adabiyotlar tahlili. Kiberjinoyatchilik axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarni ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig'indisidir

NIST tomonidan ishlab chiqilgan Privacy Framework shaxsiy ma’lumotlarga oid risklarni aniqlash va boshqarishga yo’naltirilgan tizimli yondashuvni taklif etadi. Ushbu ramka tashkilotlarga ma’lumotlarni to’lashdan tortib, ularni qayta ishlash va saqlashgacha bo’lgan barcha bosqichlarda xavflarni minimallashtirish, jarayonni shaffof qilish hamda foydalanuvchilar xuquqlarini ta’minlash imkonini beradi. Shu bilan birga, NIST SP 800-122 hujjati shaxsni aniqlovchi ma’lumotlarni tasniflash, zaifliklarni toppish, shifrlash, audit va nazorat jarayonlarini to’g’ri yo’lga qo’yishni o’rgatadi

Yevropa Ittifoqining GDPR qonuni esa global miqyosda ma’lumotlarni himoya qilish standardlariga kuchli ta’sir o’tgazgan normative hujjat hisoblanadi. Unda foydalanuvchilarning shaxsiy ma’lumotlar ustidan nazoratni ta’minlash, “foydalanuvchi roziligi “, “unutish huquqi”, “ma’lumotlarni portativligi” kabi tamoyillar aniq belgilangan. Ko’plab davlatlar va kompaniyalar o’z siyosatlarini aynan GDPR talablari asosida qayta ko’rib chiqmoqda.

Shuningdek, xalqaro standardlar orasida ahamiyatga ega bo’lib axborot xavfsizligi boshqarish tizimini (ISMS) yaratish va rivojlantirish bo’yicha to’liq metodologiyani o’z ichiga oladi. Standard talabalarida foydalanish tashkilotlarga ma’lumotlarni himoya qilish bo’yicha doimiy monitoring, risklarni baholash va texnik hamda tashkiliy choralarni uyg’unlashrish imkonini beradi.

Ilmiy adabiyotlar Ichida Ross Andersonning “Security Engineering “ asari kiberxavfsizlik tizimlari qanday loyihalanishi, qanday xatoliklar va zaifliklar paydo bo’lishi mumkinligini chuqur tahlil qiladi. U real dunyodagi misollar orqali xavfsizlik tamoyillarini amaliy ko’rsatadi. Matthew Bishopning “Computer Security : Art and Science “ darsligi esa kiberxavfsizlikning nazariy asoslarini, algoritmlar, mantiqiy modellar va himoya mexanizmlarining matematik poydevorini yoritadi. Dieter Gollmanning ishlari esa kompyuter xavfsizligi bo’yicha asosiy tushunchalar,

protokollar va amaliy mexanizmlar bo'yicha mustahkam o'quv plarformasini taklif etadi.

Raqamli dunyoda shaxsiy ma'lumotlar eng qimmat resurslardan biriga aylangan. Internet, mobil ilovalar, ijtimoiy tarmoqlar va bulutli xizmatlardan foydalanishda inson o'zining katta hajmdagi ma'lumotlarni onglidek ulashadi. Kiberxavfsizlikning asosiy vazifalaridan biri – ushbu ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlashdir. Ushbu bo'limda yetakchi mutaxassislar – Ross Anderson, Bruce Schneier, Niels Ferguson hamda Kevin Mitnick asarlarida ilmiy va amaliy qarashlar asosida ilmiy va amaliy qarashlar asosida shaxsiy ma'lumotlarni himoya qilish prinsiplari yoritiladi.

Shaxsiy ma'lumotlar quyidagilarni o'z ichiga oladi:

Ism,familiya va otasining ismi

Manzil va telefon raqamlari

E-mail manzil

Ijtimoiy tarmoqlarlardagi profil ma'lumotlari

Moliyaviy ma'lumotlar (bank hisob raqamlari, kredit kartasi ma'lumotlari) Bu ma'lumotlar juda nozikdir va agar to'g'ri himoyalanmasa, kiber jinoyatchilar tomonidan osonlik bilan o'g'rilanishi yoki manipulatsiya qilinishi mumkin.

Shaxsiy ma'lumotlarni ximoya qilish bo'yicha tafsiyalar :

Murakkab parollarni tanlash: har bir hisob uchun noyob va kuchli parollardan foydalanish. Parolda katta va kichik harflar,raqamlar va maxsus belgilar bo'lishiga harakat qilish.

Ikki Faktorli Avtorizatsiya: mavjud bo'lgan ikki faktorli autentifikatsiyani yoqish. Bu, qo'shimcha xavfsizlik bosqichi bo'lib, sizga parol bilan bir qatorda qo'shimcha tekshirishni taqdim etadi.

Ma'lumotlarni Shirflash: maxsus ma'lumotlarni ijtimoiy tarmoqlarda ochiq joylamaslik. Sifatida confidentiality uchun maxsus sozlamalar o'rnatish.

Hisobni muntazam tekshirib turish: ba'zan hisobotlarni tekshirib chiqish, shuningdek, qachonki shubhali faoliyatni ko'rganda darhol hisobot berish.

Ma'lumotlarni yangilab turish: har doim dastur va qurilmalar yangilanishlarini o'rnatib boorish,chunki bu sizning xavfsizlik darajangizni oshiradi.

Shaxsiy ma'lumotlarni himoya qilish — zamonaviy insonning eng muhim vazifalaridan biri. Texnologiyalar rivojlanishi bilan xavflar ham kuchayib bormoqda. Ross Andersonning tizim xavfsizligi haqidagi ilmiy qarashlari, Schneier va Fergusonning kriptografiya bo‘yicha fundamental yondashuvlari hamda Kevin Mitnickning amaliy maslahatlari shaxsiy ma'lumotlarni himoya qilishning mukammal tizimini yaratishda asosiy tayanch sifatida xizmat qiladi.

Kiberxavfsizlik — bu faqat texnik himoya emas, balki ongli yondashuv, muntazam profilaktika, xavfni oldindan ko‘ra bilish va axborot bilan mas'uliyatli munosabatdir. Shu tamoyillarga amal qilgan har bir foydalanuvchi o‘z ma'lumotlarini yo‘qotish, buzilish yoki sizdirilish xavfidan samarali himoya qilishi mumkin.

ADABIYOTLAR RO'YXATI

1. P.W. Singer & Allan Friedman — Cybersecurity and Cyberwar: What Everyone Needs to Know

2. Sherri Davidoff & Jonathan Ham — Network Forensics: Tracking Hackers Through Cyberspace

3. Matt Bishop — Computer Security: Art and Science

4. Gene Spafford, Simson Garfinkel & Alan Schwartz — Practical Unix and Internet Security

5. Michael Howard & Steve Lipner — The Security Development Lifecycle

6. Christopher Hadnagy — Social Engineering: The Science of Human Hacking

7. Jon Erickson — Hacking: The Art of Exploitation

8. NIST — Special Publication 800 Series (SP 800-53, SP 800-30, SP 800-63 va boshqalar)