DOI: https://doi.org/10.5281/zenodo.14520823

IJTIMOIY INJINERIYA VA UNI HOZIRGI KIBERJINOYATCHILIKDAGI AHAMIYATI

Mirzayev Tolibjon To‘raqul o‘g‘li
Buxoro viloyat hokimining raqamlashtirish bo‘yicha maslahatchisi.

ANNOTASIYA:

Hayotda ko‘plab jabhalarda ijtimoiy injineriyaga tegishli muammolarni ko‘rish mumkin. Ijtimoiy injineriya bilan bog‘liq tahdidlar bugingi kunning dolzarb muammosi hisoblanadi. Maqolada ijtimoiy injineriya va uni hozirgi kiberjinoyatchilikdagi ahamiyati, undan himoyalanish usullari haqida ma’lumot berilgan.

Kalit so‘zlar

Ijtimoiy injineriya, fizik xavfsizlik, ma’lumotla, ilovalar, kompyuterlar, ichki tarmoq, tarmoq perimetri, fishing, fribgarlik, tahdid.

ABSTRACT

The problems of social engineering can be seen in many aspects of life. Threats related to social engineering are an urgent problem today. The article provides information about social engineering and its importance in modern cybercrime, as well as ways to protect against it.

Keywords

Social engineering, physical security, information, applications, computers, intranet, network perimeter, phishing, fraud, threats.

Ijtimoiy (sotsial) injineriya - turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish. Maxfiy ma’lumotlar – foydalanuvchi ismi/parollari, shaxsiy ma’lumotlari, ayblov dalillari, bank karta raqamlari va moliyaviy yoki obro‘sini yo‘qotadigan har qanday ma’lumot.

Ijtimoiy injineriya bilan bog‘liq tahdidlarni quyidagicha tasniflash mumkin:

Telefon bilan bog‘liq tahdidlar. Telefon hanuzgacha tashkilotlar ichida va ular o‘rtasidagi aloqaning eng keng tarqalgan usullaridan biri hisoblanadi. Shuning uchun, u sotsial injineriya uchun samarali vosita bo‘lib qolmoqda. Telefonda

gaplashayotganda, suhbatdoshining shaxsini tasdiqlashning imkoni yo‘q. Bu hujumchilarga xodimning, xo‘jayinning maxfiy yoki muhim tuyuladigan ma’lumotlarga ishonishi mumkin bo‘lgan har qanday shaxsning o‘rnida bo‘lish imkonini beradi. Mazkur hollarda quyidagi xavfsizlik choralarini amalga oshirish talab etiladi: telefon qiluvchining shaxsini aniqlash; raqamni aniqlash xizmatidan foydalanish; SMS – xabardagi noma’lum havolalarga e’tibor bermaslik.

Elektron pochta bilan bog‘liq tahdidlar. Ko‘pgina xodimlar har kuni korporativ va shaxsiy pochta tizimlaridan o‘nlab, hatto yuzlab elektron pochta xabarlarini qabul qilishadi. Albatta, bunday yozishmalar oqimining har bir harfiga yetarlicha e’tibor berishning imkoni yo‘q. Bu esa hujumlarni amalga oshirishni sezilarli darajada osonlashtiradi. Elektron pochta tizimlarining ko‘plab foydalanuvchilari bunday holni bir papkadan ikkinchisiga qog‘ozlarni o‘tkazishning elektron analogi sifatida qabul qilishadi va xabarlarni qabul qilishda xotirjam bo‘lishadi. Tajovuzkor pochta orqali oddiy so‘rov yuborganida, uning qurboni ko‘pincha uning xatti-harakatlari haqida o‘ylamasdan ular so‘ragan ishni bajaradi. Elektron pochtalarda xodimlarni korporativ atrof-muhit muhofazasini buzishga undaydigan giperhavolalar bo‘lishi mumkin. Bunday havolalar har doim ham da’vo qilingan sahifalarga murojaat qilmaydi.

Xavfsizlik choralarining aksariyati ruxsatsiz foydalanuvchilarning korporativ resurslardan uchun ishlab chiqilgan. Buzg‘unchi tomonidan yuborilgan giperhavolaga murojaat orqali foydalanuvchining zararli dasturni korporativ tarmoqqa yuklashi ko‘plab himoya turlarini chetlab o‘tishga imkon beradi. Giperhavola, shuningdek, ma’lumot yoki yordamni talab qiladigan qalqib chiquvchi ilovalar bilan turli xostlarga murojaatni talab qilishi mumkin.

Firibgarlikni va zararli hujumlarni oldini olishning eng samarali usuli kutilmagan foydalanuvchining elektron pochtasi xabarlariga shubha bilan qarash.

Ushbu yondashuvni butun tashkilotda tarqatish uchun xavfsizlik siyosatida belgilangan elektron pochtadan foydalanishning quyidagi elementlari kiritilishi kerak: hujjatlarga qo‘shimchalar; hujjatdagi giperhavolalar shaxsiy yoki korporativ ma’lumotlarni kompaniya ichida so‘rash; shaxsiy yoki korporativ ma’lumotlarga kompaniya tashqarisidan keladigan so‘rovlar.

Tezkor xabarlardan foydalanishga asoslangan tahdidlar. Tezkor xabar almashish - ma’lumotlarni uzatishning nisbatan yangi usuli. Ammo, u korporativ foydalanuvchilar orasida allaqachon mashhurlikka erishgan. Foydalanishning tezligi va qulayligi tufayli ushbu aloqa usuli turli xil hujumlar uchun keng imkoniyatlarni ochib beradi. Foydalanuvchilar unga telefon kabi qarashadi va uni bo‘lishi mumkin bo‘lgan dasturiy tahdidlar sifatida baholashmaydi. Tezkor xabarlar xizmatidan foydalanishga asoslangan hujumlarning ikkita asosiy turi - zararli dasturga havola va

dasturning o‘zi haqida xabarning ko‘rsatilishi hisoblanadi. Tezkor xabarlar xizmatlarining xususiyatlaridan biri - aloqaning norasmiyligi, unda har qanday nomlarni moslashtirish qobiliyati bilan bir qatorda, bu omil tajovuzkorni o‘zini boshqa odam bo‘lib ko‘rsatishiga imkon beradi. Bu esa muvaffaqiyatli hujum qilish ehtimolini sezilarli darajada oshiradi. Agar kompaniya tezkor xabarlar sababli keladigan xarajatlarni kamaytirish maqsadida boshqa afzalliklardan foydalanmoqchi bo‘lsa, korporativ xavfsizlik siyosatida tegishli tahdidlardan himoya qilish mexanizmlarini ta’minlashi kerak. Korporativ muhitda tezkor xabar almashish ustidan ishonchli boshqaruvga ega bo‘lish uchun quyidagi talablar bajarilishi shart: tezkor xabarlar uchun bitta platformani tanlash; tezkor xabar yuborish xizmatini o‘rnatishda xavfsizlik sozlamalarini aniqlash; yangi aloqalarni o‘rnatish prinsiplarini aniqlash; parol tanlash standartlarini o‘rnatish; tezkor xabarlardan foydalanish bo‘yicha tavsiyalar berish.

Sotsial injineriya mutaxassislari tashkilotlar uchun quyidagi asosiy himoya usullarini qo‘llashni tavsiya etishadi: muhim ma’lumotlar ko‘rinishida bo‘lgan, zararsiz ko‘rinadigan ma’lumot turlarini hisobga oladigan ishonchli ma’lumotlarni tasniflash siyosatini ishlab chiqish; ma’lumotlarni shifrlash yoki foydalanishni boshqarish yordamida mijoz ma’lumotlari xavfsizligini ta’minlash; xodimlarni sotsial injineriya ko‘nikmalariga o‘rgatish, ularni o‘zlari tanimaydigan odamlar bilan muloqotiga shubha bilan qarashni o‘rgatish; xodimlar orasida parollarni almashishni yoki umumiy foydalanishni taqiqlash; shaxsan tanish bo‘lmagan yoki biron – bir tarzda tasdiqlanmagan shaxsga korxonaga tegishli ma’lumotlarni berishni taqiqlash; maxfiy ma’lumotlardan foydalanishni so‘raganlar uchun maxsus tasdiqlash muolajalaridan foydalanish.

Sotsial injineriya hujumlarini oldini olishda ko‘p hollarda kompaniyalar tomonidan murakkab, ko‘p darajali xavfsizlik tizimlari qo‘llaniladi. Bunday tizimlarning ba’zi xususiyatlari va majburiyatlari quyida keltirilgan:

- Fizik xavfsizlik. Kompaniya binolari va korporativ resurslardan foydalanishni cheklaydigan to‘siqlar. Unutmaslik kerakki, kompaniyaning resurslari, masalan, kompaniya hududidan tashqarida joylashgan axlat konteynerlari fizik himoyalanmagan.
- Ma’lumotlar. Biznes ma’lumotlari: qayd yozuvlari, pochta va boshqalar bo‘lib, tahdidlarni tahlillash va ma’lumotlarni himoya qilish choralarini rejalashtirishda qog‘oz, elektron ma’lumot eltuvchilari bilan ishlash prinsiplarini aniqlash kerak.
- Ilovalar - foydalanuvchilar tomonidan boshqariladigan dasturlar. Atrofini himoya qilish uchun elektron pochta dasturlaridan, tezkor xabarlar xizmati va boshqa dasturlardan tajovuzkorlar qanday foydalanishlari mumkinligini ko‘rib chiqish kerak.

- Kompyuterlar. Korporativ kompyuterlarda qaysi dasturlardan foydalanish mumkinligini ko‘rsatadigan qat’iy prinsiplarni belgilash, foydalanuvchilar kompyuterlariga to‘g‘ridan-to‘g‘ri hujumlardan himoya qilish.
- Ichki tarmoq. Korxona tizimlariga ta’sir qiladigan tarmoq, u mahalliy, global yoki simsiz bo‘lishi mumkin. So‘nggi yillarda masofadan ishlaydigan usullarning ommaviylashi sababli, ichki tarmoqlarning chegaralari sezilarli darajada o‘zboshimchalik bilan kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilishda nima qilish kerakligini tushunishlari lozim.
- Tarmoq perimetri. Kompaniyaning ichki tarmoqlari va tashqi, masalan, Internet yoki hamkor tashkilotlar tarmoqlari o‘rtasidagi chegara.

Sotsial injineriyaga tegishli ko‘plab hujumlar mavjud, quyida ularning ayrimlari keltirilgan:

Fishing. Fishing (ing. Phishing – baliq ovlash) Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan (login/parol) foydalanish imkoniyatiga ega bo‘lish. Bu hozirda keng tarqalgan sotsial injineriya sxemalaridan biri hisoblanadi. Katta hajmdagi shaxsiy ma’lumotlarni keng tarqalishi, fishing “shamolisiz” amalgaoshmaydi. Fishingning eng keng tarqalgan namunasi sifatida jabrlanuvchining elektron pochtasiga yuborilgan rasmiy ma’lumot ko‘rinishidagi bank yoki to‘lov tizimining soxta xabarini ko‘rsatish mumkin.

Quyida keng tarqalgan fishing sxemalariga misollar keltirilgan. Mavjud bo‘lmagan havola. Fishing hujumining mazkur turida biror web saytga o‘xshash web saytga murojaat amalga oshirilishi tavsiya etiladi. Masalan, www.PayPai.com manzilini www.PayPal.com manzili sifatida yuborish mumkin. Bu holda kamdan-kam holda foydalanuvchilar “l” harfini o‘riniga “i” harfi borligiga e’tibor berishadi.
Havolaga murojaat qilinganida esa www.PayPal.com web saytga o‘xshash, biroq soxta web saytga tashrif buyuriladi va talab kiritilgan to‘lov kartasi ma’lumotlari kiritiladi. Natijada, kiritilgan ma’lumotlar xaker qo‘liga tushadi. Bunga yaqqol misol sifatida, 2003 yilda eBay foydalanuvchilariga tarqalgan fishing xabarni keltirish mumkin. Mazkur xabarda foydalanuvchilarning akkauntlari blokirovkalangani va kredit karta ma’lumotlari blokirovkadan chiqarilishi kerakligi keltirilgan va unda rasmiy web-saytga o‘xshash soxta web saytga olib boruvchi havola mavjud bo‘lgan. Ushbu fishing hujumining keltirgan zarari bir necha yuz ming dollarga teng bo‘lgan.

Taniqli korporativ brendidan foydalanishga asoslangan firibgarlik. Firibgarlikning mazkur ko‘rinishida taniqli yoki yirik kompaniyalar nomidan foydalanuvchiga xabar yuboriladi. Xabarda kompaniya tomonidan o‘tkazilgan biror tanlovda g‘alaba qozonilganligi haqidagi tabriklar bo‘lishi mumkin. Unda shuningdek, zudlik bilan qayd yozuvi ma’lumotlari va parolni o‘zgartirish kerakligi so‘raladi.

Shunga o‘xshash sxemalar texnik ko‘maklashish xizmati nomidan ham amalga oshirilishi mumkin.

Soxta lotareyalar. Mazkur fishing sxemasiga ko‘ra foydalanuvchi har qanday taniqli kompaniya tomonidan o‘tkazilgan lotereyada g‘olib bo‘lgani to‘g‘risidagi xabarni olishi mumkin. Tashqi tomondan, bu elektron xabar kompaniyaning yuqori lavozimli xodimlaridan biri nomidan yuborilganga o‘xshaydi.

Soxta antivirus va xavfsizlik dasturlari. Mazkur dasturlar firibgar dasturiy ta‘minoti yoki “chaqqon dastur” deb nomlanib, ular antivirus dasturlariga o‘xshasada, vazifasi boshqacha. Bu dasturiy ta’minot turli tahdidlar to‘g‘risidagi yolg‘on xabarnomalar asosida foydalanuvchini soxta bitimlarga jalb qilishga harakat qiladi. Foydalanuvchi ulardan foydalanganida elektron pochtada, onlayn e’lonlarda, ijtimoiy tarmoqlarda, qidiruv tizimlari natijalarida va hatto foydalanuvchi kompyuterida turli qalqib chiquvchi oynalarga duch kelishi mumkin.

IVR (Interactive Voice Response) yoki telefon orqali fishing. Fishing sxemasining mazkur usuli oldindan yozib olingan xabarlar tizimidan foydalanishga asoslangan, ular bank va boshqa IVR tizimlarining “rasmiy qo‘ng‘iroqlari”ni qayta tiklash uchun ishlatiladi. Bu hujumda jabrlanuvchi bank bilan bog‘lanib, qandaydir ma’lumotlarni tasdiqlash yoki yangilash kerakligi haqidagi so‘ovni qabul qiladi. Tizim PIN kodni yoki parolni kiritish orqali foydalanuvchi tasdig‘ini talab qiladi. Natijada, muhim ma’lumotlarni qo‘lgan kiritgan buzg‘unchi foydalanuvchi ma’lumotlaridan foydalanish imkoniyatiga ega bo‘ladi. Masalan, parolni almashtirish uchun “1” ni bosing va operator javobini olish uchun “2” ni bosing.

Preteksting. Mazkur fishing sxemasida xaker o‘zini boshqa shaxs sifatida ko‘rsatadi va oldindan tayyorlangan senariy (skript) bo‘yicha maxfiy axborotni olishni maqsad qiladi. Ushbu hujumda qurbonni shubhalanmasligi uchun tegishli tayyorgarlik ko‘riladi: tug‘ilgan kun, INN, pasport raqami yoki hisob raqamining oxirgi belgilari kabi ma’lumotlar topiladi. Ushbu fishing sxemasi odatda telefon yoki elektron pochta orqali amalga oshiriladi.

Kvid pro kvo (lotinchadan: Quid pro quo). Ushbu ibora ingliz tilida “xizmat uchun xizmat” degan ma’noni anglatib, sotsial injineriyaning mazkur turida xaker korporativ tarmoq yoki elektron pochta orqali kompaniyaga murojaatni amalga oshiradi. Ko‘pincha xaker o‘zini texnik xizmat ko‘rsatuvchi sifatida tanitib, texnik xodimning ish joyidagi muammolarni bartaraf etishda “yordam berishini” aytadi. Texnik muammoni “bartaraf” etish vaqtida nishondagi shaxsni buyruqlarni bajarishga yoki jabrlanuvchining kompyuteriga turli xil dasturlarni o‘rnatishga undash amalga oshiriladi. Masalan, 2022 yilda Axborot xavfsizligi dasturi doirasida o‘tkazilgan tadqiqot ofis xodimlarining 90% har qanday xizmat yoki to‘lov uchun maxfiy ma’lumotlarni, masalan, o‘zlarining parollarini, berishga tayyor bo‘lishini ko‘rsatdi.

Yo‘l-yo‘lakay olma. Sotsial injineriyaning mazkur usulida xaker maxsus zararli dastur yozilgan ma’lumot eltuvchilardan foydalanadi va zararli dasturlar yozilgan eltuvchilarni qurbonning ish joyi yaqinida, jamoat joylarida va boshqa joylarda qoldiradi. Bunda, ma’lumot eltuvchilari tashkilotga tegishli shaklda rasmiylashtiriladi. Masalan, xaker biror korporatsiya logotipi va rasmiy web-sayt manzili tushirilgan kompakt diskni qoldirib ketadi. Ushbu disk “Rahbarlar uchun ish haqlari” nomi bilan nomlanishi mumkin. Ushbu eltuvchini qo‘lga kiritgan qurbon uni o‘z kompyuteriga qo‘yib ko‘radi va shu orqali kompyuterini zararlaydi.

Ochiq ma’lumot to‘plash. Sotsial injineriya texnikasi nafaqat psixologik bilimlarni, balki, inson haqida kerakli ma’lumotlarni to‘plash qobilyatini ham talab etadi. Bunday ma’lumotlarni olishning nisbatan yangi usuli ochiq manbalardan, ijtimoiy tarmoqlardan to‘plash. Masalan, «Одноклассники», «ВКонтакте», «Facebook», «Instagram» kabi saytlarda odamlar yashirishga harakat qilmaydigan juda ko‘p ma’lumotlar mavjud.

Yelka orqali qarash. Ushbu hujumga ko‘ra buzg‘unchi jabrlanuvchiga tegishli ma’lumotlarini uning yelkasi orqali qarab qo‘lga kiritadi. Ushbu turdagi hujum jamoat joylarida, masalan, kafe, avtobus, savdo markazlari, aeroport va temir yo‘l stansiyalarida keng tarqalgan. Mazkur hujumga doir olib borilgan so‘rovnomalar quyidagilarni ko‘rsatgan: 85% ishtirokchilar o‘zlari bilishlari kerak bo‘lmagan maxfiy ma’lumotlarni ko‘rganliklarini tan olishgan; 82% ishtirokchilar ularning ekranidagi ma’lumotlarini ruxsatsiz shaxslar ko‘rishi mumkinligini tan olishgan; - 82% ishtirokchilar tashkilotdagi xodimlar o‘z ekranini ruxsatsiz odamlardan himoya qilishiga ishonishmagan.

Teskari sotsial injineriya. Jabrlanuvchining o‘zi tajovuzkorga ma’lumotlarini taqdim qilishi teskari sotsial injineriyaga tegishli holat hisoblanadi. Bu bir qarashda ma’noga ega bo‘lmagan qarash hisoblansada, aksariyat hollarda jarblanuvchining o‘zi muammolarini hal qilish uchun tajovuzkorni yordamga jalb qiladi. Masalan, jabrlanuvchi bilan birga ishlovchi tajovuzkor jabrlanuvchi kompyuteridagi biror faylni nomini o‘zgartiradi yoki boshqa katalogga ko‘chirib o‘tkazadi. Faylni yo‘q bo‘lganini bilgan qurbon esa ushbu muammoni tezda bartaraf etishni istab qoladi. Bu vaziyatda tajovuzkor o‘zini ushbu muammoni bartaraf etuvchi sifatida ko‘rsatadi va qurbonning muammosini bartaraf etish bilan birga unga tegishli login/ parolni ham qo‘lga kiritadi. Bundan tashqari, ushbu vazifasi bilan tajovuzkor tashkilot ichida obro‘ga ega bo‘ladi va o‘z qurbonlari sonini ortishiga erishadi. Bu holatni aniqlash esa ancha murakkab ish hisoblanadi.

Mashhur sotsial injinerlar. Kevin Mitnik tarixdagi eng mashhur sotsial injinerlardan biri, u dunyodagi mashhur kompyuter xakeri, xavfsizlik bo‘yicha mutaxassis va sotsial injineriyaga asoslangan kompyuter xavfsizligiga bag‘ishlangan

ko‘plab kitoblarning ham muallifidir. Uning fikriga ko‘ra xavfsizlik tizimini buzishdan ko‘ra, aldash yo‘li orqali parolni olish osonroq.

Sotsial injineriyadan himoyalanish choralari. Hujumlarni amalga oshirishda sotsial injineriya texnikasidan foydalangan tajovuzkorlar tez-tez muloyimlik, dangasalik, xushmuomilalik bilan foydalanuvchi va tashkilot xodimlarining qiziqishlaridan foydalanadilar. Hujumlarni oldini olish esa, xodimlarning aldanayotganliklarini bilmasliklari sababli, murakkab hisoblanadi.

Sotsial injineriya hujumlarini quyidagicha aniqlash mumkin: o‘zini do‘stingiz yoki yordam so‘rab murojaat qilgan yangi xodim sifatida tanishtirish; o‘zini yetkazib beruvchi, hamkor kompaniyaning xodimi yoki qonun vakili sifatida tanishtirish; o‘zini biror rahbar sifatida tanishtirish; biror zaiflikni bartaraf etuvchi yoki jabrlanuvchiga biror nimani yangilash imkoniyatini taqdim qiluvchi sotuvchi yoki ishlab chiqaruvchi sifatida tanishtirish; muammo yuzaga kelganida yordam beruvchi sifatida tanishtirish; ishonchni hosil qilish uchun ichki xotirjamlik va terminologiyadan foydalanish; “maktub”ga turli zararli dasturlarni qo‘shib yuborish; soxta ochilgan oynada login/ parolni qayta kiritishni so‘rash; foydalanuvchi nomi va paroli bilan saytga ro‘yxatdan o‘tish uchun biror sovg‘a taklif etish; jabrlanuvchi kompyuteriga yoki dasturiga kiritilgan kalitlarni yozib olish (keylogger dasturlari); turli xil zararli dasturiy vositaga ega ma’lumot eltuvchilarini foydalanuvchi stoliga tashlash; turli qo‘ng‘iroqlardagi ovozli xabarlar va h.

FOYDALANILGAN ADABIYOTLAR

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma, – T. “Nihol print” OK, 2021. – 224 b.
2. Imamova Shafoat Mahmudovna. A SIMULATION TRAINER'S EDUCATIONAL COMPETENCE IN THE PROCESS OF FORMING STUDENTS' PROFESSIONAL COMPETENCE// INTERNATIONAL JOURNAL ON INTEGRATED EDUCATION Volume 6, Issue 9, Sep- 2023 P.75-77.
3. Imomova Shafoat Mahmudovna. TALABALARNING KASBIY KOMPETENSIYALARINI RIVOJLANTIRISHGA YANGICHA YONDASHUVLAR// Educational Research in Universal Sciences. VOLUME 2, SPECIAL ISSUE 14, 2023, C.1075-1081
4. Imamova Sh.M. Methodology of Development of Programming Skills in Mathematical Systems in Students Based on Computer Simulation Trainers// NATURALISTA CAMPANO Volume 28 Issue 1, 2024, -pp. 551-557.

5. Imomova Shafoat Mahmudovna, Qobilov Komil Hamidovich. Oliy Ta’lim Muassasalarida Masofadan OQitish Jarayonini Takomillashtirish// Miasto Przyszłości, Vol. 31 (2023), C.312-314.

6. Imomova Shafoat Mahmudovna, Norova Fazilat Fayzulloyevna. Ta’lim jarayonlarini raqamli texnologiyalar asosida takomillashtirish// Miasto Przyszłości, Vol. 32 (2023), C.47-49.

7. Imomova Shafoat Mahmudovna. PEDAGOGIK TEXNIKA – KASBIY KOMPETENSIYALARNI RIVOJLANTIRISHNING ASOSIY OMILI SIFATIDA// Pedagogik mahorat. 1 tom. 2- son (2024 yil, fevral),2024, C. 56-59.

8. S.K. Ganiev, Z.T. Xudoykulov, N.B. Nasrullaev. Основы кибербезопасности: Учебное пособие, – T. “Mahalla oila nashriyoti”, 2021. – 224 b.