AXBOROT XAVFSIZLIGINI TA'MINLASHDA TARMOQ HUJUMLARNING TURLARI

ANVARJON ABDUJABBOROVICH MAXKAMOV

O'zbekiston xalqaro islomshunoslik akademiyasi

Zamonaviy axborot-kommunikatsiya

texnologiyalari kafedrasi dotsenti, PhD

mahkamovanvar2020@gmail.com

Annotation. *Ushbu maqolada axborot xavfsizligini ta'minlashda tarmoq hujumlarining turlari va ular qanday amalga oshiriladi, ulardan qanday himiyalanish zarurligi tahlili keltirib o'tilgan.*

Ayni vaqtga kelib har bir tarmoqdan bo'layotgan hujumlarning xavfsizligini ta'minlash hozirgi kundagi eng dolzarb muammolardan biri hisoblanadi. Shuning uchun hozirgi kunda axborot xavfsizligini ta'minlashda tarmoq hujumlarining turlari va ular qanday amalga oshirilishini oldini olish, xavfsizligini ta'minlash keltirib o'tilgan.

Keywords: *tarmoq, hujum, fishing, kiberxavfsizlik, kiber tahdid, axborot xavfsizligi.*

Introduction. *This article analyzes the types of network attacks in ensuring information security, how they are carried out, and how to protect against them.*

Nowadays, ensuring security against attacks from every network is one of the most pressing problems today. Therefore, in ensuring information security today, the types of network attacks and how they are carried out are discussed, as well as ensuring their security.

Keywords: *network, attack, phishing, cybersecurity, cyber threat, information security.*

Аннотация. *В данной статье анализируются типы сетевых атак на обеспечение информационной безопасности, способы их осуществления и методы защиты от них.*

В настоящее время обеспечение безопасности от атак из любой сети является одной из самых актуальных проблем. Поэтому в контексте обеспечения информационной безопасности сегодня рассматриваются типы сетевых атак и способы их осуществления, а также меры по обеспечению безопасности от них.

Ключевые слова: *сеть, атака, фишинг, кибербезопасность, киберугрозы, информационная безопасность.*

KIRISH

Hozirgi vaqtga kelib axborot xavfsizligini ta’minlashda tarmoq hujumlarining turlari va ulardan qanday himoyalanishni amalga oshirish zamonaviy axborot texnologiyalarisiz tasavvur qilib bo‘lmaydi. Shu sababdan butun dunyoda axborotga bo‘lgan talab va extiyoj ham kun sayin ortib bormoqda. Ayniqsa, axborot texnologiyalarining rivojlanib borishi ma’lumotlar xajmining ortib borishiga sabab bo‘lmoqda. Bu esa axborot xavfsizligini ta’minlashda tarmoq hujumlarining turlari va ulardan qanday himoyalanishni ta’minlash yoki himoyalash zarur.

ASOSIY QISM

Tarmoq hujumlari kompyuter tarmoqlari va tizimlariga ruxsatsiz kirish, operatsiyalarni buzish, ma’lumotlarni o‘g‘irlash yoki biron-bir tarzda zarar etkazish uchun mo‘ljallangan zararli harakatlarni anglatadi. Ushbu hujumlar tarmoqning xavfsizligi va yaxlitligini buzish uchun tarmoq infratuzilmasi, dasturiy ta’minot yoki inson xatti-harakatlaridagi zaifliklardan foydalanadi. Tarmoq hujumlari tarmoq ichida turli darajalarda, jumladan, jismoniy qatlam, tarmoq qatlami, transport qatlami va amaliy qatlamda sodir bo‘lishi mumkin.

Tarmoq hujumlari turli shakllarda bo‘lishi mumkin, ularning har biri kompyuter tarmoqlari va tizimlaridagi zaifliklardan foydalanish uchun mo‘ljallangan. Tarmoq hujumlarining ba’zi keng tarqalgan turlarini keltirib o‘tamiz.

Fishing (Phishing). Fishing hujumlari elektron pochta, tezkor xabar almashish yoki zararli veb-saytlar orqali ishonchli shaxs sifatida niqoblash orqali shaxslarni o‘zlarining shaxsiy ma’lumotlarini, masalan, login ma’lumotlari yoki moliyaviy tafsilotlarni oshkor qilish uchun aldashni o‘z ichiga oladi.

Fishing - kiberhujumning bir turi bo‘lib, shaxslarni ishonchli shaxs sifatida niqoblash orqali kirish ma’lumotlari, moliyaviy ma’lumotlar yoki shaxsiy ma’lumotlar kabi maxfiy ma’lumotlarni oshkor etishda aldashdan iborat. Fishing hujumlari odatda elektron pochta orqali sodir bo‘ladi, lekin ular lahzali xabarlar, ijtimoiy media yoki hatto telefon qo‘ng‘iroqlari (vishing deb ataladi) kabi boshqa aloqa kanallari orqali ham sodir bo‘lishi mumkin.

Tarmoqlar kontekstida fishing hujumlarining ba’zi muhim jihatlari:

Elektron pochta fishing: Elektron pochta fishingi fishing hujumining eng keng tarqalgan shaklidir. Hujumchilar banklar, onlayn xizmatlar yoki ishonchli tashkilotlar kabi qonuniy manbalardan kelgan ko‘rinadigan aldamchi elektron pochta xabarlarini yuborishadi. Elektron pochta xabarlari ko‘pincha shoshilinch yoki jozibali xabarlarni o‘z ichiga oladi, ular qabul qiluvchilarni zararli havolalarni bosishga, qo‘shimchalarni yuklab olishga yoki firibgar veb-saytlarga maxfiy ma’lumotlarini kiritishga undaydi.

Spear fishing: Spear fishing hujumlari aniq shaxslar yoki tashkilotlarga qaratilgan yuqori maqsadli fishing urinishlaridir. Buzg‘unchilar fishing xabarlarini shaxsiylashtirish va ularni yanada ishonchli qilish uchun o‘zlarining ismlari, lavozimlari yoki mansubliklari kabi maqsadlari haqida ma’lumot to‘plashadi.

Whaling: Whaling - bu yuqori darajadagi rahbarlar yoki tashkilot ichida muhim vakolatlarga ega bo‘lgan shaxslarga qaratilgan fishing hujumining bir turi. Hujumchilar maxfiy korporativ ma’lumotlarga kirish yoki moliyaviy firibgarlikni amalga oshirish uchun ushbu shaxslarni aldashga harakat qilishadi.

Pharming: Pharming hujumlari tarmoqning DNS (domen nomlari tizimi) ni manipulyatsiya qilish yoki qurbonning kompyuteridagi xostlar faylini o‘zlari bilmagan holda firibgar veb-saytlarga yo‘naltirish uchun o‘zgartirishni o‘z ichiga oladi. Bu jabrlanuvchilarni o‘zlarining nozik ma’lumotlarini taqdim etgan holda qonuniy veb-saytlar bilan o‘zaro aloqada ekanliklariga ishonishadi.

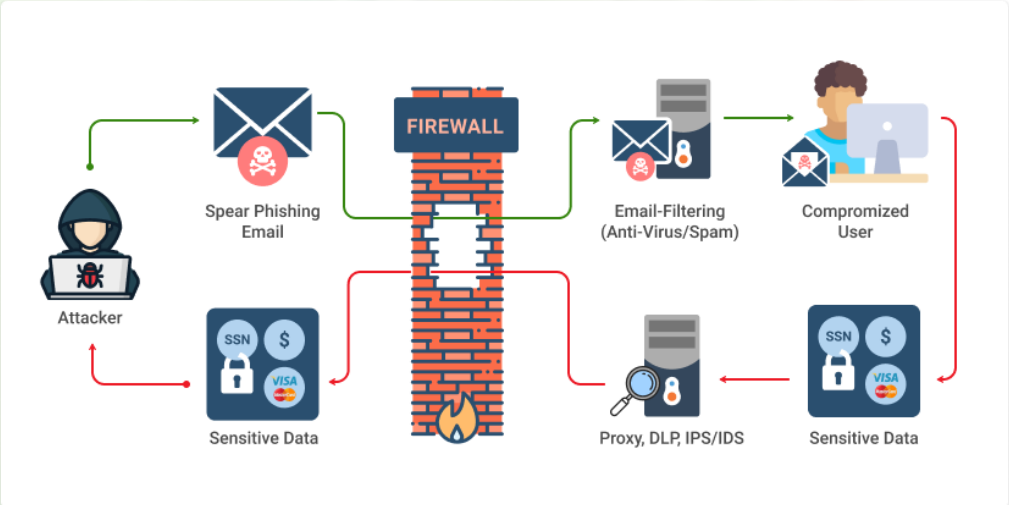
Smishing: Smishing hujumlari matnli xabarlar (SMS) yoki boshqa xabar almashish platformalari orqali sodir bo‘ladi. Buzg‘unchilar foydalanuvchilarni aldab, maxfiy ma’lumotlarni oshkor qilish maqsadida ma’lum bir raqamga

qo‘ng‘iroq qilish bo‘yicha ko‘rsatmalar yoki zararli havolalarni o‘z ichiga olgan yolg‘on xabarlarni yuborishadi.

Angler Phishing: Angler fishingi mashhur ijtimoiy media platformalari yoki veb-saytlarning sharhlar bo‘limlaridan foydalanadigan hujum turidir. Buzg‘unchilar foydalanuvchilarni zararli veb-saytlarga kirishga yoki ularning hisob ma’lumotlarini oshkor qilishga undaydigan soxta havolalar yoki sharhlarni joylashtiradilar.

Credential Harvesting: Credential Harvesting hujumlari ko‘pincha turli onlayn xizmatlar, jumladan elektron pochta hisoblari, ijtimoiy media platformalari, onlayn banking yoki korporativ tizimlar uchun kirish ma’lumotlarini o‘g‘irlashga qaratilgan. Buzg‘unchilar bu o‘g‘irlangan hisob ma’lumotlaridan ruxsatsiz kirish yoki boshqa zararli maqsadlarda foydalanadilar.

Clone fishing: Clone fishing kichik o‘zgarishlar bilan qonuniy elektron pochta yoki veb-saytning deyarli bir xil nusxasini yaratishni o‘z ichiga oladi. Buzg‘unchilar haqiqiy havolalar yoki qo‘shimchalarni zararli havolalar bilan almashtirib, foydalanuvchilarni soxta tarkib bilan o‘zaro aloqada bo‘lish uchun aldashadi.



1-rasm. Fishing turlari

Training and Awareness: Training and Awareness hujumlari insonning zaifligi va aldoviga tayanadi. Tashkilotlar va shaxslar uchun xavfsizlik bo‘yicha xabardorlik dasturlarini amalga oshirish va foydalanuvchilarni fishing urinishlarini

aniqlash va hisobot berish bo‘yicha o‘rgatish uchun muntazam treninglar o‘tkazish juda muhimdir.

Fishing hujumlaridan himoyalanish uchun hushyor bo‘lish va profilaktika choralarini ko‘rish muhimdir. Bularga havolalarni bosish yoki qo‘shimchalarni ochishda ehtiyot bo‘lish, elektron pochta yoki veb-saytlarning qonuniyligini tekshirish, dasturiy ta’minot va xavfsizlik nuqtalarini muntazam yangilash, kuchli va noyob parollardan foydalanish, elektron pochtani filtrlash va fishingga qarshi texnologiyalardan foydalanish kiradi.

Xizmatni rad etish (DoS) (Denial-of-Service (DoS) Attack). Xizmatni rad etish (DoS) hujumi - bu kompyuter tizimi yoki tarmog‘ini noqonuniy so‘rovlar oqimi bilan to‘ldirish yoki tizim resurslarini ishlatish uchun zaifliklardan foydalanish orqali uning mavjudligini buzishga qaratilgan zararli urinishdir. DoS hujumining maqsadi maqsadli tizim yoki tarmoqni qonuniy foydalanuvchi so‘rovlariga javob bera olmaydigan qilib, qonuniy foydalanuvchilarga xizmat ko‘rsatishdan samarali ravishda voz kechishdir.

DoS hujumlarining bir necha turlari mavjud, quyida uning ba’zi turlarini keltirib o‘tamiz.

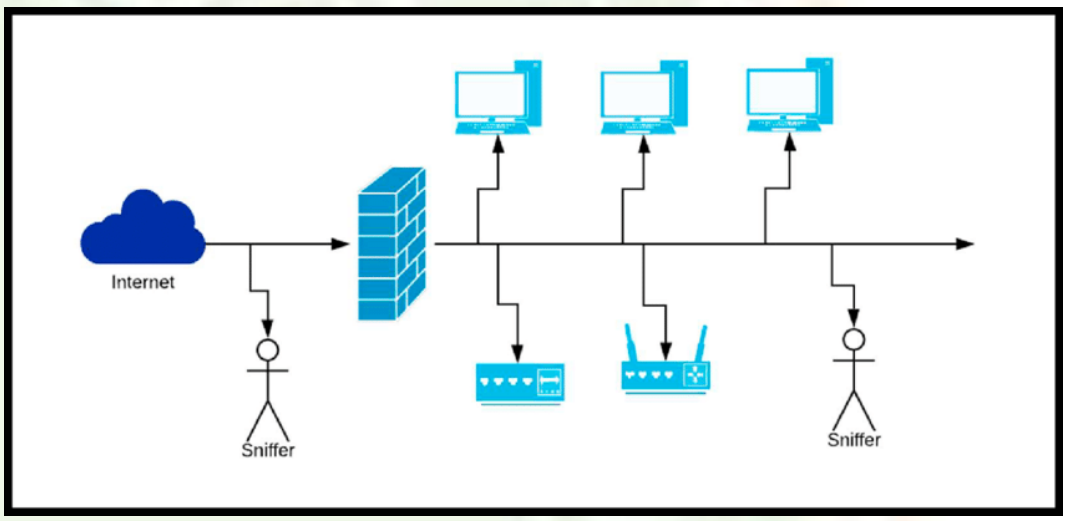
O‘tkazish qobiliyatiga asoslangan hujumlar: Ushbu hujumlar maqsadli tizim yoki tarmoqning tarmoq o‘tkazish qobiliyatini iste'mol qilishga qaratilgan. Misol uchun, tajovuzkor botnetdan (buzilgan kompyuterlar tarmog‘i) maqsadni yuqori hajmdagi trafik bilan to‘ldirish uchun foydalanishi mumkin, bu uning qonuniy so‘rovlarni bajarish qobiliyatini oshirib yuborishi mumkin.

Resurslarni tugatish hujumlari: Bu hujumlar maqsadli tizim yoki tarmoqdagi zaifliklardan uning manbalarini, masalan, protsessor, xotira yoki disk maydonini sarflash uchun foydalanadi. Masalan, tajovuzkor ko‘p sonli maxsus ishlab chiqilgan so‘rovlarni yuborishi mumkin, ular ortiqcha ishlov berish quvvati yoki xotirani iste'mol qiladi, bu esa tizimning sekinlashishiga yoki ishdan chiqishiga olib keladi.

Ilova qatlamiga hujumlar: Bu hujumlar tizimda ishlaydigan maxsus ilovalar yoki xizmatlarga qaratilgan. Ular maqsadli xizmatni to‘ldirish yoki uning

resurslarini iste'mol qilish uchun dastur qatlamidagi zaifliklardan foydalanadilar. Misollar, HTTP suv toshqini, bu erda veb-server juda ko‘p HTTP so‘rovlari bilan bombardimon qilinadi yoki DNS kuchaytirish hujumlari, bu erda tajovuzkor DNS javoblari bilan nishonni to‘ldirish uchun noto‘g‘ri sozlangan DNS serverlaridan foydalanadi.

Tarmoqni hidlash (Network Sniffing). Tarmoqni sniffing qilish tarmoq bo‘ylab harakatlanayotganda parollar yoki maxfiy ma’lumotlar kabi nozik ma’lumotlarni olish uchun tarmoq trafigini qo‘lga kiritish va tahlil qilishni o‘z ichiga oladi. Tarmoq sniffing, shuningdek, paketlarni sniffing yoki tarmoq monitoringi sifatida ham tanilgan, tarmoq trafigini qo‘lga olish va tahlil qilish amaliyotidir. Bu ma’lumot olish, tarmoq ishlashini kuzatish yoki tarmoq muammolarini bartaraf etish uchun kompyuter tarmog‘i bo‘ylab oqayotgan ma’lumotlar paketlarini ushlab turish va tekshirishni o‘z ichiga oladi. Tarmoqni hidlash haqida tushunish uchun ba’zi muhim fikrlarlarni quyida keltirib o‘tamiz.



2-rasm. Tarmoqni sniffing qilish

Tarmoqni tahlil qilish: Tarmoqni tekshirish ma’murlar yoki tahlilchilarga tarmoq xatti-harakatlari haqida tushunchaga ega bo‘lish, qiyinchiliklarni aniqlash, muammolarni bartaraf etish va tarmoq ish faoliyatini optimallashtirish uchun tarmoq trafigini tekshirish imkonini beradi.

Xavfsizlik monitoringi: Tarmoqni tekshirish ruxsatsiz kirish urinishlari, zararli dasturlarni infektsiyalari yoki shubhali aloqa shakllari kabi potentsial xavfsizlik tahdidlarini aniqlash va tahlil qilish uchun ishlatilishi mumkin.

Protokol tahlili: Tarmoq paketlarini qo‘lga olish va tahlil qilish orqali sniffing vositalari foydalanilayotgan protokollar, paketlar tuzilishi va tarmoq qurilmalari o‘rtasida ma’lumotlar almashinuvi haqida batafsil ma’lumot berishi mumkin.

Noqonuniy rejim: Tarmoqni sniffing asboblari mo‘ljallangan maqsaddan qat'i nazar, tarmoq interfeysi orqali o‘tadigan barcha tarmoq trafigini qo‘lga kiritish imkonini beruvchi promiscuous rejimda ishlaydi.

Port Mirroring/Spanning: Ba’zi tarmoqlar ma’lum tarmoq portlaridan monitoring portiga trafikni takrorlash uchun portni aks ettirish yoki spanni ishlatadi, bu markazlashtirilgan paketlarni olish va tahlil qilish imkonini beradi.

Packet Sniffers: Ushbu dasturiy vositalar tarmoq paketlarini ushlaydi va tahlil qiladi. Masalan, Wireshark, tcpdump va Microsoft Network Monitor.

Tarmoq TAPlari: Tarmoq TAP (Test kirish nuqtasi) tarmoq qurilmalari o‘rtasida joylashgan apparat qurilmasi bo‘lib, tarmoq trafigini passiv kuzatish va yozib olish imkonini beradi.

Tarmoq monitoringi dasturi: Tarmoqni monitoring qilish uchun maxsus dasturiy ta’minot tarmoq trafigini qo‘lga olish va tahlil qilish, shu jumladan real vaqtda monitoring, ogohlantirish va hisobot berish uchun ilg‘or imkoniyatlarni taqdim etadi.

Tarmoq unumdorligini monitoring qilish: Tarmoq ma’murlari tarmoqdan foydalanishni kuzatish, o‘tkazish qobiliyatini talab qiluvchi ilovalarni aniqlash va tarmoq unumdorligi bilan bog‘liq muammolarni bartaraf etish uchun hidlash vositalaridan foydalanishi mumkin.

Tarmoq muammolarini bartaraf etish: Tarmoq paketlarini tekshirish orqali ma’murlar tarmoq muammolarini aniqlashlari, noto‘g‘ri konfiguratsiyalarni aniqlashlari yoki aloqa xatolarini tahlil qilishlari mumkin.

Tarmoq xavfsizligi tahlili: Sniffing vositalari shubhali yoki zararli faoliyatni aniqlash, potentsial zaifliklarni aniqlash yoki xavfsizlik hodisalarini tekshirish kabi xavfsizlik maqsadlarida tarmoq trafigini kuzatish va tahlil qilishda yordam berishi mumkin.

Ruxsatsiz kirish: Yomon niyatli shaxslar qo‘lidagi hidlash vositalaridan parollar, login ma’lumotlari yoki tarmoq orqali uzatiladigan maxfiy ma’lumotlar kabi nozik ma’lumotlarni qo‘lga kiritish uchun foydalanish mumkin.

Maxfiylik buzilishi: Tarmoqni sniffing tarmoq aloqalari mazmunini to‘sib qo‘yishi va fosh qilishi mumkin, bu esa foydalanuvchilar yoki tashkilotlarning maxfiyligini buzishi mumkin.

Yumshatish choralari: Xavfsiz protokollar (masalan, HTTPS) yordamida tarmoq trafigini shifrlash, nozik ma’lumotlarni alohida tarmoqlarga bo‘lish, tarmoqqa kirishni boshqarish vositalarini joriy etish va kirishni aniqlash/oldini olish tizimlarini qo‘llash tarmoqni sindirish bilan bog‘liq xavflarni kamaytirishga yordam beradi.

Shuni ta’kidlash kerakki, tarmoqni tekshirish qonuniy va axloqiy chegaralar doirasida, tegishli manfaatdor tomonlarning tegishli ruxsati va roziligi bilan amalga oshirilishi kerak. Tegishli ruxsatsiz tarmoq trafigini hidlash noqonuniy hisoblanadi va maxfiylik huquqlarini buzish hisoblanadi.

Xulosa. Axborot xavfsizligini ta’minlashda tarmoq hujumlarining turlari va ular qanday amalga oshirish bir qator afzalliklarni taqdim etadi. Ta’kidlash joizki, hatto eng professional foydalanuvchilar ham zararli dasturlarning ba’zi shakllarini yuklab olishlari yoki onlayn firibgarlik va shaxsiy ma’lumotlarni o‘g‘irlash qurboni tarmoq orqali amalga oshiriladi. Viruslar, josuslik dasturlari va shaxsiy ma’lumotlarni o‘g‘irlashning oldini olish anchagini jiddiy masaladir. Professional xakerlar viruslarni yaratishning murakkab usul va algoritmlarini topishmoqda. Ushbu viruslar kompyuterga o‘rnashgandan so‘ng, ular qayta ishlash tezligini keskin sekinlashtirishi, muhim ma’lumotlarni o‘chirishi va kompyuter yoki tarmoq tizimlariga zarar yetkazishi mumkin. Shaxsiy ma’lumotlarni o‘g‘irlash va josuslik dasturlari, shuningdek, parollar, moliyaviy ma’lumotlar, kredit karta raqamlari va

tizimingiz foydalanuvchilarining ijtimoiy xavfsizlik raqamlari kabi maxfiy shaxsiy ma'lumotlarni himoya qilish uchun dasturiy ta'minotdan foydalanish orqali oldini olish mumkin. Aslida, kiberhujumlarning yoki tarmoqdan amalga oshiriladigan hujumlarning 80% zaif o'g'irlangan parollar tufayli yuzaga keladi, shuning uchun ularni ehtiyotkorlik bilan himoya qilish kerak bo'ladi.

FOYDALANILGAN ADABIYOTLAR RO'YHATI

1. Fazilov, S. X., Mahkamov, A. A., & Jumayev, T. S. (2018). Algorithm for extraction of identification features in ear recognition. Информатика: проблемы, методология, технологии, 3-7.

2. Mahkamov, A. A., Jumayev, T. S., Tuhtanazarov, D. S., & Dadamuxamedov, A. I. (2024). Using AdaBoost to improve the performance of simple classifiers. In Artificial Intelligence, Blockchain, Computing and Security Volume 2 (pp. 755-760). CRC Press.

3. Zhumaev, T.S., Mirzaev, N.S., & Makhkamov, A.S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27),

4. Маҳкамов, А. А., & Инадуллаев, Х.Ў.Ў. (2021). Сравнительный анализ биометрических систем в обеспечении информационной безопасности. Universum: технические науки, (12-1 (93)), 32-37.

5. Махкамов А. А. Алгоритмы идентификации личности человека по изображению ушных раковин //Исследования технических наук. – 2015. – №. 4. – С. 28-32.

6. Tuhtanazarov, D., Xodjayeva, M., Jumayev, T., & Mahkamov, A. (2022, June). Computational algorithm and program for determining the indicators of wells based on processing of information of oil fields. In AIP Conference Proceedings (Vol. 2432, No. 1, p. 060021). AIP Publishing LLC.

7. Zhumaev, T. S., Mirzaev, N. S., & Makhkamov, A. S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27), 4.

8. Жумаев, Т. С., Мирзаев, Н. С., & Махкамов, А. С. (2015). Алгоритмы сегментации цветных изображений, основанные на выделение сильносвязанных элементов. Исследования технических наук, (4), 22-27.

9. Махкамов, А. А., & Дадамухамедов, А. И. (2022). Алгоритм выделения области ушных раковин при распознавании личности. Universum: технические науки, (5-1 (98)), 14-17.

10. Махкамов, А. А. (2015). Алгоритмы идентификации личности человека по изображению ушных раковин. Исследования технических наук, (4), 28-32.

11. Е.А.Степанов, И.К.Корнеев, Информационная безопасность и защита информации. – М.: Инфра, 2002.