EOC
EUROASIAN
ONLINE
CONFERENCES

SPAIN
CONFERENCE

INTERNATIONAL CONFERENCE ON SUPPORT OF MODERN SCIENCE AND INNOVATION

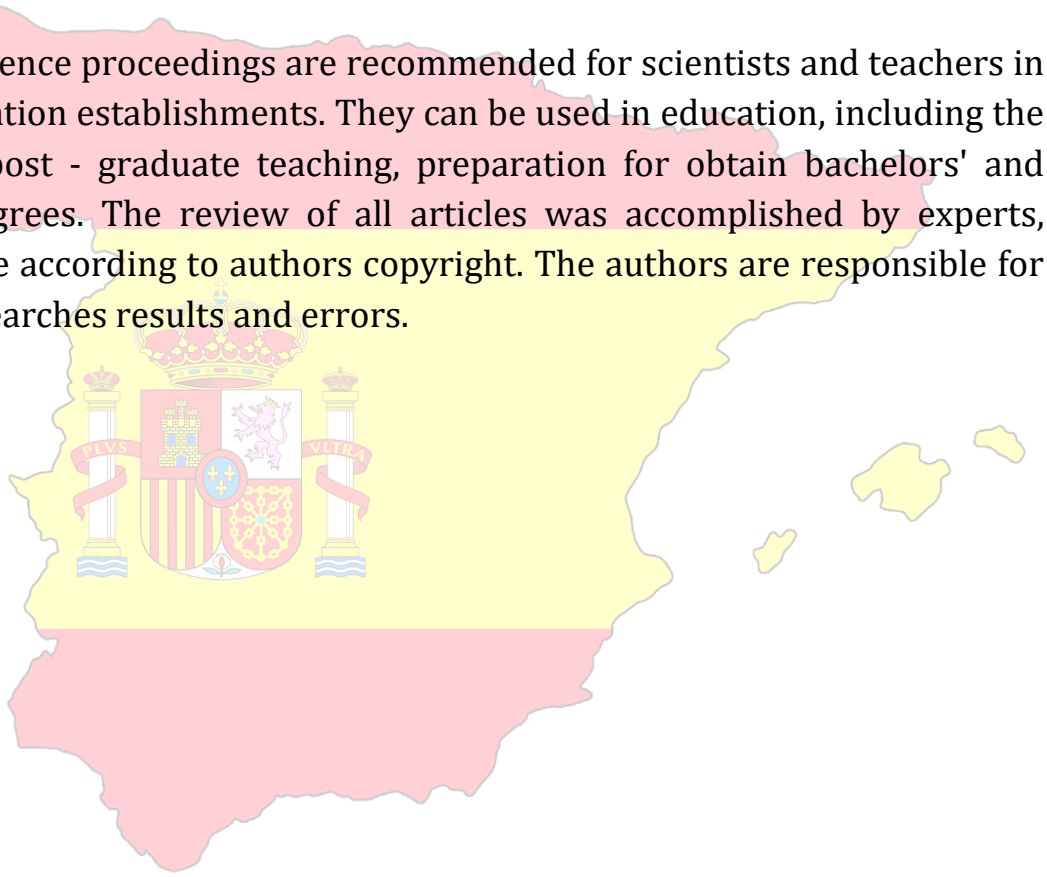
Google Scholar zenodo OpenAIRE doi digital object identifier

INTERNATIONAL CONFERENCE ON SUPPORT OF MOERN SCIENCE AND INNOVATION: a collection scientific works of the International scientific conference – Madrid, Spain, 2026, Issue 5.

Languages of publication: Uzbek**,** English, Russian, German, Italian, Spanish,

The collection consists of scientific research of scientists, graduate students and students who took part in the International Scientific online conference **«INTERNATIONAL CONFERENCE ON SUPPORT OF MOERN SCIENCE AND INNOVATION»**. Which took place in Spain, 2026.

Conference proceedings are recommended for scientists and teachers in higher education establishments. They can be used in education, including the process of post - graduate teaching, preparation for obtain bachelors' and masters' degrees. The review of all articles was accomplished by experts, materials are according to authors copyright. The authors are responsible for content, researches results and errors.



RANSOMWARE ISHLASH MEXANIZMI VA SHIFRLASH ALGORITMLARI

Sobirovjonov Begzod Qaxramon og'li
Farg'ona davlat universiteti "Matematika va informatika" kafedrasi o'qituvchisi
Tursunaliyeva Sarvinoz G'ulomjon qizi
Farg'ona davlat universiteti talabasi
To'ychiboyeva Durdona To'lqinjon qizi
Farg'ona davlat universiteti talabasi

Annotatsiya. Zamonaviy axborot xavfsizligi muhitida zararli dasturlar, xususan ransomware (tovon talab qiluvchi zararli dasturlar) tahdidi tobora kuchayib bormoqda. Ushbu tahdidlar tashkilotlar va foydalanuvchilarning muhim ma'lumotlarini shifrlash orqali ularga kirishni cheklaydi hamda ularni tiklash evaziga moliyaviy to'lov talab qiladi. Ushbu maqolada ransomware'ning ishlash mexanizmi chuqur tahlil qilingan bo'lib, uning tizimga kirib borish usullari, tarqalish bosqichlari va zarar yetkazish jarayonlari izchil yoritilgan. Shuningdek, maqolada ransomware tomonidan qo'llaniladigan zamonaviy shifrlash algoritmlari, jumladan simmetrik va assimetrik kriptografiya usullarining o'ziga xos jihatlari, ularning afzallik va kamchiliklari ilmiy asosda bayon etilgan. Bundan tashqari, shifrlash jarayonida kalitlarni boshqarish, ma'lumotlarni tiklash imkoniyatlari hamda xavfsizlik choralarini kuchaytirish usullari ham ko'rib chiqilgan. Tadqiqot natijalari ransomware hujumlariga qarshi samarali himoya strategiyalarini ishlab chiqishda kriptografik yondashuvlarning muhim ahamiyatga ega ekanligini ko'rsatadi.

Abstract. In the modern information security environment, the threat of malicious programs, in particular ransomware (malware demanding ransom), is becoming increasingly serious. These threats restrict access to important data of organizations and users by encrypting them and demanding a financial payment in exchange for their recovery. This article provides an in-depth analysis of the mechanism of ransomware operation, consistently covering its methods of penetration into the system, stages of spread, and damage infliction processes. The article also describes the specific aspects of modern encryption algorithms used by ransomware, including symmetric and asymmetric cryptography methods, their advantages and disadvantages on a scientific basis. In addition, key management during the encryption process, data recovery options, and methods for strengthening security measures are also considered. The research results show the importance of cryptographic approaches in developing effective protection strategies against ransomware attacks.

Kalit so'zlar: Ransomware, axborot xavfsizligi, zararli dasturlar, shifrlash algoritmlari, kriptografiya, simmetrik shifrlash, assimetrik shifrlash, kalit boshqaruvi, ma'lumotlarni himoyalash, kiberxavfsizlik, zararli hujumlar, ma'lumotlarni tiklash.

Keywords: Ransomware, information security, malware, encryption algorithms, cryptography, symmetric encryption, asymmetric encryption, key management, data protection, cybersecurity, malicious attacks, data recovery.

KIRISH. Axborot texnologiyalarining jadal rivojlanishi va raqamli transformatsiya jarayonlarining kengayishi natijasida kiberxavfsizlik masalalari tobora dolzarb ahamiyat kasb etmoqda. Xususan, so‘nggi yillarda zararli dasturlar orasida ransomware (tovon talab qiluvchi dasturlar) alohida xavf sifatida ajralib chiqmoqda. Ilgari oddiy virus va troyan dasturlar orqali ma’lumotlarga zarar yetkazilgan bo‘lsa, bugungi kunda ransomware yordamida foydalanuvchilarning muhim fayllari shifrlanib, ularni tiklash uchun katta miqdorda mablag‘ talab qilinmoqda. Bu esa tashkilotlar, bank tizimlari, davlat muassasalari hamda oddiy foydalanuvchilar uchun jiddiy tahdid tug‘dirmoqda. Ransomware dasturlarining ishlash mexanizmi murakkab va ko‘p bosqichli jarayonlardan iborat bo‘lib, ular odatda fishing xatlari, zararli havolalar, soxta dasturlar yoki tizim zaifliklari orqali qurilmaga kirib boradi. Tizimga kirgandan so‘ng, ular tezkor ravishda fayllarni aniqlaydi, ularni bloklaydi va kuchli kriptografik algoritmlar yordamida shifrlaydi. Natijada foydalanuvchi o‘z ma’lumotlariga kira olmay qoladi va ularni qayta tiklash uchun maxsus kalit talab qilinadi.

Zamonaviy ransomware dasturlari oddiy shifrlash usullaridan farqli ravishda murakkab kriptografik algoritmlardan foydalanadi. Xususan, ular simmetrik (AES kabi) va assimetrik (RSA kabi) shifrlash usullarining kombinatsiyasini qo‘llaydi. Bunda ma’lumotlar tezkor shifrlanishi uchun simmetrik algoritmlar ishlatilsa, kalitlarni xavfsiz uzatish va saqlash uchun assimetrik kriptografiya qo‘llaniladi. Bu esa shifrlangan ma’lumotlarni maxsus kalitsiz tiklashni deyarli imkonsiz qiladi.

Bugungi kunda ransomware tahdidlari faqat lokal kompyuterlar bilan cheklanib qolmay, balki bulutli tizimlar, korporativ tarmoqlar va hatto IoT qurilmalariga ham ta’sir ko‘rsatmoqda. Shu sababli, ularning oldini olish, aniqlash va bartaraf etish bo‘yicha samarali mexanizmlarni ishlab chiqish muhim vazifaga aylangan. Antivirus tizimlari, xavfsizlik devorlari (firewall), zaxira nusxalar (backup) hamda foydalanuvchilarni xabardor qilish kabi choralar ransomware hujumlariga qarshi kurashishda muhim o‘rin tutadi.

Ushbu tadqiqotning dolzarbligi shundan iboratki, ransomware hujumlarining soni va murakkabligi ortib borayotgan bir sharoitda, ularning ishlash mexanizmini chuqur o‘rganish hamda qo‘llaniladigan shifrlash algoritmlarini tahlil qilish orqali samarali himoya choralarini ishlab chiqish zarur. Shu bois, mazkur maqolada ransomware dasturlarining ishlash prinsiplari, ularning tarqalish yo‘llari, shifrlash algoritmlarining turlari va amaliy qo‘llanilishi keng yoritiladi. So‘nggi ilmiy tadqiqotlar shuni ko‘rsatadiki, ransomware hujumlariga qarshi kurashishda faqat texnik choralar yetarli emas, balki kompleks yondashuv talab etiladi. Masalan, kiberxavfsizlik bo‘yicha zamonaviy ilmiy manbalarda kriptografik algoritmlarning mustahkamligi, kalitlarni boshqarish tizimlari va foydalanuvchi xatti-harakatlarini tahlil qilish muhim omillar sifatida qayd etilgan. Shu bilan birga, xalqaro

tashkilotlar va IT kompaniyalar tomonidan ishlab chiqilgan xavfsizlik standartlari ransomware tahdidlarini kamaytirishda muhim rol o‘ynamoqda.

Umuman olganda, ransomware va uning asosida yotgan shifrlash algoritmlarini o‘rganish nafaqat nazariy, balki amaliy jihatdan ham katta ahamiyatga ega bo‘lib, u zamonaviy axborot tizimlarining xavfsizligini ta’minlashda muhim vosita hisoblanadi.

XULOSA. Olib borilgan tadqiqotlar shuni ko‘rsatdiki, ransomware dasturlari zamonaviy kiberxavfsizlik muhitida eng xavfli tahdidlardan biri sifatida shakllanib bormoqda. Tahlillar natijasida aniqlanishicha, ushbu zararli dasturlar murakkab ishlash mexanizmlariga ega bo‘lib, tizimga yashirin kirish, tezkor tarqalish va foydalanuvchi ma’lumotlarini to‘liq nazorat ostiga olish imkonini beradi. Ayniqsa, ransomware tomonidan qo‘llaniladigan simmetrik va assimetrik shifrlash algoritmlarining uyg‘unlashuvi ma’lumotlarni tiklashni deyarli imkonsiz darajaga olib keladi.

O‘tkazilgan kuzatuvlar shuni ko‘rsatadiki, ransomware hujumlari nafaqat texnik zaifliklardan, balki foydalanuvchilarning ehtiyotsizligi, xabardorlik darajasining pastligi va xavfsizlik qoidalariga amal qilmaslik natijasida ham muvaffaqiyatli amalga oshiriladi. Shu bois, himoya choralarini faqat texnik vositalar bilan cheklab qo‘yish yetarli emas, balki foydalanuvchilarni doimiy ravishda o‘qitish va ogohlantirish ham muhim ahamiyat kasb etadi.

Shuningdek, ransomware hujumlariga qarshi samarali kurashish uchun zamonaviy antivirus dasturlari, xavfsizlik devorlari, zaxira nusxa olish tizimlari va kriptografik himoya usullaridan kompleks foydalanish zarur. Ayniqsa, ma’lumotlarni muntazam ravishda zaxiralash va ularni alohida xavfsiz muhitda saqlash muhim himoya choralaridan biri hisoblanadi.

Shu bilan birga, kiberxavfsizlik sohasida olib borilayotgan ilmiy tadqiqotlar ransomware’ning yangi turlarini aniqlash, ularning ishlash mexanizmini chuqur o‘rganish hamda samarali himoya strategiyalarini ishlab chiqishga qaratilgan. Oliy ta’lim tizimida kiberxavfsizlik va kriptografiya fanlarini chuqurlashtirib o‘qitish, amaliy laboratoriya mashg‘ulotlarini kengaytirish hamda real holatlarga asoslangan treninglarni joriy etish bu boradagi bilim va ko‘nikmalarni yanada mustahkamlashga xizmat qiladi.

Natijada, ransomware va uning asosida yotgan shifrlash algoritmlarini o‘rganish nafaqat nazariy jihatdan, balki amaliy nuqtai nazardan ham muhim bo‘lib, u zamonaviy axborot tizimlarining xavfsizligini ta’minlashda ajralmas vosita sifatida o‘z o‘rnini tobora mustahkamlab bormoqda.

Foydalanilgan adabiyotlar ro‘yxati

1. Stallings, W. Cryptography and Network Security: Principles and Practice. – Pearson, 2017.
2. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020.
3. NIST. Advanced Encryption Standard (AES), FIPS PUB 197. – 2017.
4. Rivest, R., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. – 1978.
5. ENISA. Ransomware Threat Landscape Report. – 2022.