ZARARKUNANDA DASTURLAR (MALWARE) VA ULARNING ASOSIY TURLARI: VIRUS, QURT VA TROYAN

Samarqand iqtisodiyot va servis instituti

"XALQARO IQTISODIY MUNOSABATLAR" fakulteti

Iqtisodiy xavfsizlik yo‘nalishi

IKX-123 4-KURS

Abdunabiyeva Sarvinoz Erkin qizi

abdunabiyevgayrat8@gmail.com

Samarqand iqtisodiyot va servis instituti

Axborot texnologiyalari kafedrasi asistenti

Rustamov Sherzod Norxudjayevich

Annotatsiya: Maqolada zararkunanda dasturlar (malware) tushunchasi hamda ularning uch asosiy turi — virus, qurt va troyan — ilmiy asosda, biroq oddiy va tushunarli tilda tahlil qilinadi. Tadqiqotning maqsadi — zararkunanda dasturlarning mohiyatini, tarqalish mexanizmlarini va turlararo farqlarini sistemalashtirish hamda O‘zbekiston Respublikasi normativ-huquqiy bazasi va xalqaro tajriba asosida himoya choralarini asoslashdan, shuningdek, mavzuni keng auditoriya uchun tushunarli talqin qilishdan iborat. Mavzuning dolzarbligi raqamli xizmatlarning kengayishi, har kuni yangi zararli dasturlar paydo bo‘layotgani va tovlamachilik dasturlari bilan bog‘liq buzilishlarning ko‘payishi bilan belgilanadi. Tadqiqotda ilmiy adabiyotlar va xalqaro standartlarni tahlil qilish, qiyosiy-tasniflash, tarixiy-tahliliy usullar hamda miqdoriy illyustrativ hisob-kitob usullaridan foydalanildi. Tahlilda nazariy ta’riflar bilan birga Morris, Code Red va Slammer qurtlari kabi tarixiy misollar ham qamrab olindi. Natijalar shuni ko‘rsatdiki, virus tarqalishi uchun xost fayl va foydalanuvchi harakatiga, qurt tarmoq zaifliklariga, troyan esa aldov (ijtimoiy muhandislik)ga tayanadi; zamonaviy hujumlar esa ko‘pincha bu turlarni birlashtirgan gibrid xarakterga ega. Maqolada normativ-huquqiy, tashkiliy va

texnik takliflar hamda oddiy foydalanuvchilar va tashkilotlar uchun amaliy tavsiyalar shakllantirildi.

Kalit so‘zlar: zararkunanda dastur (malware), kompyuter virusi, kompyuter qurti, troyan oti, o‘z-o‘zini ko‘paytirish, ijtimoiy muhandislik, tovlamachilik dasturi, kiberxavfsizlik, antivirus himoyasi, axborot xavfsizligi.

Abstract: The article analyses the concept of malicious software (malware) and its three principal types — viruses, worms, and Trojans — on a scientific basis but in plain and accessible language. The aim of the study is to systematize the essence, propagation mechanisms, and differences between these types of malware and to substantiate protective measures on the basis of the regulatory framework of the Republic of Uzbekistan and international experience, and to present the topic in a form understandable to a broad audience. The relevance of the topic is determined by the expansion of digital services, the daily emergence of new malicious programs, and the growing number of breaches involving ransomware. The study employed analysis of the scientific literature and international standards, comparative classification, historical-analytical methods, and illustrative quantitative calculations. The analysis covers theoretical definitions as well as historical cases such as the Morris, Code Red, and Slammer worms. The results demonstrate that a virus depends on a host file and user action, a worm on network vulnerabilities, and a Trojan on deception (social engineering), while modern attacks are often hybrid in nature, combining these types. Normative-legal, organizational, and technical proposals, as well as practical recommendations for ordinary users and organizations, are formulated in the article.

Keywords: malware, computer virus, computer worm, Trojan horse, self-replication, social engineering, ransomware, cybersecurity, antivirus protection, information security.

KIRISH

Zamonaviy jamiyatda smartfon, kompyuter va tarmoqqa ulangan qurilmalar bank xizmatlaridan tortib davlat xizmatlarigacha bo‘lgan jarayonlarning asosiy vositasiga

aylandi. Bu muhitda eng keng tarqalgan tahdidlardan biri zararkunanda dasturlardir. AV-TEST mustaqil laboratoriyasining statistik ma’lumotlariga ko‘ra, har kuni yuz minglab yangi zararli dastur namunalari ro‘yxatga olinadi,[1] Verizon kompaniyasining 2024-yilgi hisobotida esa tovlamachilik dasturlari (ransomware) va boshqa tovlamachilik usullari tahlil qilingan buzilishlarning taxminan uchdan bir qismida qayd etilgan.[2] Shu sababli zararkunanda dasturlarning turlari va ishlash tamoyillarini nafaqat mutaxassislar, balki oddiy foydalanuvchilar ham tushunishi zarur: tahdidni tanimagan odam undan himoyalana olmaydi.

Mavzuning huquqiy dolzarbligi, avvalo, konstitutsiyaviy normalar bilan belgilanadi. 2023-yil 30-aprelda umumxalq referendumida qabul qilingan O‘zbekiston Respublikasi Konstitutsiyasining yangi tahririda shaxsiy hayotning daxlsizligi hamda shaxsga doir ma’lumotlarni himoya qilish huquqi kafolatlangan.[3] Zararkunanda dasturlar aynan shu huquqqa tahdid soladi: josuslik dasturi yozishmalar va parollarni o‘g‘irlaydi, tovlamachilik dasturi ma’lumotlarni shifrlab, egasini ulardan mahrum qiladi. 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun ma’lumotlar operatorlariga ularni yo‘qolish, ruxsatsiz kirish va boshqa noqonuniy harakatlardan himoya qilish uchun huquqiy, tashkiliy va texnik choralarni ko‘rish majburiyatini yuklaydi,[4] zararli dasturlardan himoya esa bunday choralarning ajralmas qismidir.

2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonun mamlakatda kiberxavfsizlik sohasidagi munosabatlarni, subyektlarning vakolat va majburiyatlarini hamda muhim axborot infratuzilmasini himoya qilish asoslarini belgilab,

[1]AV-TEST Institute. Malware statistics & trends report. URL: https://www.av-test.org/en/statistics/malware/

[2]Verizon. 2024 Data Breach Investigations Report. — Verizon Business, 2024. URL: https://www.verizon.com/business/resources/reports/dbir/

[3]O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahriri), 31-modda // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[4]O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

kiberhodisalarni aniqlash va ularga javob berishni tizimli faoliyat sifatida mustahkamladi.[5] Strategik darajada 2020-yil 5-oktabrdagi PF-6079-son Farmon bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi davlat va tijorat xizmatlarini onlayn shaklga o‘tkazishni jadallashtirdi;[6] har bir yangi raqamli xizmat esa, bir tomondan, aholi uchun qulaylik, boshqa tomondan, zararkunanda dasturlar uchun yangi nishon bo‘ladi. Jinoyat-huquqiy jihatdan Jinoyat kodeksining axborot texnologiyalari sohasidagi jinoyatlar uchun javobgarlikni belgilovchi XX[1] bobi, jumladan, zararli dasturlarni yaratish va tarqatishga oid normalari ushbu hodisaga qarshi huquqiy kurashning asosini tashkil etadi.[7]

Shunday qilib, huquqiy baza mavjud bo‘lsa-da, uning amaliy ijrosi aholi va tashkilot xodimlarining tahdidni to‘g‘ri tushunishiga bog‘liq. Zararkunanda dasturlarning turlari ko‘pincha aralashtirib yuboriladi: kundalik nutqda “virus” so‘zi hamma narsani bildirib keladi, aslida esa virus, qurt va troyan turli usullarda tarqaladi va turlicha himoyani talab qiladi. Mazkur tadqiqotning maqsadi ushbu tushunchalarni ilmiy aniqlik va oddiy til uyg‘unligida izohlash, ularning farqlarini ko‘rsatish va himoya bo‘yicha amaliy takliflar ishlab chiqishdan iborat. Tadqiqotda ilmiy adabiyotlar va xalqaro standartlarni tahlil qilish, qiyosiy-tasniflash va tarixiy-tahliliy usullar, shuningdek, tarqalish tezligining oddiy miqdoriy hisob-kitobi qo‘llanildi.

Zararkunanda dastur (malware) — foydalanuvchining roziligisiz, odatda yashirin ravishda tizimga kiritilib, ma’lumotlarning maxfiyligi, yaxlitligi yoki mavjudligiga zarar yetkazish yoki tizim ishini buzish maqsadida yaratilgan dastur; bu mazmundagi ta’rif NIST SP 800-83 qo‘llanmasida keltirilgan.[8] Bunday dasturlarning nazariy ildizi J. fon

[5]O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[6]O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi // Lex.uz. URL: https://lex.uz

[7]O‘zbekiston Respublikasi Jinoyat kodeksi (1994-yil 22-sentabrdagi 2012-XII-son Qonun bilan tasdiqlangan), XX[1] bob (axborot texnologiyalari sohasidagi jinoyatlar) // Lex.uz. URL: https://lex.uz

[8]Souppaya M., Scarfone K. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication 800-83, Revision 1. — Gaithersburg: NIST, 2013.

Neymanning o‘z-o‘zini ko‘paytiruvchi avtomatlar nazariyasiga borib taqaladi,[9] “kompyuter virusi” tushunchasini esa F. Koen 1987-yildagi ishida rasmiy ta’riflab, virus boshqa dasturlarni o‘zgartirib, ularga o‘z nusxasini kiritishga qodir dastur ekanini ko‘rsatgan.[10] P. Sor o‘z monografiyasida zararli kodni tasniflashda uning tarqalish usuli, boshqa fayllarga bog‘liqligi va yuklamasi (payload) kabi belgilarga e’tibor qaratgan.[11] Ana shu uch belgi — o‘zini ko‘paytirishi, xostga bog‘liqligi va tarqalish usuli — virus, qurt va troyanni bir-biridan ajratishning asosiy mezonlaridir.

Oddiy tilda virusni biologik virusga o‘xshatish mumkin: u o‘zi mustaqil “yashay” olmaydi, boshqa dastur yoki fayl — “xost” ichiga joylashib oladi va o‘sha fayl ishga tushirilgandagina faollashadi. Shu sababli virus tarqalishi uchun odatda foydalanuvchining harakati — zararlangan faylni ochish, boshqaga yuborish yoki flesh-xotira orqali ko‘chirish — kerak bo‘ladi. Virus odatda ko‘paytirish moduli, yuklama (zarar yetkazuvchi qism) va ba’zan faollashish sharti (masalan, muayyan sana)dan iborat bo‘ladi. Yuklama fayllarni buzishi, tizimni sekinlashtirishi yoki boshqa zararli amallarni bajarishi mumkin. Virus bilan kurashishning asosiy qiyinligi shundaki, u qonuniy fayl ichida yashirinadi va foydalanuvchi o‘zi uni ishga tushiradi.

Qurt (worm) esa virusdan farqli ravishda mustaqil dastur bo‘lib, xost faylga muhtoj emas va odatda foydalanuvchi harakatisiz, tarmoq yoki dasturlardagi zaifliklardan foydalanib, o‘zini boshqa kompyuterlarga ko‘chiradi. Eng mashhur dastlabki misol — 1988-yilgi Morris qurti: E. Spafford tahliliga ko‘ra, u taxminan 6000 ta kompyuterni, ya’ni o‘sha davrda tarmoqqa ulangan tugunlarning qariyb o‘ndan bir qismini ishdan chiqargan.[12] Viruslarning tarqalishini epidemiologik modellar bilan tavsiflash mumkinligini J. Kefart

[9]von Neumann J. Theory of Self-Reproducing Automata / ed. and completed by A.W. Burks. — Urbana: University of Illinois Press, 1966.

[10]Cohen F. Computer viruses: Theory and experiments // Computers & Security. — 1987. — Vol. 6, No. 1. — P. 22–35.

[11]Szor P. The Art of Computer Virus Research and Defense. — Upper Saddle River: Addison-Wesley, 2005.

[12]Spafford E.H. The Internet Worm Program: An Analysis // ACM SIGCOMM Computer Communication Review. — 1989. — Vol. 19, No. 1. — P. 17–57.

va S. Uayt yo‘naltirilgan graflarga asoslangan modellar orqali ko‘rsatgan.[13] 2001-yilgi Code Red qurti 14 soatdan kamroq vaqt ichida 359 mingdan ortiq tugunni zararlagan,[14] 2003-yil yanvaridagi SQL Slammer esa rivojlanishining dastlabki bosqichida zararlangan tugunlar sonini taxminan har 8,5 soniyada ikki baravar oshirib, bir necha daqiqa ichida zaif tugunlarning taxminan 90 foizini, jami 75 mingdan ortiq tugunni zararlagan.[15] Illustrativ hisob-kitob: agar zararlangan tugunlar soni har 8,5 soniyada ikki baravar ko‘paysa, bitta tugundan 75 000 tugunga yetish uchun $\log_2(75\,000) \approx 16{,}2$ marta ikki baravar ko‘payish kerak, ya’ni taxminan $16{,}2 \times 8{,}5 \approx 138$ soniya (2,3 daqiqa) ketadi. Bu idealizatsiyalangan hisob bo‘lib, amalda jarayon tarmoq o‘tkazuvchanligi bilan cheklanadi, biroq u qurtni inson javob bera olmaydigan tezlikda yoyilishini ko‘rsatadi. S. Staniford va hamkasblari esa oldindan tayyorlangan zaif tugunlar ro‘yxatidan foydalanuvchi qurtlar nazariy jihatdan butun zaif tugunlar to‘plamini o‘ta qisqa vaqtda zararlashi mumkinligi gipotezasini asoslagan.[16] Muhimi shuki, Slammer tarqalgan paytda uning zaifligini yopuvchi yamoq allaqachon mavjud edi, ya’ni ko‘plab tizimlar shunchaki yangilanmagan edi.

Troyan (troyan oti) o‘zini foydali yoki zararsiz dastur sifatida ko‘rsatadi, biroq yashirin ravishda zararli vazifani bajaradi. Atama qadimgi yunon afsonasidagi yog‘och otdan kelib chiqqan bo‘lib, kompyuter xavfsizligi kontekstida J. Anderson tomonidan 1972-yilda AQSh Harbiy-havo kuchlari uchun tayyorlangan hisobotda qo‘llangan.[17] Virus va qurtdan farqli o‘laroq, troyan odatda o‘z-o‘zini ko‘paytirmaydi; uning tarqalishi aldov — soxta o‘rnatuvchi, “bepul” yoki qalbaki dastur, elektron pochtadagi ilova — orqali

[13]Kephart J.O., White S.R. Directed-graph epidemiological models of computer viruses // Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy. — IEEE, 1991. — P. 343–359.

[14]Moore D., Shannon C., Brown J. Code-Red: a case study on the spread and victims of an Internet worm // Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement (IMW ’02). — ACM, 2002. — P. 273–284.

[15]Moore D., Paxson V., Savage S. et al. Inside the Slammer Worm // IEEE Security & Privacy. — 2003. — Vol. 1, No. 4. — P. 33–39.

[16]Staniford S., Paxson V., Weaver N. How to 0wn the Internet in Your Spare Time // Proceedings of the 11th USENIX Security Symposium. — USENIX Association, 2002. — P. 149–167.

[17]Anderson J.P. Computer Security Technology Planning Study. Vol. II. ESD-TR-73-51. — Bedford, MA: Electronic Systems Division, U.S. Air Force, 1972.

amalga oshadi, ya’ni u texnik zaiflikdan emas, balki inson ishonuvchanligidan foydalanadi. Troyan “orqa eshik” (backdoor) ochishi, parol va bank ma’lumotlarini o‘g‘irlashi yoki boshqa zararli dasturlarni yuklab olishi mumkin. Misol uchun, Emotet dastlab bank troyani sifatida paydo bo‘lib, keyinchalik boshqa zararli dasturlarni yetkazuvchi platformaga aylangan va CISA ogohlantirishida eng qimmat va buzg‘unchi zararli dasturlardan biri sifatida ta’riflangan.[18]

Uch tur o‘rtasidagi farqni qisqacha shunday ifodalash mumkin: virus xostga yopishib, foydalanuvchi yordamida tarqaladi; qurt mustaqil bo‘lib, tarmoq orqali o‘zi tarqaladi; troyan o‘zini boshqa narsa deb ko‘rsatib, foydalanuvchini aldaydi. Biroq zamonaviy amaliyotda bu chegaralar xiralashgan: hujum ko‘pincha troyan (masalan, soxta ilova) orqali kiradi, qurt kabi tarmoqdagi boshqa kompyuterlarga yoyiladi va yakunda tovlamachilik dasturini yuklaydi. ENISA tomonidan tayyorlangan 2023-yilgi tahdidlar manzarasi hisobotida tovlamachilik dasturlari asosiy tahdidlar qatorida ko‘rsatilgan bo‘lib,[19] bu zararkunanda dasturlarning iqtisodiy jihatdan eng foydali turi — ma’lumotlarni shifrlab, to‘lov talab qilish — tomon evolyutsiya qilganini ko‘rsatadi. Shu sababli turlarni bilish himoyani to‘g‘ri tanlash uchun zarur, ammo bitta tur bo‘yicha himoya yetarli emas.

Himoya bo‘yicha xalqaro tajriba chuqur himoya tamoyiliga tayanadi. CIS Critical Security Controls to‘plamining 10-nazorati zararli dasturlardan himoyani — antivirus yoki EDR vositalarini joriy etish, ularni avtomatik yangilash va olinadigan tashuvchilarda avtomatik ishga tushirishni o‘chirishni — alohida nazorat sifatida belgilaydi.[20] Amaliy jihatdan har bir tur uchun asosiy chora turlicha: viruslarga qarshi — noma’lum fayllarni ishga tushirmaslik va antivirusni yangilab turish; qurtlarga qarshi — operatsion tizim va

[18]CISA. Alert TA18-201A: Emotet Malware. — Cybersecurity and Infrastructure Security Agency, 2018. URL: https://www.cisa.gov

[19]ENISA. ENISA Threat Landscape 2023. — Athens: European Union Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu

[20]Center for Internet Security. CIS Critical Security Controls, Version 8, Control 10: Malware Defenses. — East Greenbush, NY: CIS, 2021. URL: https://www.cisecurity.org/controls

dasturlarni o‘z vaqtida yangilash hamda keraksiz tarmoq xizmatlarini yopish; troyanlarga qarshi — dasturlarni faqat rasmiy manbalardan yuklab olish va gumonli xabarlardagi ilovalarni ochmaslik. Barcha turlar uchun umumiy choralar — oddiy foydalanuvchi huquqlarida ishlash, muhim ma’lumotlarning zaxira nusxalarini tarmoqdan ajratilgan holda saqlash va tarmoqni segmentlarga bo‘lish.

XULOSA

Tadqiqot natijalariga ko‘ra, zararkunanda dasturlar uch asosiy mezon — o‘zini ko‘paytirishi, xostga bog‘liqligi va tarqalish usuli bo‘yicha tasniflanadi: virus xost faylga va foydalanuvchi harakatiga, qurt tarmoq zaifliklariga, troyan esa aldovga tayanadi. Qurtlarning tarqalish tezligi (hisob-kitobga ko‘ra, bir tugundan o‘n minglab tugunga bir necha daqiqada yetishi) inson javobiga ishonib bo‘lmasligini, shu sababli oldindan yangilash va avtomatlashtirilgan himoya zarurligini asoslaydi. Zamonaviy hujumlar gibrid xarakterda bo‘lgani uchun faqat bir turga qarshi himoya yetarli emas. Huquqiy jihatdan zararli dasturlardan himoya Konstitutsiyada kafolatlangan shaxsiy hayot daxlsizligi va shaxsga doir ma’lumotlarni himoya qilish huquqining amaliy mexanizmi hisoblanadi.

Mualliflik takliflari: 1) aholi va xodimlar uchun zararkunanda dasturlarning turlari va oddiy himoya qoidalari bo‘yicha tushunarli o‘quv materiallari va ommaviy axborot kampaniyalarini ishlab chiqish; 2) tashkilotlarda dasturlarni yangilash (patch management), zaxira nusxalash va xodimlarni o‘qitish tartibini ichki hujjatda mustahkamlash; 3) muhim axborot infratuzilmasi obyektlarida CIS Controls va NIST SP 800-83 kabi xalqaro tavsiyalarga uyg‘un zararli dasturlardan himoya bo‘yicha uslubiy talablarni belgilash; 4) mahalliy sharoitda zararli dasturlar bilan bog‘liq hodisalar bo‘yicha umumlashtirilgan statistik ma’lumotlar yig‘ish va ochiq hisobotlar e’lon qilish. Foydalanuvchilarga esa operatsion tizim va dasturlarni yangilab turish, dasturlarni faqat rasmiy manbalardan yuklab olish, noma’lum havola va ilovalarni ochmaslik, muhim ma’lumotlarning zaxira nusxasini saqlash va antivirus vositasidan foydalanish tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

[1] AV-TEST Institute. Malware statistics & trends report. URL: https://www.av-test.org/en/statistics/malware/

[2] Verizon. 2024 Data Breach Investigations Report. — Verizon Business, 2024. URL: https://www.verizon.com/business/resources/reports/dbir/

[3] O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahriri), 31-modda // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[4] O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[5] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[6] O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi // Lex.uz. URL: https://lex.uz

[7] O‘zbekiston Respublikasi Jinoyat kodeksi (1994-yil 22-sentabrdagi 2012-XII-son Qonun bilan tasdiqlangan), XX¹ bob (axborot texnologiyalari sohasidagi jinoyatlar) // Lex.uz. URL: https://lex.uz

[8] Souppaya M., Scarfone K. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication 800-83, Revision 1. — Gaithersburg: NIST, 2013.

[9] von Neumann J. Theory of Self-Reproducing Automata / ed. and completed by A.W. Burks. — Urbana: University of Illinois Press, 1966.

[10] Cohen F. Computer viruses: Theory and experiments // Computers & Security. — 1987. — Vol. 6, No. 1. — P. 22–35.

[11] Szor P. The Art of Computer Virus Research and Defense. — Upper Saddle River: Addison-Wesley, 2005.

[12] Spafford E.H. The Internet Worm Program: An Analysis // ACM SIGCOMM Computer Communication Review. — 1989. — Vol. 19, No. 1. — P. 17–57.

[13] Kephart J.O., White S.R. Directed-graph epidemiological models of computer viruses // Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy. — IEEE, 1991. — P. 343–359.

[14] Moore D., Shannon C., Brown J. Code-Red: a case study on the spread and victims of an Internet worm // Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement (IMW ’02). — ACM, 2002. — P. 273–284.

[15] Moore D., Paxson V., Savage S. et al. Inside the Slammer Worm // IEEE Security & Privacy. — 2003. — Vol. 1, No. 4. — P. 33–39.

[16] Staniford S., Paxson V., Weaver N. How to 0wn the Internet in Your Spare Time // Proceedings of the 11th USENIX Security Symposium. — USENIX Association, 2002. — P. 149–167.

[17] Anderson J.P. Computer Security Technology Planning Study. Vol. II. ESD-TR-73-51. — Bedford, MA: Electronic Systems Division, U.S. Air Force, 1972.

[18] CISA. Alert TA18-201A: Emotet Malware. — Cybersecurity and Infrastructure Security Agency, 2018. URL: https://www.cisa.gov

[19] ENISA. ENISA Threat Landscape 2023. — Athens: European Union Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu

[20] Center for Internet Security. CIS Critical Security Controls, Version 8, Control 10: Malware Defenses. — East Greenbush, NY: CIS, 2021. URL: https://www.cisecurity.org/controls