FIDYA DASTURLARI (RANSOMWARE) VA ULARNING KORXONA HAMDA BANKLARGA YETKAZADIGAN IQTISODIY ZARARI

Samarqand iqtisodiyot va servis instituti

"XALQARO IQTISODIY MUNOSABATLAR" fakulteti

Iqtisodiy xavfsizlik yo‘nalishi

IKX-123 4-KURS

Abdurashidova Nigina Ilhom qizi

885759988

niginaabdurashidova418@gmail.com

Samarqand iqtisodiyot va servis instituti

Axborot texnologiyalari kafedrasi asistenti

Rustamov Sherzod Norxudjayevich

Annotatsiya.

Maqolada fidya dasturlari (ransomware)ning korxona va banklarga yetkazadigan iqtisodiy zarari tahlil qilingan. Mavzuning dolzarbligi raqamli xizmatlarga bog‘liqlikning ortishi, hujumlarning “ikki karra tovlamachilik” va xizmat sifatidagi fidya dasturlari (RaaS) modeliga o‘tishi hamda moliya sektorida bir martalik uzilishning ham keng iqtisodiy oqibatlarga olib kelishi bilan izohlanadi. Maqsad – fidya dasturlaridan ko‘riladigan zararni to‘g‘ridan-to‘g‘ri va bilvosita tarkibiy qismlarga ajratish, moliya tashkilotlari uchun xatarlarni baholash va himoya choralarini takomillashtirish bo‘yicha takliflar berishdir. Tadqiqotda normativ-huquqiy hujjatlar tahlili, xalqaro hisobotlar (Sophos, IBM, Chainalysis)ni qiyosiy o‘rganish, aniq hodisalar (Change Healthcare, Jaguar Land Rover) tahlili hamda ochiq statistik ma’lumotlarni miqdoriy qayta hisoblash usullaridan foydalanildi. Natijada iqtisodiy zararning to‘rt qatlamli (to‘lov, tiklash, uzilish, nufuz va huquqiy) modeli asoslandi; to‘langan fidya umumiy zararning kichik qismini tashkil etishi, asosiy yo‘qotish operatsion uzilish va ta’minot zanjiri orqali yuzaga kelishi

ko‘rsatildi; zaifliklarni tezkor bartaraf etish, zaxira nusxalarni sinash, hodisaga javob rejasi va kiberstrahovkani joriy etish bo‘yicha tavsiyalar ishlab chiqildi.

Kalit so‘zlar: fidya dasturlari, ransomware, kiberxavfsizlik, iqtisodiy zarar, banklar, korxonalar, ikki karra tovlamachilik, zaxira nusxa, kiberstrahovka, operatsion uzilish.

Abstract.

The article analyzes the economic damage that ransomware inflicts on enterprises and banks. Its relevance is explained by growing dependence on digital services, the shift of attackers to double extortion and ransomware-as-a-service, and the fact that even a short outage in the financial sector causes wide economic consequences. The aim is to break down direct and indirect losses from ransomware, assess risks for financial institutions and propose improvements to protection measures. The study uses legal analysis, a comparative review of international reports (Sophos, IBM, Chainalysis), case analysis (Change Healthcare, Jaguar Land Rover) and quantitative recalculation of public statistics. A four-layer model of economic loss (payment, recovery, disruption, reputational and legal) is substantiated; the ransom actually paid is shown to be a small share of total loss, with the main damage arising from operational disruption and supply-chain effects; recommendations on prompt vulnerability remediation, tested backups, incident response planning and cyber insurance are developed.

Keywords: ransomware, cybersecurity, economic damage, banks, enterprises, double extortion, backups, cyber insurance, operational disruption.

KIRISH

Iqtisodiyotning raqamlashuvi korxona va banklar faoliyatini axborot tizimlariga deyarli to‘liq bog‘lab qo‘ydi: to‘lovlar, hisob-kitoblar, ombor va ishlab chiqarish jarayonlari uzluksiz ishlaydigan tarmoqlarga tayanadi. Shu sababli fidya dasturlari (ransomware) – tizim yoki ma’lumotlarni shifrlab, ularni qaytarish evaziga pul talab qiladigan zararli dasturlar – kiberjinoyatlar orasida eng katta iqtisodiy zarar keltiruvchi tahdidga aylandi. Bunday hujumning moliyaviy ta’siri faqat talab qilingan pul bilan

cheklanmaydi: u ishlab chiqarishning to‘xtashi, mijozlarning yo‘qotilishi, jarima va sud xarajatlari hamda nufuzga yetgan zarar bilan o‘lchanadi.

Huquqiy jihatdan masala bir necha normada aks etadi. 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonun kiberhujum va muhim axborot infratuzilmasi tushunchalarini belgilab, sohaning huquqiy asosini yaratgan.[1] Jinoyat kodeksining 278⁶-moddasi zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatishni jinoyat deb belgilaydi, 165-modda esa tovlamachilikni qamrab oladi; keyingi o‘zgartirishlarda qurilma yoki akkauntni zararli dastur orqali bloklab, pul talab qilish holatlari uchun javobgarlik kuchaytirilishi nazarda tutilgan.[2][3] Demak, fidya dasturlari mahalliy qonunchilikda ham alohida e’tibor markazida.

Shunga qaramay, ochiq manbalarda O‘zbekistonda fidya dasturlaridan ko‘rilgan zarar ajratilgan holda e’lon qilinmaydi: rasmiy statistika kiberjinoyatlarni umumiy holda, asosan bank kartalari bilan bog‘liq firibgarlik sifatida ko‘rsatadi. Maqsad – xalqaro dalillar va mahalliy ma’lumotlar asosida fidya dasturlaridan ko‘riladigan iqtisodiy zararning tarkibiy modelini ishlab chiqish va korxona hamda banklar uchun amaliy tavsiyalar asoslashdir. Ilmiy yangilik – zararni to‘lov, tiklash, uzilish hamda nufuz va huquqiy qatlamlarga ajratuvchi model hamda to‘langan fidya umumiy zararning kichik qismi, degan ishchi gipotezaning raqamli asoslanishidir.

Fidya dasturlarining iqtisodiy mohiyati vaqt o‘tishi bilan o‘zgargan. Dastlab alohida kompyuterlarni bloklash bilan cheklangan hujumlar bugun uyushgan, xizmat sifatida sotiladigan jinoiy sanoatga aylandi: dastur ishlab chiquvchilari tayyor vositani hamkorlarga ijaraga beradi, hamkorlar esa hujumni amalga oshirib, daromadni bo‘lishadi. Bu model hujum uchun zarur malakani pasaytirdi, hujumlar sonini oshirdi. Yana bir

[1] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – Lex.uz

[2] O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr): 165-modda (tovlamachilik), 278⁶-modda (zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish). – Lex.uz

[3] Internet orqali tovlamachilik va noqonuniy mayning uchun javobgarlik kuchaytiriladi // Zamin.uz; Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga javobgarlik belgilanadi // Yuz.uz (Oliy Majlis Senati matbuot xizmati materiallari).

muhim o‘zgarish – “ikki karra tovlamachilik”: jinoyatchi ma’lumotni shifrlashdan oldin uni o‘g‘irlaydi va to‘lanmasa, oshkor qilish bilan tahdid qiladi. Natijada zaxira nusxadan tiklash ham mijoz ma’lumotlarining sizib chiqishi xavfini yo‘qotmaydi. Chainalysis ma’lumotlariga ko‘ra, 2024-yilda ma’lumot oshkor qilish saytlari soni keskin ko‘paydi va bir yilda 56 ta yangi sayt paydo bo‘ldi, bu 2023-yilga nisbatan ikki baravardan ortiq.[4]

To‘g‘ridan-to‘g‘ri zararning birinchi qatlami – fidyaning o‘zi. Chainalysis hisobiga ko‘ra, 2024-yilda qurbonlar fidya sifatida jami 813,55 million dollar to‘lagan, bu 2023-yildagi rekord 1,25 milliard dollardan 35 foiz kam (813,55 : 1250 ≈ 0,65 – muallif hisobi).[5] Pasayish huquqni muhofaza qilish organlari operatsiyalari va qurbonlarning to‘lashdan bosh tortishi bilan izohlangan; shu bilan birga yil davomida bitta Fortune 50 kompaniyasining Dark Angels guruhiga 75 million dollar to‘lagani qayd etilgan. IBM tadqiqotiga ko‘ra, 2025-yilda fidya talab qilingan tashkilotlarning 63 foizi to‘lashdan bosh tortgan (2024-yilda 59 foiz), biroq hujumchi tomonidan oshkor etilgan fidya yoki tovlamachilik hodisasining o‘rtacha umumiy narxi hanuz 5,08 million dollarni tashkil etadi; ma’lumotlar sizib chiqishining umumiy o‘rtacha qiymati esa 4,44 million dollarni tashkil etgan.[6]

Moliya sektori uchun manzara alohida ahamiyatga ega. Sophos 2025-yil hisobotida 17 mamlakatdagi 369 moliya tashkilotining tajribasi tahlil qilingan. Unga ko‘ra, hujumlarning 40 foizida asosiy sabab ekspluatatsiya qilingan zaiflik, 22 foizida zararli elektron xat, 17 foizida o‘g‘irlangan hisob ma’lumotlari bo‘lgan. Hujumlarning 59 foizi ma’lumotlar shifrlanishi bilan yakunlangan (2024-yilda 49 foiz), shifrlangan ma’lumotli tashkilotlarning 31 foizida ma’lumot o‘g‘irlanishi ham kuzatilgan. Moliya sohasidagi o‘rtacha (median) fidya talabi bir yilda 50 foizga oshib, 2 million dollardan 3 million

[4] Chainalysis. The 2025 Crypto Crime Report: Ransomware chapter. – Chainalysis, February 2025. – Qarang: Ransomware payments fell by 35% in 2024 // BleepingComputer, 2025.

[6] IBM Security, Ponemon Institute. Cost of a Data Breach Report 2025. – IBM, 2025.

dollarga yetgan va bu so‘rovda qatnashgan barcha tarmoqlar orasida eng yuqori ko‘rsatkich bo‘lgan; median to‘lov esa 2,1 million dollarni tashkil etgan. To‘lovchilar talabning o‘rtacha 92 foizini to‘lagan (2024-yilda 75 foiz).[7] To‘langan fidya va talabning bu nisbati (2,1 : 3,0 = 70 foiz, medianlar nisbati sifatida) jinoyatchilar bilan muzokaraning cheklangan samarasini ko‘rsatadi.

Ikkinchi qatlam – tiklash xarajatlari. Sophos ma’lumotiga ko‘ra, moliya tashkilotlari uchun hujumdan keyin tiklanishning o‘rtacha qiymati (fidyani hisobga olmaganda) 1,74 million dollar bo‘lgan; bu 2024-yildagi 2,58 million dollardan 33 foiz kam. Tashkilotlarning 57 foizi bir hafta ichida, 98 foizi uch oy ichida to‘liq tiklangan.[8] Bu o‘rinda diqqatga sazovor holat shuki, 2025-yilda moliya tashkilotlari ma’lumotni qaytarish uchun zaxira nusxadan (44 foiz) ko‘ra ko‘proq fidya to‘lash orqali (67 foiz) foydalangan – to‘rt yil ichida birinchi marta. Bu zaxira nusxalarning ishonchliligi va ularni tiklash tajribasi yetarli emasligini bildiradi. Agar median fidya (2,1 mln) va o‘rtacha tiklash xarajati (1,74 mln)ni birgalikda hisoblasak, to‘lagan moliya tashkiloti uchun bevosita xarajat taxminan 3,84 million dollarga yetadi (muallifning taxminiy hisobi; median va o‘rtacha qiymat aralashtirilgani sababli yo‘naltiruvchi xarakterga ega).

Uchinchi, eng katta qatlam – operatsion uzilish va bilvosita zarar. Buni Change Healthcare hodisasi yaqqol ko‘rsatadi: 2024-yil fevralida BlackCat (ALPHV) guruhi AQShdagi tibbiy to‘lovlarni qayta ishlovchi bu tizimni shifrladi; UnitedHealth guruhi 22 million dollar fidya to‘laganini tan oldi. Shunga qaramay, kompaniyaning 2024-yil uchun jami yo‘qotishi 3,09 milliard dollar deb baholangan.[9] Demak, jami zarar to‘langan fidyadan taxminan 140 baravar ko‘p (3090 : 22 ≈ 140,5 – muallif hisobi). Bu hodisa

[7] Sophos. The State of Ransomware in Financial Services 2025. – Sophos Whitepaper, November 2025. – 369 respondent, 17 mamlakat.

[9] UnitedHealth Group Change Healthcare hujumi xarajatlari bo‘yicha hisobotlari // Kaspersky Daily, GovInfoSecurity (Change Healthcare Attack Cost Estimate Reaches Nearly $2.9B), 2024–2025.

moliyaviy infratuzilma (to‘lov va hisob-kitob tizimlari) uzilishi minglab mijozlarning pul oqimiga bevosita ta’sir etishini ko‘rsatadi: bir tizimning to‘xtashi ketma-ket muammolarni tug‘diradi.

Ishlab chiqarish sohasida ham xuddi shu qonuniyat kuzatiladi. 2025-yil 1-sentyabrdan Jaguar Land Rover kompaniyasiga qilingan kiberhujum zavodlarni taxminan besh hafta to‘xtatdi. Cyber Monitoring Centre uni Buyuk Britaniya tarixidagi moliyaviy jihatdan eng zararli kiberhodisa deb baholab, umumiy iqtisodiy zararni taxminan 1,9 milliard funt sterling (taxminan 2,55 milliard dollar) deb hisobladi; hodisadan 5 mingdan ortiq tashkilot jabrlangan, zararning yarmidan ko‘pini kompaniyaning o‘zi, qolganini ta’minot zanjiri va mahalliy iqtisodiyot ko‘targan.[10] Muhim jihati shuki, tahlilchilar bu holatda fidya talabi izlarini topmagan va yo‘qotishlarning deyarli barchasi ma’lumot o‘g‘irlanishi emas, balki ishlab chiqarish uzilishidan kelib chiqqan. Shu bois bu hodisani fidya dasturlari mantiqining – zarar ko‘lami talab qilingan puldan emas, uzilish davomiyligidan kelib chiqadi – ehtiyotkorlik bilan keltirilgan tasdig‘i sifatida qarash mumkin.

To‘rtinchi qatlam – nufuz, huquqiy va sug‘urta xarajatlari. IBM ma’lumotiga ko‘ra, buzilishni aniqlash va to‘xtatishning o‘rtacha davomiyligi 241 kunni tashkil etgan; hodisadan keyin tashkilotlar o‘rtacha taxminan 100 kun davomida operatsion uzilishni boshdan kechirgan, ayrim tashkilotlarda hodisadan keyin sug‘urta mukofotlari taxminan 200 foizga oshgani qayd etilgan.[11] Shuningdek, fidya hodisasi haqida huquqni muhofaza qilish organlariga xabar bergan tashkilotlar ulushi 53 foizdan 40 foizga tushgan: bu yashirin zararni oshirib, jinoyatchilarni aniqlash imkonini qisqartiradi. Banklar uchun nufuz zarari alohida xavfli, chunki mijoz ishonchi yo‘qolsa, depozitlar va kreditlash hajmi kamayadi.

[10] Cyber Monitoring Centre. Jaguar Land Rover cyber event: Category 3 systemic event (2025-yil oktyabr) // BBC, Bloomberg, Express & Star materiallari.

O‘zbekiston misolida fidya dasturlarining o‘ziga xos statistikasi e’lon qilinmagan, ammo umumiy kiberxavf ko‘lami katta. IIV Kiberxavfsizlik markazi ma’lumotiga ko‘ra, 2019-yilda 863 ta kiberjinoyat qayd etilgan bo‘lsa, 2024-yilda 58 800 tasi qayd etilgan (58 800 : 863 ≈ 68,1 baravar); kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 2023-yildagi 6,2 foizdan 2024-yilda 44,4 foizga o‘sgan; oxirgi uch yilda fuqarolarning 1,9 trillion so‘mdan ortiq mablag‘i talon-taroj qilingan, faqat 2024-yilda 603 milliard so‘m. Jinoyatlarning 98 foizi bank kartalari bilan bog‘liq, 60 foizi zararli havola va dastur orqali sodir etilgan.[12] Toshkent shahrida 2024-yilda kiberjinoyatlardan 381 milliard so‘m zarar ko‘rilgan, uning atigi 4 foizi (14,2 milliard so‘m) qaytarilgan.[13] Demak, zararli dastur orqali tizimga kirish va foydalanuvchini aldash yo‘li mahalliy jinoyatchilikda ham asosiy vosita; bu fidya dasturlari uchun ham zamin yaratadi, chunki bir xil texnik va ijtimoiy usullar (zararli fayl, fishing havola) qo‘llaniladi. Shu bois fidya dasturlari bo‘yicha alohida statistikaning yo‘qligini ularning yo‘qligi deb baholash noto‘g‘ri; bu gipoteza maxsus hisobot bilan tasdiqlanishi lozim.

Yuqoridagi dalillardan fidya dasturlaridan ko‘riladigan zararning to‘rt qatlamli modeli kelib chiqadi. Birinchi qatlam – fidyaning o‘zi; ikkinchi – tiklash (tizim, ish vaqti, qurilma, maslahat xarajatlari); uchinchi – operatsion uzilish (yo‘qotilgan daromad, ta’minot zanjiridagi buzilish, mijozlarga xizmat ko‘rsata olmaslik); to‘rtinchi – nufuz, jarima, sud va sug‘urta xarajatlari. Raqamlar shuni ko‘rsatadiki, birinchi qatlam eng ko‘zga ko‘rinadigan, biroq eng katta emas: Change Healthcare holatida u umumiy zararning taxminan 0,7 foizini tashkil etgan (22 : 3090 ≈ 0,0071). Shu sababli “to‘lab qutulish” mantiqi iqtisodiy jihatdan noto‘g‘ri: to‘lov ma’lumot qaytarilishini kafolatlamaydi (Change Healthcare holatida guruh o‘z hamkorini aldab, pulni o‘zlashtirgan, ma’lumot esa

[12] IIV Kiberxavfsizlik markazi press-turi, 2025-yil 29-may // Spot.uz, 2025-yil 29-may.

[13] Uzbekistan’s cybercrime crisis: How scammers steal millions and evade capture // Kun.uz, 2025-yil 12-mart.

boshqa guruh qo‘liga o‘tgani qayd etilgan[14]), uzilishdan ko‘riladigan zararni bartaraf etmaydi va jinoyatchilarni yangi hujumlarga rag‘batlantiradi.

Himoya choralarini ham shu qatlamlarga bog‘lab qurish mumkin. Birinchidan, Sophos ma’lumotiga ko‘ra, moliya sohasida hujumlarning 40 foizi zaifliklar orqali sodir bo‘lgani uchun, yangilanishlarni tezkor o‘rnatish va zaifliklarni muntazam skanerlash eng samarali profilaktika hisoblanadi; respondentlarning 44 foizi himoya vositalarining yo‘qligini yoki noma’lum zaifliklarni sabab sifatida ko‘rsatgan.[15] Ikkinchidan, zaxira nusxalar nafaqat yaratilishi, balki muntazam tiklab sinab ko‘rilishi va asosiy tarmoqdan ajratilgan holda saqlanishi lozim. Uchinchidan, hodisaga javob berish rejasi va tarmoqni segmentlarga ajratish uzilish ko‘lamini qisqartiradi. IBM ma’lumotiga ko‘ra, tashkilotning o‘zi hodisani aniqlasa, jinoyatchi xabar bergan holatga nisbatan o‘rtacha 900 ming dollar tejaladi, shuningdek sun’iy intellekt va avtomatlashtirishdan keng foydalangan tashkilotlar buzilish boshiga o‘rtacha 1,9 million dollar tejagan.[16] To‘rtinchidan, kiberstrahovka va aniq hujjatlashtirilgan biznes uzluksizligi rejasi zararning moliyaviy yukini taqsimlaydi; JLR misolida bu ayniqsa muhimligi ko‘rsatildi, chunki ayrim xabarlarga ko‘ra kompaniya hujum vaqtida faol kiberstrahovkaga ega bo‘lmagan.[17]

Banklar uchun qo‘shimcha choralar zarur: tranzaksiyalarni real vaqt rejimida kuzatish, muhim tizimlar uchun “oltin nusxa” (immutable backup) va muqobil to‘lov kanallarini saqlash, uchinchi tomon xizmat ko‘rsatuvchilarining (to‘lov provayderlari, bulutli xizmatlar) xavfsizligini nazorat qilish. Change Healthcare hodisasi bir kompaniyaga qilingan hujum minglab tashkilotni to‘xtatishi mumkinligini isbotladi; shu sababli bank va to‘lov tashkilotlari ta’minot zanjiri xatarini mustaqil baholashi kerak. Huquqiy jihatdan esa muhim axborot infratuzilmasi subyektlari uchun hodisalar haqida

majburiy va tezkor xabar berish tartibini, shuningdek fidya to‘lovlari bo‘yicha aniq siyosatni (to‘lov taqiqlanishi yoki oldindan ogohlantirish) takomillashtirish maqsadga muvofiq.

XULOSA

Tadqiqot quyidagi xulosalarga olib keldi. Birinchidan, fidya dasturlari tarixiy jihatdan alohida tizimlarni bloklashdan uyushgan, xizmat sifatida sotiladigan va ma’lumot o‘g‘irlashga asoslangan jinoiy sanoatga aylandi; shu sababli faqat zaxira nusxaga tayanish yetarli emas. Ikkinchidan, iqtisodiy zarar to‘rt qatlamdan iborat: fidya, tiklash, operatsion uzilish hamda nufuz va huquqiy xarajatlar; Change Healthcare misolida to‘langan 22 million dollar jami 3,09 milliard dollar zararning taxminan 0,7 foizini tashkil etgan. Uchinchidan, moliya tashkilotlarida hujumlarning 59 foizi shifrlash bilan yakunlangan, median fidya talabi 3 million dollarga yetgan va 2025-yilda fidya to‘lash zaxira nusxadan foydalanishdan ko‘proq qo‘llangan, bu himoya chidamliligining pasayishini bildiradi. To‘rtinchidan, O‘zbekistonda kiberjinoyatlar 2019–2024-yillarda 863 tadan 58 800 tagacha o‘sgani va ulushi 44,4 foizga yetgani fidya dasturlari xavfini ham oshiradi, biroq bu xavf alohida statistikada ajratilmagan.

Mualliflik takliflari: korxona va banklarda zaiflik boshqaruvi hamda zaxira nusxalarni muntazam tiklash sinovlarini majburiy talab sifatida joriy etish; hodisaga javob rejasini va biznes uzluksizligi rejasini yiliga kamida bir marta mashq qilish; kiberstrahovka bozorini rivojlantirish; IIV va Markaziy bank statistikasida fidya dasturlari hodisalarini alohida ko‘rsatish; muhim axborot infratuzilmasi subyektlari uchun hodisa haqida majburiy xabar berish muddatlarini belgilash; xodimlarning raqamli gigiyenasi bo‘yicha o‘qitish dasturlarini kengaytirish. Korxona va fuqarolar uchun asosiy qoida: fidya to‘lamaslik, hodisani darhol vakolatli organga xabar qilish va tiklash uchun oldindan tayyorlangan rejaga tayanish.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – Lex.uz

2. O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr): 165-modda, 278⁶-modda. – Lex.uz

3. Sophos. The State of Ransomware in Financial Services 2025. – Sophos Whitepaper, November 2025.

4. IBM Security, Ponemon Institute. Cost of a Data Breach Report 2025. – IBM, 2025.

5. Chainalysis. The 2025 Crypto Crime Report (ransomware). – Chainalysis, February 2025; Ransomware payments fell by 35% in 2024 // BleepingComputer, 2025.

6. Change Healthcare Attack Cost Estimate Reaches Nearly $2.9B // GovInfoSecurity, 2024; The ransomware attack on UnitedHealth Group // Kaspersky Daily, 2025.

7. Cyber Monitoring Centre. Jaguar Land Rover cyber event (Category 3 systemic event), 2025-yil oktyabr; JLR Hack Costs UK Economy £1.9 Billion // Bloomberg, 2025-yil 23-oktyabr.

8. IIV Kiberxavfsizlik markazi press-turi, 2025-yil 29-may // Spot.uz, 2025-yil 29-may.

9. Uzbekistan’s cybercrime crisis: How scammers steal millions and evade capture // Kun.uz, 2025-yil 12-mart.

10. Internet orqali tovlamachilik va noqonuniy mayning uchun javobgarlik kuchaytiriladi // Zamin.uz; Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga javobgarlik belgilanadi // Yuz.uz.