



TODAY'S STATE OF PROTECTING BANKS FROM CYBER RISKS

SHIRINOV KHUSAN AZIM O'G'LI

Graduate School of Business and Entrepreneurship under the Cabinet of
Ministers of the Republic of Uzbekistan, master degree

Abstract: This article modern digital transformation under the circumstances banking in the sector cyber security status complex analysis to do , global and regional trends study , basic cyber threats determination and modern protection measures efficiency evaluation goal does . In the article Uzbekistan and In the context of Central Asia cyber security problems deep analysis to do separately attention focused .

Keywords: cyber security , banking, finance institutions , cyber attacks , defense measures

Introduction

Digital of technologies intense development with together banking The sector is also large. to changes exposed is happening . COVID-19 pandemic due to global finance system example unseen digital to transformation entered . However , this process with together cyber The risks are also acute. increased .

Trend Micro report according to , 2021 first in the middle banking in the field ransom programs attacks increased by 1318% . Federal Reserve Bank of New York to the report according to , finance firms other 300 times from the fields more cyber to attacks exposed will be .

Uzbekistan in the context of situation further anxious . Last five year inside In Uzbekistan cyber crimes 68 times increased . In 2024 all 44.4% of crimes cyber crimes organization reached .

This of the research purpose banking in the sector cyber security status analysis to do and modern protection strategies is learning .

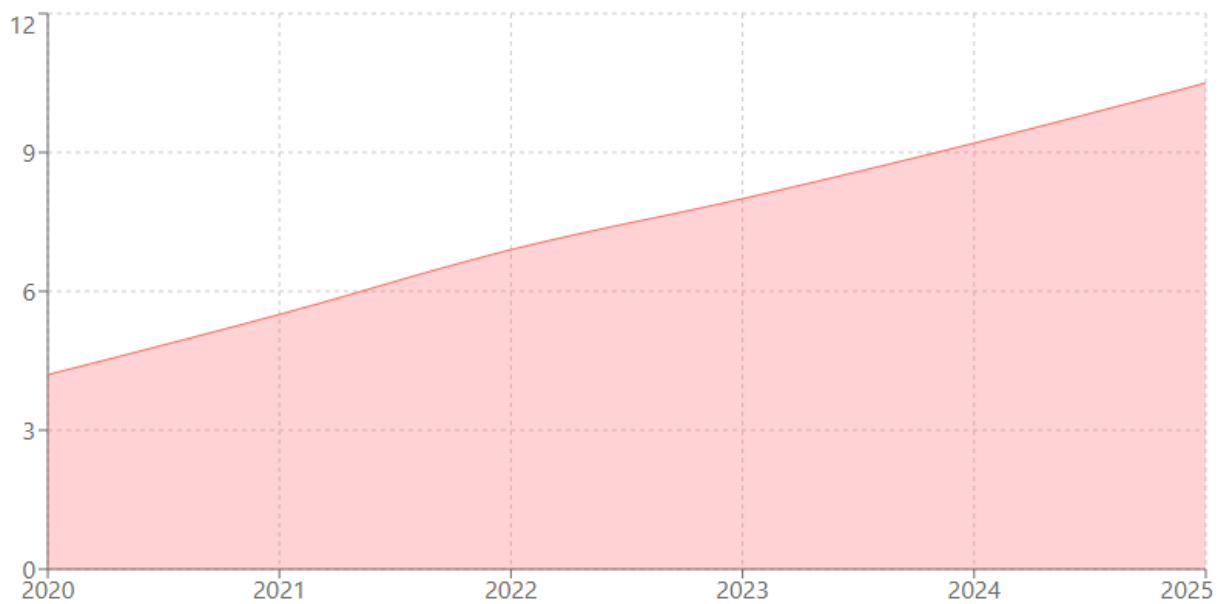


Figure 1. Global Cyber Crime Damage Scale

Method and materials

Research methodology

This research following methods based on done increased :

1. **Information collection** : 2024-2025 for international cyber security reports analysis
2. **Statistical Analysis** : Global and regional cyber attacks statistics study
3. **Comparative Analysis** : Different countries and regions experience comparison
4. **Expert ratings** : The industry leader experts thoughts generalization

Information sources

- World Economic Forum Global Cyber Security Outlook 2025
- International Currency Foundation reports
- Uzbekistan Cyber Security Center information
- International banking and cyber security companies reports

Research circle

Research 2019-2025 range cover takes and following directions own inside takes :

- Global cyber risks dynamics
- Banking in the sector main threats
- Uzbekistan and In the context of Central Asia situation



- Modern protection technologies

Results

1. Global Cyber Risks Statistics

Worldwide cyber crime damage size by 2025 come \$ 10.5 trillion annually organization to be able forecast This number is being cyber threats to the global economy the impact shows .

Home statistic information :

- Global data in 2024 violation average worth 4.88 million dollars organization reached
- By 2023 relatively information violation expenses increased by 10%
- Past more than 30,000 per year weakness it was determined that previous 17% more than the indicators

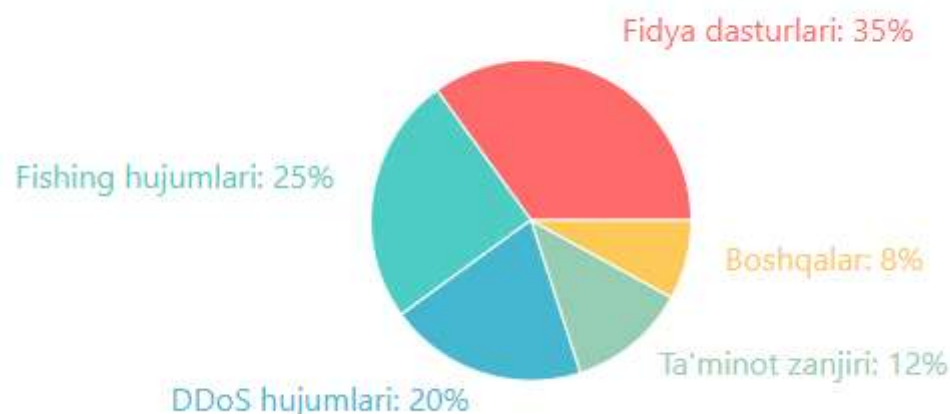


Figure 2. Main Cyber Attack Types (%)

Banking In the sector Cyber Threats

Home attack types . March - June 2020 in the months to banks anti- phishing and ransom programs attacks in 2019 this to the period increased by 520% compared to .

The widest widespread attack types :

1. **Ransom Ransomware** - Average ransom attack damage size 1.82 million dollars



2. **Phishing attacks** - Akamai report According to , phishing attacks almost 50% of finance services to the sector aimed at
3. **DDoS attacks** - in 2021 many vectored DDoS attacks increased by 80%
4. **Maintenance chain attacks** - ENISA forecast according to , in 2021 supply chain attacks in 2020 4 times more than increases

Financial damage indicators

- Finance in the sector information violation average \$5.85 million damage brings
- Financial motivated attacks general 95% of attacks organization will
- Finance 63% of institutions fatal cyber attacks increased confession reached

Uzbekistan and Central In Asia Situation

Statistical indicators . Latest five year inside In Uzbekistan cyber crimes 68 times increased :

- **2019** : 863 crimes (**in 18** categories)
- **2024** : 58,800 crimes (**in 62** categories)
- In 2024 cyber crimes number by 2023 9.1 times compared increased

Financial Loss . 2021-2024 between In Uzbekistan cyber crimes as a result 1.9 trillion soums (\$148.9 million) stolen from citizens :

- **In 2024 loss** : 603 billion soums (47.3 million dollars)

Attacks map . In 2024 Out of 12 million in Uzbekistan more than cyber attack attempt record was :

- 11.2 million in 2023 cyber attack
- 2024 first more than 3,290,860 in the quarter cyber attack

Artificial intellect and the car study . More than 71% of banks cyber threats determination and prevent to take for artificial from the intellect uses .

Blockchain technology . By 2025 come 48% of banks safe and transparent transactions for blockchain from technology uses .

Quantum Cryptography . 75% of banks will be crypto by 2030 come quantum cyber security threats preparation is seeing .



Market growth Global Cybersecurity in **Banking** security market from \$ 74.3 billion in 2022 to 2032 up to \$ 282 billion growth this is expected 14.4% annual growth pace organization will reach .

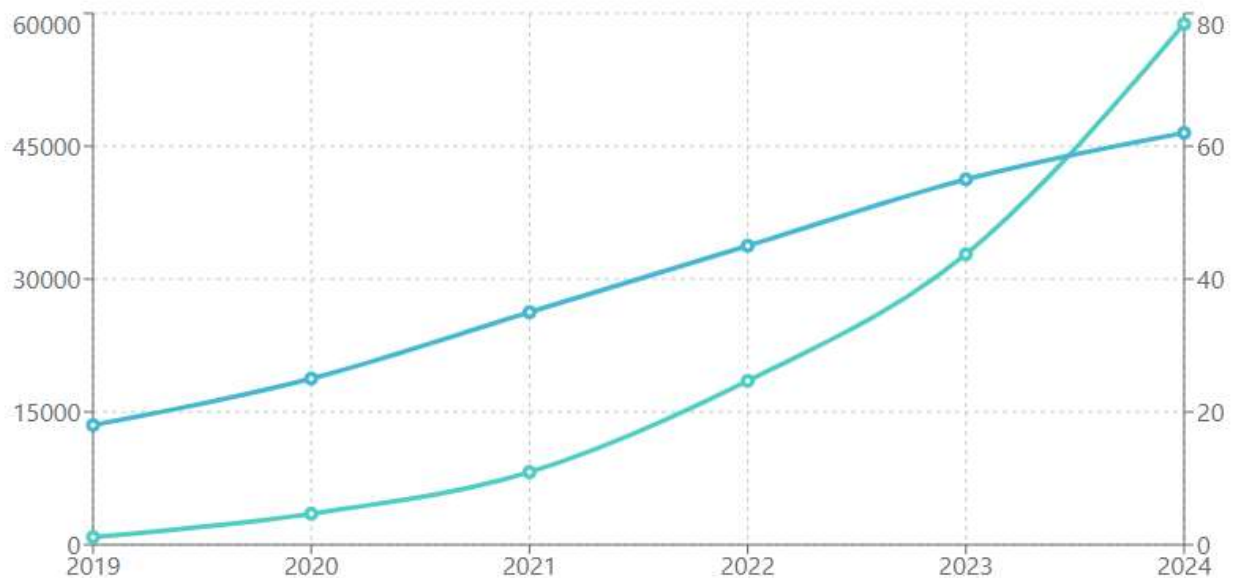


Figure 3. In Uzbekistan Cyber Crimes Dynamics

Discussion

Home problems and difficulties

Staff deficit . By 2025 come cyber security 3.4 million workers in the sector place empty to remain is expected . This is a global problem. and Uzbekistan too except it's not .

To order eater of standards fragmentation

Over 76% of CISOs various jurisdictions according to of the rules dispersion their organizations compatibility storage to the ability noticeable impact to do emphasized .

Artificial intellect paradox . 66% of organizations are using AI cyber to safety the most important impact to show Despite expectations , only 37% of AI tools current from reaching before their safety assessment processes there is .

Uzbekistan for recommendations

1. Legislation base reinforcement

In 2022 acceptance made Cyber security about law implementation mechanisms develop necessary .



2. International cooperation

Central Eurasia Cyber Security Summit such as events through regional cooperation strengthen .

3. Personnel preparation

Universities and profession in colleges cyber security experts preparation programs expansion .

Global trends and future forecasts

In 2025 finance institutes for cyber security landscape fast in development continue will be . Home directions :

1. **Cybersecurity as a Service (CaaS)** models wide spread
2. **Zero Trust** architecture current to be
3. **Quantum cryptography** technologies transition
4. **AI- driven** security solutions development

Conclusion

Research to the results according to , banking in the sector cyber security issue global on a scale the most current from problems one is . By 2025 global cyberspace crime damage volume of 10.5 trillion dollars to reach forecast this of the matter seriousness shows .

REFERENCES

1. CyberCrime Magazine. (2025). *Global Cybercrime Costs Projected to Reach \$10.5 Trillion Annually by 2025*
2. DashDevs . (2024). *Banking Cybersecurity Challenges: Threats & Solutions for 2025*
3. Financial Services Information Sharing and Analysis Center. (2024). *Cybersecurity Budget Survey*
4. IMF Finance & Development. (2021). *The Global Cyber Threat to Financial Systems*
5. Uzbekistan Internal affairs ministry Cyber crimes center . (2025). *Cyber crimes statistics*



6. UpGuard . (2025). *The 6 Biggest Cyber Threats for Financial Services in 2025*
7. World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*
8. Special Eurasia. (2025). *Rising Cybercrime Alarms Uzbekistan's National Security*