PROSPECTS FOR IMPLEMENTING CYBERSECURITY OUTSOURCING

Uzakov Ortik Shaymardanovich
Karshi State Technical University "Optical Communication Systems and Networks" Associate Professor of the Department
https://doi.org/10.5281/zenodo.17912075

Abstract. *Over the past five years, the Managed Security Service Provider (MSSP) market has been growing at an annual rate of 12-15% as a global and local perspective for the introduction of cybersecurity outsourcing services around the world. The requirements for cybersecurity are increasing sharply as part of the digital economy development strategy in Uzbekistan. This article examines the benefits, risks, regulatory and legal compliance of cybersecurity outsourcing, internal and external outsourcing, financial performance assessment, and real-world scenarios for IT enterprises.*

Keywords*: Cybersecurity outsourcing, MSSP, SOC-as-a-Service, digital transformation, digital economy, cyber threat, information and cloud security, data security, development strategy, remote management.*

Annotatsiya. *So'nggi besh yil ichida dunyo bo'yicha kiberxavfsizlik xizmatlari outsorsingini joriy etishning global va mahalliy istiqbollari sifatida Managed Security Service Provider (MSSP) bozorida yillik 12-15%ga o'sish kuzatilmoqda. O'zbekistonda raqamli iqtisodiyotni rivojlantirish strategiyasi doirasida kiberxavfsizlikka qo'yilayotgan talablar keskin oshmoqda. Ushbu maqolada kiberxavfsizlik outsorsingining afzalliklari, xavf-xatarlari, me'yoriy-huquqiy jihatdan moslashuvi, ichki va tashqi outsorsing, moliyaviy samaradorlikni baholash va IT korxonalari uchun real ssenariylar ko'rib chiqiladi.*

Kalit so'zlar*: Kiberxavfsizlik outsorsingi, MSSP, SOC-as-a-Service, raqamli transformatsiya, raqamli iqtisodiyot, kibertahdid, axborot va bulut xavfsizligi, ma'lumotlar xavfsizligi, taraqqiyot strategiyasi, masofaviy boshqaruv.*

Абстрактный. *За последние пять лет рынок поставщиков управляемых услуг безопасности (MSSP) рос на 12-15% в год, что отражает глобальную и локальную перспективу внедрения услуг аутсорсинга в сфере кибербезопасности по всему миру. В рамках стратегии развития цифровой экономики в Узбекистане резко возросли требования к кибербезопасности. В данной статье рассматриваются преимущества, риски, нормативно-правовые аспекты аутсорсинга в сфере кибербезопасности, внутреннего и внешнего аутсорсинга, оценка финансовых показателей и реальные сценарии для ИТ-предприятий.*

Ключевые слова: *Аутсорсинг в сфере кибербезопасности, MSSP, SOC-as-a-Service, цифровая трансформация, цифровая экономика, киберугрозы, информационная и облачная безопасность, безопасность данных, стратегия развития, удаленное управление.*

INTRODUCTION

Cybersecurity outsourcing is the process of outsourcing some or all of an organization's internal security functions to an external specialist (MSSP/MDR/vCISO Services) or provider

(outsourcer). These providers offer services such as monitoring, threat detection and response, vulnerability management, auditing, and compliance support.

If internal security resources are limited, hiring qualified security professionals or external cybersecurity experts with specialized expertise is a good fit for the organization. Businesses in highly regulated industries may be able to use external cybersecurity services to ensure data security.

Organizations use cybersecurity outsourcing for a variety of reasons, including:

small businesses turn to external cybersecurity to gain enterprise-level security capabilities without the high costs of building internal teams;

mid-market companies often take a hybrid approach to cybersecurity, needing some security functions while outsourcing specialized needs;

mega enterprises use external experts to fill specific gaps in their security programs, while organizations in highly regulated industries work with specialized outsource partners to ensure compliance.

REVIEW OF LITERATURE ON THE SUBJECT

Based on the Decree of the President of the Republic of Uzbekistan No. PQ-60 dated January 28, 2022 "On the Development Strategy of New Uzbekistan for 2022 - 2026", the "Cybersecurity Strategy of the Republic of Uzbekistan for 2023 - 2026" was developed and tasks for the sector were defined [1].

According to Gartner's 2024 Magic Quadrant for Managed Security Services, enterprises will outsource more than 50% of their cybersecurity budgets by 2028. According to Cybersecurity Ventures and IDC's 2025 Worldwide Managed Security Services Forecast, the MSSP market in the Central Asia region is projected to grow at a CAGR of 28% from 2023 to 2028 [2].

According to Kaspersky Lab's 2024 IT Security Economics report, Central Asian businesses suffered an average of $1.2 million in losses from cyberattacks, and 68% of respondents to a local survey by the ISACA Tashkent Chapter complained about a lack of qualified cybersecurity personnel.

RESEARCH METHODOLOGY

The study included statistical analysis, expert evaluation, using monographic, expert and systematic analysis methods, the problems of implementing processes for the implementation of cybersecurity outsourcing systems in enterprises, the main directions of information security policy actions of enterprises, the processes of protecting and managing information systems and improving their cybersecurity mechanisms, and the effective organization of reliable protection processes for enterprise information systems were analyzed and proposals for effective solutions were prepared.

ANALYSIS AND RESULTS

According to a report by Cybersecurity Ventures, the annual cost of global cybercrime is expected to exceed $10.5 trillion by 2025. At the same time, according to ISC² research, the global shortage of qualified cybersecurity professionals has exceeded 4 million people. In such conditions, enterprises are forced to outsource cybersecurity to external providers instead of creating a complete protection system with their own internal resources [3].

The global cybersecurity outsourcing market is expected to be worth approximately $70-80 billion in 2025, and is expected to exceed $100 billion by 2028, with a compound annual growth rate (CAGR) of 10-12%. The main reasons for the rapid growth of cybersecurity outsourcing are the 75% increase in the number of cyberattacks in 2024 and the shortage of qualified specialists (70% of companies complain about staff shortages) [4].

Fortune 500 companies (72%) outsource at least some of their cybersecurity, and the MSSP market is expected to grow 2x between 2020 and 2025 due to GDPR requirements in the European Union, according to a 2024 report. The Asia-Pacific region is witnessing a 4x growth in cybersecurity outsourcing.

As of 2024, more than 43 thousand web resources and more than 1.8 million legal entities in Uzbekistan are connected to e-government and digital economy systems. In 2023-2025, more than 300 significant cyber incidents were recorded in state bodies and large enterprises. The lack of personnel and high costs for creating internal cybersecurity units indicate the relevance of the outsourcing model [5].

Considering that it takes 5-7 years to train qualified personnel in the field of cybersecurity, and that the IT budget of an enterprise is on average 1.5-3% per year, the number of cyberattacks in the rapidly developing digital banking and fintech sectors is expected to increase 4 times in 2023-2025. Therefore, it is expected that 60-70% of cybersecurity will be implemented through external providers in 2025-2030 [6].

Cybersecurity outsourcing is when a company or organization outsources its cybersecurity functions to a specialized external provider, rather than having to completely manage them in-house, such as 24/7 monitoring, early threat detection, incident response, security posture enforcement, log file analysis, and other processes. Such providers are commonly referred to as “MSSPs.” They provide security experts, cutting-edge tools, expertise, and processes.

“SOC as a Service” is a combination of processes, real-time monitoring, log analysis, automated alerting, threat detection, and response in the form of a service.

Today, due to the digitalization of economic sectors, the widespread implementation of AI/ML, and remote management technologies, the demand for cybersecurity is increasing globally. In this regard, many companies find it convenient to resort to outsourcing instead of forming an internal team. AI-based threat detection, automated warning systems, and threat intelligence integrations are becoming widespread among providers. As threat response, auditing, and regulatory requirements increase, the demand for services such as quality of service assurance, standards compliance, and logging by outsourcing providers is increasing [7].

Table 1

Types and models of cybersecurity outsourcing

	Service type	Brief description	Suitability for Uzbekistan
1	Managed Detection and Response (MDR)	24/7 monitoring, threat detection and response	high
2	Security Operations Center as-a-Service (SOCaaS)	full external SOC (SIEM + SOAR + Threat Intelligence)	medium, high
3	Vulnerability Management as-a-Service	continuous scanning and vulnerability remediation	high
4	Cloud Security Posture Management (CSPM)	cloud infrastructure protection (AWS, Azure, Yandex.Cloud)	very high
5	Incident Response Retainer	rapid intervention in the event of an emergency	high

6	Compliance-as-a-Service	Support for ISO 27001, PCI DSS, and Critical Information Infrastructure requirements	middle

Cybersecurity outsourcing is the practice of companies outsourcing their cybersecurity systems, including threat detection, data protection, incident response, alert system management, and remote service provision, to external providers [8].

Table 2

Benefits of Cybersecurity Outsourcing

Advantage	Description
Access to qualified expertise	Outsourcing providers typically work with a team of experts with extensive experience, certifications, and expertise. This gives a company more expertise than hiring one or more security experts in-house.
Cost optimization	Equipment, licenses, regular salary, training, design for building a SOC within the enterprise
24/7 monitoring and quick response	Cyber threats don't just happen during business hours. With SOC-aaS, continuous monitoring, log analysis, and rapid response to threats and protection systems are dependent on continuous operation, even on weekends.
Modern technologies and threat intelligence	Outsourcing providers often use the latest SIEM, EDR, automation, AI/ML analytics, ARP, Threat intelligence platforms that can be difficult for internal departments to achieve.
Flexibility and scalability	As the business network expands or the infrastructure changes, the provider can easily expand the scope of its services. This is especially convenient for small and medium-sized businesses.
Compliance and audit compliance	Many providers will have expertise in international standards (e.g., ISO 27001, PCI DSS, GDPR analogs) and manage processes such as audits, logging, reporting
Data privacy	NDA + organization and optimization of encrypted channels
Provider reliability	Service providers' SOC 2 Type II, ISO 27001 certification compliance
Lock-in effect	hybrid model working with multiple providers
Compliance with national legislation	Conducting OWASP systems audits for “critical” objects

In an organization, security operations is the part of the IT department responsible for monitoring, detecting, investigating, and responding to a wide range of cyber threats. An organization needs to ensure the ideal alignment of people, processes, and technologies for security operations [9].

Table 3

Comparative analysis of internal and external cybersecurity outsourcing

Section	Internal cybersecurity	External Cybersecurity (MSSP)
Initial investment	high initial capital costs; infrastructure setup costs;	minimum initial investment; reduction in capital expenditures;

	purchase of safety equipment; special place and conditions are required.	pay-as-you-go model; rapid implementation.
Budget structure	capital expenditures; periodic technology investments; unexpected expenses; Technology updates always require money.	operating expenses; fixed monthly/annual subscription fee; predetermined costs; Financial planning is easy.
Personnel costs	full salary for specialists; benefits and overhead; recruitment costs; employee retention bonuses; training costs.	low cost due to resource sharing; personnel costs are borne by MSSP; recruitment and retention costs in MSSP; Training costs are covered by MSSP.
Operating expenses	24/7 staffing is required; overtime pay in incidents; continuous training; maintenance costs; reserve personnel for important positions.	cheaper due to large scale; 24/7 monitoring service; incident response is in the SLA; The tools are managed by the MSSP; backup is within the service.
Scaling costs	with growth, the cost increases sharply; new people are needed; the purchase of new equipment is necessary; The cost increases with complexity.	flexible scaling; the cost increases slightly as it grows; payment only for the service used; easy to increase service.
Technology costs	full purchase of equipment; regular maintenance; systems integration costs; new version purchases; risk of technology obsolescence.	enterprise-level tools at a low price; Technology costs are shared; constant updates within the service; use of the latest technologies; there is no risk of wear and tear.
Training and expertise	constant training is necessary; certification costs; conference expenses; Loss of knowledge due to employee turnover; limited experience.	training costs are covered by MSSP; extensive expertise; employee turnover is not a problem; experience in many threats; specialized experts are available.
Hidden costs	productivity decreases in incidents; knowledge is lost when an employee leaves; security management will be a burden; Coverage gaps during the transition period; lots of documentation required.	contract management costs; restrictions on requirements; there may be special setup costs; provider switching costs; early termination penalties.
Total costs	too expensive for small companies; large investment in specialists and technology;	cheaper for most organizations;

	Costs in incidents are variable; cost increases with increasing expertise; cost increases with increasing complexity.	stable subscription costs; economies of scale; inexpensive special expertise; access to a wide range of opportunities at an affordable price.

The following can be highlighted as practical recommendations for Uzbek businesses, including:

launch 24/7 monitoring of SI-MDR, Vulnerability Management services in small and medium-sized businesses (50% cost savings);

SOCaaS in banks, Central Bank expertise, integration of hybrid models;

introduction of assessment in state-owned enterprises by the Cybersecurity Center, external CSPM, and rating criteria;

Implementing blockchain CSPM, compliance-as-a-service systems for personal data in fintech and the digital economy;

Strengthen internal teams with cybersecurity graduates [10].

CONCLUSIONS AND SUGGESTIONS

Cybersecurity outsourcing is not only an economic but also a strategic necessity for Uzbekistan. With the right choice of provider and legal considerations, companies can save up to 50-70% of the resources spent on building an internal team, and increase the speed of response by 10 times.

It is expected that by 2026, a sufficient number of local MSSPs will appear in the country. Until then, the most optimal approach was to use a hybrid model of Kaspersky, Group-IB, Positive Technologies, and local providers.

Internal cybersecurity focuses on supporting the technological processes of managed IT services, while external cybersecurity optimizes security threats, vulnerabilities, and compliance. While a managed IT provider may maintain systems and implement basic security measures, a dedicated cybersecurity provider offers and implements specialized expertise in threat detection, incident response, and advanced security functions.

LIST OF REFERENCES USED

1. Gartner. Magic Quadrant for Managed Security Services, 2024.
2. Cybersecurity Ventures. Cybercrime Report, 2025.
3. IDC Worldwide Managed Security Services Forecast, 2024-2028.
4. Kaspersky. IT Security Economics, 2024.
5. Deloitte. Global Cybersecurity Survey, 2024.
6. ISACA. State of Cybersecurity, 2024.
7. O.Sh. Uzakov, “Innovative factors in preventing cyber threats in digital transformation". Special issue of the scientific electronic journal Digital Economy. OAV№0237, ISSN 2181-4430, pp. 1862-1868.

8. O.Sh. Uzakov, “Logistics outsourcing of business processes”. Marketing Scientific, Practical and Popular Journal, July 2025, No. 7, No. 240874. ISSN: 3060-4621, international level 9710, electronic edition, July 31, pp. 70-77.
9. O.Sh. Uzakov, “Software product logistics”. Engineering and Economics Socio-economic, Innovative Technical, Scientific and Practical Journal of Science and Education, July 2025, No. 7, pp. 30-34. ORCID 0009-0005-0456-1432
10. O.Sh. Uzakov, “Implementation of logistics information systems into technological processes". Green Economy and Development Social, Economic, Technological, Scientific, Popular Journal, ISSN: 2992-8982, July 2025, Issue No. 7, pp. 330-335. ORCID 0009-0005-0456-1432
11. Shaymardanovich UO Analysis of cybersecurity vulnerabilities in the digital economy //Intellectual education technological solutions and innovative digital TOOLS. - 2024. - T. 3. - No. 28. - P. 88-92.