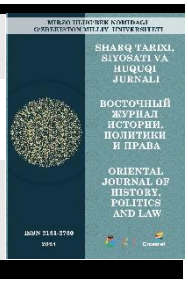
DOI: https://doi.org/10.37547/supsci-ojhpl-06-04-75 **Pages: 678-695**

Oriental Journal of History, Politics and Law

SUPPORT SCIENCE

ORIENTAL JOURNAL OF HISTORY, POLITICS AND LAW

journal homepage:
https://www.supportscience.uz/index.php/ojhpl



NEW CHALLENGES OF REGIONAL SECURITY: CYBER THREATS AND DIGITAL TRANSFORMATION

Saodat Ubaydullaeva
Tashkent State University of Oriental Studies
E-mail: sadulya75@mail.ru
Tashkent, Uzbekistan

ABOUT ARTICLE

Key words: Cybersecurity, cyber threats, digital transformation, regional security, artificial intelligence, information warfare, digital governance, cybercrime, cyberspace, digital security.

Received: 05.04.26
Accepted: 06.04.26
Published: 07.04.26

Abstract: Digital technologies have become part of almost every sphere of modern life. Governments, banks, educational institutions, healthcare systems, and businesses now depend heavily on internet-based platforms and digital communication. Because of this dependence, questions of cybersecurity and regional stability have become more important than before. Alongside the advantages of digital transformation, new risks and security problems have also appeared. Cyber attacks, online fraud, information leakage, digital espionage, and manipulation through social media are now common challenges for many countries and regions.

This article examines the connection between cyber threats and regional security in the context of digital transformation. The study focuses on how modern technologies influence security systems and how cyber threats affect political, economic, and social stability. Attention is also given to artificial intelligence, information warfare, online communication platforms, and the growing role of cyberspace in international relations.

The research is based on analytical, descriptive, and comparative methods. Academic articles, international reports, statistical materials, and recent studies related to cybersecurity and digital technologies were reviewed during the research process.

Different examples of cyber incidents and digital security problems were also analyzed.

The study shows that digital transformation creates both opportunities and vulnerabilities. Digital technologies improve communication, simplify administrative processes, support economic development, and expand access to information. At the same time, the growth of digital infrastructure increases the risk of cyber attacks and information manipulation. Modern cyber threats target not only individuals but also state institutions, transport systems, energy networks, and financial organizations.

The research also shows that artificial intelligence is becoming an important factor in cybersecurity. AI technologies help detect suspicious activity, process large amounts of information, and strengthen cyber defense systems. However, the same technologies may also be used for harmful purposes, including automated attacks, fake digital content, and large-scale misinformation campaigns.

Another important issue is the growing influence of information warfare. Social media and digital platforms make it possible to spread false information very quickly. In some cases, this influences public opinion, increases social tension, and creates political instability. Because of this, cybersecurity today includes not only technical protection but also information security and digital awareness.

The article concludes that regional security in the digital era requires stronger cybersecurity systems, international cooperation, technological modernization, and wider digital education. Cyber threats continue to evolve together with technology, therefore security policies must also adapt to new conditions and challenges.

MINTAQAVIY XAVFSIZLIKNING YANGI CHAQIRIQLARI: KIBER TAHDIDLAR VA RAQAMLI TRANSFORMATSIYA

Saodat Ubaydullayeva
Toshkent davlat sharqshunoslik universiteti
E-mail: sadulya75@mail.ru
Toshkent, O‘zbekiston

MAQOLA HAQIDA

Kalit so‘zlar: Kiberxavfsizlik, kiber tahdidlar, raqamli transformatsiya, mintaqaviy xavfsizlik, sun’iy intellekt, axborot urushi, raqamli boshqaruv, kiberjinoyatchilik, kiber makon, raqamli xavfsizlik.

Annotatsiya: Raqamli texnologiyalar zamonaviy hayotning deyarli barcha sohalarining ajralmas qismiga aylandi. Hukumatlar, banklar, ta’lim muassasalari, sog‘liqni saqlash tizimlari va biznes tuzilmalari bugungi kunda internetga asoslangan platformalar hamda raqamli kommunikatsiyaga katta darajada bog‘liqdir. Shu sababli, kiberxavfsizlik va mintaqaviy barqarorlik masalalari avvalgidan ham muhimroq ahamiyat kasb etmoqda. Raqamli transformatsiyaning afzalliklari bilan bir qatorda yangi xavf va xavfsizlik muammolari ham paydo bo‘lmoqda. Kiberhujumlar, onlayn firibgarlik, ma’lumotlarning sizib chiqishi, raqamli josuslik va ijtimoiy tarmoqlar orqali manipulyatsiya bugungi kunda ko‘plab davlatlar va mintaqalar uchun odatiy muammolarga aylangan.

Mazkur maqola raqamli transformatsiya sharoitida kiber tahdidlar va mintaqaviy xavfsizlik o‘rtasidagi bog‘liqlikni o‘rganadi. Tadqiqot zamonaviy texnologiyalar xavfsizlik tizimlariga qanday ta’sir ko‘rsatayotgani hamda kiber tahdidlar siyosiy, iqtisodiy va ijtimoiy barqarorlikka qanday ta’sir qilayotganiga qaratilgan. Shuningdek, sun’iy intellekt, axborot urushi, onlayn kommunikatsiya platformalari va xalqaro munosabatlarda kiber makonning ortib borayotgan roliga alohida e’tibor qaratilgan.

Tadqiqot tahliliy, tavsifiy va qiyosiy metodlarga asoslangan. Tadqiqot jarayonida kiberxavfsizlik va raqamli texnologiyalar bilan bog‘liq ilmiy maqolalar, xalqaro hisobotlar, statistik materiallar va so‘nggi tadqiqotlar o‘rganildi. Shuningdek, turli kiber hodisalar va raqamli xavfsizlik muammolari misollari ham tahlil qilindi.

Tadqiqot natijalari shuni ko‘rsatadiki, raqamli transformatsiya bir vaqtning o‘zida ham imkoniyatlar, ham zaifliklarni yuzaga keltiradi. Raqamli texnologiyalar kommunikatsiyani yaxshilaydi, ma’muriy jarayonlarni soddalashtiradi, iqtisodiy rivojlanishni qo‘llab-quvvatlaydi va axborotdan foydalanish imkoniyatlarini kengaytiradi. Shu bilan birga, raqamli

infratuzilmaning rivojlanishi kiberhujumlar va axborotni manipulyatsiya qilish xavfini oshiradi. Zamonaviy kiber tahdidlar nafaqat alohida shaxslarni, balki davlat institutlari, transport tizimlari, energetika tarmoqlari va moliyaviy tashkilotlarni ham nishonga olmoqda.

Tadqiqot shuningdek, sun'iy intellekt kiberxavfsizlikning muhim omiliga aylanib borayotganini ko‘rsatadi. Sun'iy intellekt texnologiyalari shubhali faoliyatni aniqlash, katta hajmdagi ma'lumotlarni qayta ishlash va kiberhimoya tizimlarini mustahkamlashga yordam beradi. Biroq ayni texnologiyalar zararli maqsadlarda ham qo‘llanilishi mumkin, jumladan avtomatlashtirilgan hujumlar, soxta raqamli kontent yaratish va keng ko‘lamli dezinformatsiya kampaniyalarida foydalanilishi ehtimoli mavjud.

Yana bir muhim masala — axborot urushining kuchayib borayotgan ta'siridir. Ijtimoiy tarmoqlar va raqamli platformalar yolg‘on ma'lumotlarni juda tez tarqatish imkonini beradi. Ayrim hollarda bu jamoatchilik fikriga ta'sir ko‘rsatadi, ijtimoiy keskinlikni kuchaytiradi va siyosiy beqarorlikni yuzaga keltiradi. Shu sababli bugungi kunda kiberxavfsizlik nafaqat texnik himoyani, balki axborot xavfsizligi va raqamli savodxonlikni ham o‘z ichiga oladi.

Maqolada xulosa qilinishicha, raqamli davrda mintaqaviy xavfsizlikni ta'minlash uchun kiberxavfsizlik tizimlarini kuchaytirish, xalqaro hamkorlikni rivojlantirish, texnologik modernizatsiya va keng qamrovli raqamli ta'limni yo‘lga qo‘yish zarur. Kiber tahdidlar texnologiyalar bilan birga rivojlanishda davom etmoqda, shu sababli xavfsizlik siyosati ham yangi sharoit va chaqiriqlarga moslashib borishi kerak.

НОВЫЕ ВЫЗОВЫ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ: КИБЕРУГРОЗЫ И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

Саодат Убайдуллаева
Ташкентский государственный университет востоковедения
E-mail: sadulya75@mail.ru
Ташкент, Узбекистан

О СТАТЬЕ

Ключевые слова: Кибербезопасность, киберугрозы, цифровая трансформация, региональная безопасность, искусственный интеллект, информационная война, цифровое управление, киберпреступность, киберпространство, цифровая безопасность.

Аннотация: Цифровые технологии стали частью практически всех сфер современной жизни. Государственные органы, банки, образовательные учреждения, системы здравоохранения и бизнес сегодня в значительной степени зависят от интернет-платформ и цифровой коммуникации. В связи с этой зависимостью вопросы кибербезопасности и региональной стабильности приобретают всё большее значение. Наряду с преимуществами цифровой трансформации появляются и новые риски, а также проблемы безопасности. Кибератаки, онлайн-мошенничество, утечка информации, цифровой шпионаж и манипуляции через социальные сети стали распространёнными вызовами для многих государств и регионов.

Данная статья рассматривает взаимосвязь между киберугрозами и региональной безопасностью в условиях цифровой трансформации. Исследование сосредоточено на том, как современные технологии влияют на системы безопасности и каким образом киберугрозы воздействуют на политическую, экономическую и социальную стабильность. Особое внимание уделяется искусственному интеллекту, информационной войне, онлайн-коммуникационным платформам и растущей роли киберпространства в международных отношениях.

Исследование основано на аналитическом, описательном и сравнительном методах. В ходе исследования были изучены научные статьи, международные отчёты, статистические материалы и современные исследования, связанные с кибербезопасностью и цифровыми технологиями. Также были проанализированы различные примеры киберинцидентов и проблем цифровой безопасности.

Результаты исследования показывают, что цифровая трансформация

создаёт одновременно как возможности, так и уязвимости. Цифровые технологии улучшают коммуникацию, упрощают административные процессы, способствуют экономическому развитию и расширяют доступ к информации. В то же время рост цифровой инфраструктуры увеличивает риск кибератак и информационных манипуляций. Современные киберугрозы нацелены не только на отдельных людей, но и на государственные учреждения, транспортные системы, энергетические сети и финансовые организации.

Исследование также показывает, что искусственный интеллект становится важным фактором кибербезопасности. Технологии искусственного интеллекта помогают выявлять подозрительную активность, обрабатывать большие объёмы информации и укреплять системы киберзащиты. Однако те же технологии могут использоваться и в вредоносных целях, включая автоматизированные атаки, создание фальшивого цифрового контента и масштабные кампании по дезинформации.

Ещё одной важной проблемой является растущее влияние информационной войны. Социальные сети и цифровые платформы позволяют очень быстро распространять ложную информацию. В некоторых случаях это влияет на общественное мнение, усиливает социальную напряжённость и создаёт политическую нестабильность. Поэтому сегодня кибербезопасность включает не только техническую защиту, но и информационную безопасность, а также цифровую грамотность.

В статье делается вывод о том, что региональная безопасность в цифровую эпоху требует усиления систем кибербезопасности, международного сотрудничества, технологической модернизации и расширения цифрового образования. Киберугрозы продолжают развиваться вместе с технологиями, поэтому политика безопасности также

должна адаптироваться к новым условиям и вызовам.

Introduction. The modern world is closely connected with digital technologies. Over the last few decades, the internet, computer systems, mobile technologies, and digital communication platforms have become an essential part of everyday life. Today people use digital technologies not only for communication but also for education, healthcare, banking, trade, public administration, and international cooperation. Because of this rapid technological development, societies and governments are becoming increasingly dependent on digital systems and online infrastructure.

The digital era has changed the way states function and interact with society. Many government services are now provided through electronic platforms, while businesses depend on online systems for financial operations, communication, and data storage. Educational institutions use digital learning technologies, and healthcare systems actively apply electronic databases and online services. This process is usually described as digital transformation. Digital transformation means the integration of digital technologies into social, political, and economic systems. It affects not only technology itself but also human behavior, communication, management, and security.

At the same time, the expansion of digital systems has created new risks and vulnerabilities. As societies become more dependent on digital infrastructure, cyber threats are becoming more dangerous and widespread. Cybersecurity has therefore become one of the key issues of modern regional and international security. In recent years, the number of cyber attacks has increased significantly across the world. Governments, banks, hospitals, universities, transport systems, and private companies are frequent targets of cybercrime and digital attacks.

Cyber attacks can lead to financial losses, information leakage, disruption of public services, and damage to critical infrastructure. Modern cyber threats include hacking, phishing, malware, ransomware, identity theft, cyber espionage, and attacks on communication systems. Some cyber attacks are carried out by criminal organizations, while others may be connected with political conflicts and international competition. Because of this, cybersecurity today is no longer only a technical issue; it has become an important part of national and regional security policy.

One of the most serious challenges in the digital era is the growth of information warfare. Social media platforms and online communication systems make it possible to spread information very quickly. However, these technologies are also used to distribute fake news, propaganda, manipulated content, and disinformation. False information can influence public opinion, increase

political tension, and create instability in society. Information warfare has therefore become one of the most important tools of modern geopolitical competition.

Another major issue is the protection of critical infrastructure. Energy systems, banking networks, transport systems, communication channels, and healthcare databases are highly dependent on digital technologies. Cyber attacks on such systems may create serious social and economic consequences. In some cases, attacks on critical infrastructure can affect entire regions and threaten national stability.

Artificial intelligence is also changing the nature of cybersecurity and cyber threats. AI technologies help organizations detect suspicious activity, process large amounts of information, and improve cyber defense systems. However, the same technologies can also be used for harmful purposes, including automated cyber attacks, deepfake production, and digital manipulation. The growing influence of artificial intelligence in cyberspace creates new challenges for governments and international security organizations.

Regional security in the digital age is no longer limited to military conflicts and territorial disputes. Modern threats are increasingly connected with cyberspace, digital communication, and information technologies. As a result, many states are investing more resources into cybersecurity systems, digital defense strategies, and international cyber cooperation.

The topic of cyber threats and digital transformation has become especially important in recent years because modern societies cannot function effectively without digital infrastructure. Cybersecurity today affects governments, businesses, public institutions, and ordinary users. The increasing number of cyber incidents shows that digital security has become one of the main priorities of regional and international security systems.

Literature Review. The rapid development of digital technologies and the expansion of cyberspace have become one of the most discussed topics in modern academic research. Many scholars note that digital transformation has changed not only economic and social systems but also approaches to security and international stability. Modern societies are becoming increasingly dependent on digital infrastructure, which creates both new opportunities and serious cybersecurity risks.

Recent studies show that digital transformation improves communication, management systems, financial operations, and access to information. At the same time, researchers emphasize that increasing digital dependence creates new vulnerabilities connected with cyber threats, data leakage, and attacks on critical infrastructure. Saeed et al. point out that businesses and public institutions are becoming more vulnerable to cyber attacks because modern digital systems store

large amounts of sensitive information and depend heavily on interconnected technologies (Saeed et al., 2023). Similar ideas are discussed by Serac, who explains that digital transformation increases organizational exposure to cyber risks and requires stronger cybersecurity strategies and protection systems (Serac, 2023).

Researchers also pay significant attention to cybersecurity risk management. According to Haque et al., cyber threats in the digital era are becoming more complex and organized, especially with the rapid growth of cloud technologies, artificial intelligence, and online platforms. The authors note that cybersecurity today is not limited to technical protection because human behavior, organizational management, and digital awareness also influence cyber resilience (Haque et al., 2025).

The relationship between digital transformation and regional security is another important topic in recent literature. Scholars argue that cyber threats can affect not only individual organizations but also entire regions and state systems. Attacks on banking networks, transport infrastructure, healthcare systems, and communication channels may create economic instability and social tension. Because of this, many countries now consider cybersecurity one of the main components of national and regional security policy.

Studies related to Uzbekistan also show that digital transformation creates both positive changes and new challenges. Urinboyev and Khusainova explain that the process of digitalization in Uzbekistan supports economic modernization, electronic governance, and technological development, but at the same time increases the need for stronger digital protection systems and cybersecurity regulation (Urinboyev & Khusainova, 2025). Maksudov also emphasizes that cybersecurity and data privacy are becoming increasingly important in Uzbekistan because modern digital systems require reliable protection against cyber attacks and unauthorized access to information (Maksudov, 2024).

Artificial intelligence and information warfare are also widely discussed in recent academic works. Researchers note that AI technologies can improve cyber defense systems by detecting suspicious activity and analyzing large amounts of information more efficiently. However, artificial intelligence may also be used for cybercrime, automated attacks, deepfake production, and online manipulation. Because of this, the role of AI in cybersecurity is often described as both beneficial and risky.

Another major issue discussed in modern studies is information warfare and the spread of misinformation through social media platforms. Fake news, manipulated digital content, and propaganda campaigns may influence public opinion and create political instability. Several

scholars argue that cyberspace has become an important field of geopolitical competition where states, organizations, and non-state actors attempt to influence social and political processes through digital communication technologies.

Although many studies examine cybersecurity and digital transformation separately, fewer works focus on their combined influence on regional security. The rapid development of technology continuously creates new forms of cyber threats, which means that cybersecurity strategies also need constant modernization. This makes the relationship between cyber threats, digital transformation, and regional security an important area for further research figure 1.

Figure 1. Distribution of Major Cybersecurity Risks in the Process of Digital Transformation

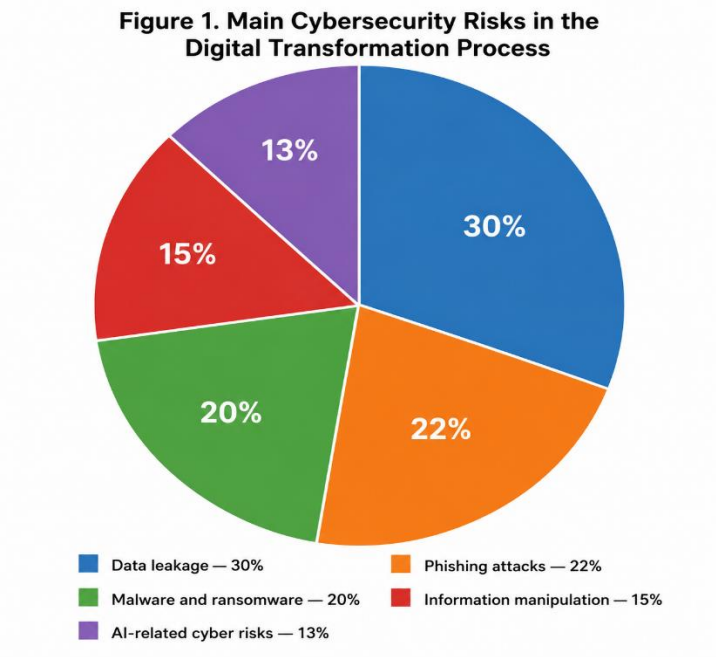


Figure 1 shows the main cybersecurity risks that appear during the process of digital transformation. According to the chart, data leakage represents the largest category with 30%. This indicates that unauthorized access to confidential information and personal data remains one of the most serious problems in modern digital systems. The growing use of online platforms, cloud technologies, and digital databases increases the possibility of information exposure and privacy violations.

Phishing attacks account for 22% of cyber risks. This type of attack usually targets users through fake emails, websites, or messages in order to steal passwords, banking information, or

other sensitive data. The high percentage demonstrates that social engineering remains one of the most common methods used by cybercriminals.

Malware and ransomware make up 20% of the identified risks. These attacks involve harmful software that damages systems, blocks access to information, or demands payment for restoring digital data. The spread of malware continues to threaten businesses, government institutions, and individual users.

Information manipulation represents 15% of the chart. This category includes fake news, propaganda, misleading digital content, and online disinformation campaigns. Such activities may influence public opinion, create social tension, and affect political stability, especially during periods of conflict or elections.

AI-related cyber risks account for 13% of the total. Although this percentage is smaller compared to other categories, it reflects the growing influence of artificial intelligence in cyberspace. AI technologies can be used for automated attacks, deepfake creation, and advanced digital manipulation, creating new challenges for cybersecurity systems.

Overall, the figure demonstrates that digital transformation brings not only technological progress but also significant cybersecurity challenges. The results highlight the importance of stronger digital protection systems, cybersecurity awareness, and international cooperation in reducing modern cyber risks.

Research Methods. This study examines the relationship between cyber threats, digital transformation, and regional security. The research is based on qualitative and analytical approaches because the topic requires detailed examination of modern cybersecurity challenges, technological changes, and their influence on society and state security systems.

During the research process, descriptive analysis was widely used. This method helped explain the main concepts connected with cybersecurity, digital transformation, information warfare, and regional security. Different forms of cyber threats such as phishing, malware, ransomware, cyber espionage, and information manipulation were analyzed through descriptive interpretation. Researchers note that analytical approaches are especially important in cybersecurity studies because modern cyber risks constantly evolve together with technological development (Haque et al., 2025).

Comparative analysis was another important method used in this research. Different scientific views and approaches related to cybersecurity and digital transformation were compared in order to identify similarities and differences between existing studies. The experiences of different countries and regions in the field of cybersecurity were also examined. Comparative

analysis made it possible to observe how digital transformation affects security systems in different social and political environments. Similar approaches are frequently used in studies related to digital security and cyber resilience (Serac, 2023).

Content analysis was applied to scientific articles, academic publications, reports, and digital materials related to cybersecurity and regional security. This method helped identify the most common themes, risks, and challenges discussed in recent literature. Special attention was given to studies published between 2021 and 2025 because cybersecurity technologies and digital systems develop rapidly, and recent information is especially important for understanding modern cyber threats.

The study also used statistical and graphical materials collected from academic publications and cybersecurity reports. Pie charts, tables, and analytical data were included in order to demonstrate the distribution of cyber risks and the influence of digital transformation on different sectors. These materials helped present the information more clearly and supported the analytical part of the research. Saeed et al. emphasize that statistical assessment and risk analysis are important for understanding modern cybersecurity vulnerabilities in digital environments (Saeed et al., 2023).

The theoretical basis of the research is connected with modern studies in cybersecurity, information technology, digital governance, and regional security. Scientific works discussing artificial intelligence, cyberspace, cybercrime, and information warfare were analyzed as part of the literature review. Particular attention was paid to studies examining the risks created by digital dependence and online communication technologies. According to Maksudov, cybersecurity and data privacy are becoming increasingly important in countries undergoing active digital transformation because digital systems require stronger protection mechanisms and legal regulation (Maksudov, 2024).

The research process included several stages. At the first stage, scientific literature and digital sources related to cybersecurity and regional security were collected and reviewed. At the second stage, the selected materials were analyzed and grouped according to their thematic relevance. The final stage focused on interpretation of the collected information and formulation of conclusions regarding the impact of cyber threats on regional security in the context of digital transformation.

The chosen methods made it possible to examine the topic from different perspectives and provide a broader understanding of modern cybersecurity challenges. Since cyber threats continue

to evolve together with technological progress, analytical and comparative approaches were considered the most appropriate methods for this study Table 1.

Table 1. Research Methods Used in the Study

Method	Purpose	Use in the Study
Descriptive method	To explain the topic	Cyber threats and digital transformation were described
Comparative method	To compare different views	Cybersecurity approaches of different countries were compared
Content analysis	To study scientific materials	Articles, reports, and digital sources were analyzed
Analytical method	To examine relationships	The impact of cyber threats on regional security was analyzed
Statistical review	To present data clearly	Charts and cybersecurity statistics were used

Table 1 presents the main research methods used in the study. Different methods were combined in order to examine cyber threats, digital transformation, and regional security from several perspectives. Descriptive and analytical methods helped explain the main cybersecurity concepts and modern digital challenges. Comparative analysis was used to compare different approaches to cybersecurity and regional protection systems. Content analysis made it possible to study scientific articles, reports, and recent academic materials related to cyberspace and digital security. Statistical review was applied to support the research with visual and numerical data. The combination of these methods provided a broader understanding of modern cybersecurity risks and their influence on regional stability.

Results and Discussion. The research shows that digital transformation has significantly changed the nature of regional security. Modern societies are becoming increasingly dependent on digital technologies, online communication systems, and electronic infrastructure. Although digital transformation creates many opportunities for economic growth and technological development, it also increases vulnerability to cyber threats. As a result, cybersecurity has become one of the main priorities of modern states and international organizations.

One of the main findings of the study is the rapid growth of cyber threats in recent years. Cyber attacks now target not only individuals and private companies but also government institutions, healthcare systems, banking networks, transport infrastructure, and communication

systems. The increasing number of cyber incidents demonstrates that cyberspace has become an important field of political, economic, and social competition.

The analysis shows that phishing, malware, ransomware, and data leakage remain among the most widespread cybersecurity risks. Phishing attacks are especially dangerous because they often target ordinary users through fake websites, emails, or messages. Many people unknowingly provide passwords, banking information, or personal data to cybercriminals. Malware and ransomware attacks also continue to create serious financial and technical damage for organizations and institutions.

Another important result is the growing role of information warfare in modern regional security. Social media platforms and digital communication technologies make it possible to spread information almost instantly. However, these technologies are also widely used for propaganda, fake news, and online manipulation. Information attacks may influence public opinion, create political instability, and increase social tension. The study shows that information warfare is becoming one of the most powerful instruments in geopolitical conflicts.

The research also demonstrates that artificial intelligence has both positive and negative effects on cybersecurity. On the positive side, AI technologies improve cyber defense systems by detecting suspicious activity, processing large amounts of information, and responding to threats more efficiently. Many organizations now use artificial intelligence for automated monitoring and cybersecurity management.

At the same time, AI technologies also create new security risks. Deepfake videos, automated cyber attacks, and AI-based manipulation tools are becoming more common in cyberspace. Such technologies make cyber threats more complex and more difficult to detect. This creates additional challenges for governments, security organizations, and digital platforms.

Another major issue identified during the research is the vulnerability of critical infrastructure. Energy systems, healthcare institutions, transport networks, communication systems, and banking platforms are highly dependent on digital technologies. Cyber attacks targeting such infrastructure may create serious economic losses and social disruption. In some cases, cyber incidents may even affect regional stability and public safety.

The findings also show that cybersecurity awareness remains an important problem in many countries. Even strong technical systems may become vulnerable if users do not follow digital security rules. Weak passwords, unsafe online behavior, and low digital literacy often increase the risk of cyber attacks. This means that cybersecurity today depends not only on technology but also on human behavior and public awareness.

The research demonstrates that international cooperation plays an important role in cybersecurity protection. Since cyber threats cross national borders, individual states often cannot solve these problems independently. Many countries now cooperate through information exchange, cybersecurity agreements, and joint digital security programs. International organizations also actively support the development of cybersecurity strategies and digital protection systems.

Another important result is that digital transformation continuously changes the structure of regional security. Traditional security systems were mainly focused on military power and territorial conflicts, while modern threats are increasingly connected with cyberspace and information technologies. Cybersecurity therefore becomes part of economic security, political stability, and social protection.

The discussion also shows that cyber threats evolve together with technology. As new digital systems appear, new forms of cybercrime and digital manipulation also emerge. Because of this, cybersecurity strategies require constant modernization and adaptation. Governments, organizations, and educational institutions must regularly update their digital security systems and improve cybersecurity education.

Conclusion. The study shows that digital transformation has become one of the most influential factors shaping modern regional security. The rapid development of internet technologies, artificial intelligence, cloud systems, and digital communication platforms has changed political, economic, and social processes across the world. Modern societies now depend heavily on digital infrastructure, which increases both technological opportunities and cybersecurity risks.

The research demonstrates that cyber threats are becoming more complex, widespread, and dangerous. Cybercrime, phishing attacks, malware, ransomware, data leakage, and information manipulation affect not only private organizations but also governments, financial institutions, healthcare systems, and critical infrastructure. Because of this, cybersecurity can no longer be viewed only as a technical issue. It has become an important part of regional stability, national security, and international cooperation.

One of the major findings of the study is the growing influence of information warfare in cyberspace. Social media platforms and online communication systems are widely used for spreading fake news, propaganda, and manipulated digital content. Such activities may influence public opinion, increase social tension, and create political instability. This shows that modern

cybersecurity includes not only digital protection but also information security and media awareness.

The research also highlights the dual role of artificial intelligence in cybersecurity. AI technologies improve cyber defense systems by detecting suspicious activity and analyzing large amounts of data more efficiently. At the same time, AI may also be used for harmful purposes, including automated attacks, deepfake technologies, and online manipulation. This creates new security and ethical challenges for modern societies.

Another important conclusion is that digital transformation continuously changes the structure of regional security. Traditional security models focused mainly on military and territorial threats, while modern security systems increasingly depend on cyberspace and digital technologies. As a result, states and international organizations are investing more resources into cybersecurity strategies, digital defense systems, and technological modernization.

The study also confirms that cybersecurity awareness is extremely important. Even advanced technological systems remain vulnerable if users lack digital literacy and basic online security knowledge. Human behavior therefore plays a major role in preventing cyber threats and protecting digital infrastructure.

International cooperation is another key factor identified in the research. Since cyber threats often cross national borders, no country can fully solve cybersecurity problems independently. Cooperation between states, organizations, and international institutions is necessary for exchanging information, developing cybersecurity policies, and responding to modern digital risks. The study demonstrates that digital transformation creates both opportunities and vulnerabilities. Technological progress supports economic development, communication, and modernization, but at the same time increases dependence on digital systems and exposure to cyber threats. Because of this, cybersecurity will remain one of the main priorities of regional and international security in the coming years.

Future cybersecurity policies should focus on strengthening digital infrastructure, improving cybersecurity education, supporting international cooperation, and developing effective legal and technological protection systems. Continuous adaptation to technological change will be necessary because cyber threats evolve together with digital transformation.

References:

1. Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors (Basel, Switzerland), 23. https://doi.org/10.3390/s23156666.

2. Serac, C. (2023). DIGITAL TRANSFORMATION VULNERABILITIES: ASSESSING THE RISKS AND STRENGTHENING CYBER SECURITY. THE ANNALS OF THE UNIVERSITY OF ORADEA. ECONOMIC SCIENCES. https://doi.org/10.47535/1991auoes32(1)059.

3. Urinboyev, R., & Khusainova, I. (2025). CHALLENGES OF THE DIGITALIZATION PROCESS IN UZBEKISTAN. International Affairs: Politics, Economics, Law. https://doi.org/10.63407/629013.

4. Maksudov, M. (2024). The Role of Cybersecurity and Data Privacy in Uzbekistan: Safeguarding Digital Landscapes in the 21st Century. INFORMATION TECHNOLOGIES AND MANAGEMENT. https://doi.org/10.30525/978-9934-26-459-7-16.

5. Kizi, K. (2024). CYBERSECURITY IN UZBEKISTAN: PROTECTING THE DIGITAL ECONOMY. International Journal of Economic Integration and Regional Competitiveness. https://doi.org/10.61796/ijeirc.v1i6.139.

6. Farrukh, K. (2025). Uzbekistan on the Path of Digitalization. Economic Cooperation Organization Economic Journal. https://doi.org/10.71447/5by84y71.

7. Mengniyozov, A. (2026). BANK XIZMATLARINING RAQAMLI TRANSFORMATSIYASI VA KIBERXAVFSIZLIKNI TA’MINLASH MUAMMOLARI. Iqtisodiy taraqqiyot va tahlil. https://doi.org/10.60078/2992-877x-2026-vol4-iss2-pp129-139.

8. Alisherovnaга, A. (2025). Digital Transformation Of Tourism In Uzbekistan: E-Services And Tourism Safety. Journal of Management and Economics. https://doi.org/10.55640/jme-05-12-05.

9. Boburjon, S. (2025). The Formation and Development History of The Legal Foundations of Information Security Policy in The Republic of Uzbekistan. International Journal of Law And Criminology. https://doi.org/10.37547/ijlc/volume05issue06-04.

10. Boburjon, S. (2025). The Formation and Development History of The Legal Foundations of Information Security Policy in The Republic of Uzbekistan. International Journal of Law And Criminology. https://doi.org/10.37547/ijlc/volume05issue06-04.

11. Orumbayeva, M., & Kurmangali, A. (2022). CYBERSECURITY AND CURRENT GLOBAL THREATS IN CENTRAL ASIA. PUBLIC ADMINISTRATION AND CIVIL SERVICE. https://doi.org/10.52123/1994-2370-2022-657.

12. Mura, S., Yeleukhan, K., Duman, Z., & Parkhatzhan, I. (2025). China's Co-Operation with Central Asian Countries on Cyber Security. Journal of Posthumanism. https://doi.org/10.63332/joph.v5i5.1415.

13. Thommandru, A., Maratovich, F., & Saparovna, N. (2024). Fortifying Uzbekistan's Integrity Landscape: Harnessing India's Tech-Driven Anti-Corruption Strategies. Sustainable Futures. https://doi.org/10.1016/j.sftr.2024.100206.

14. Ramadhan, I. (2020). STRATEGI KEAMANAN CYBER SECURITY DI KAWASAN ASIA TENGGARA. , 3, 181-192. https://doi.org/10.33541/japs.v3i1.1081.