ISSN 2181-9130

Doi Journal 10.26739/2181-9130

ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ

10 ЖИЛД, 3 СОН

ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ

ТОМ 10, НОМЕР 3

JOURNAL OF LAW RESEARCH

VOLUME 10, ISSUE 3

ТОШКЕНТ-2025

ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ

ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ | JOURNAL OF LAW RESEARCH

№3 (2025) DOI http://dx.doi.org/10.26739/2181-9130-2025-3

Контакт редакций журналов. www.tadqiqot.uz
ООО Tadqiqot город Ташкент,
улица Амира Темура пр.1, дом-2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Тел: (+998-94) 404-0000

Editorial staff of the journals of www.tadqiqot.uz
Tadqiqot LLC the city of Tashkent,
Amir Temur Street pr.1, House 2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Phone: (+998-94) 404-0000

МУНДАРИЖА | СОДЕРЖАНИЕ | CONTENT

ISSN: 2181-9130
www.tadqiqot.uz
ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ
ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ | JOURNAL OF LAW RESEARCH

12.00.03-ГРАЖДАНСКОЕ ПРАВО. ПРЕДПРИНИМАТЕЛЬСКОЕ ПРАВО. СЕМЕЙНОЕ ПРАВО. МЕЖДУНАРОДНОЕ ЧАСТНОЕ ПРАВО

Baratov Mirodiljon Khomudzhonovich,
Department head of the Institute of State and Law
Academy of Sciences of the Republic of Uzbekistan,
Doctor of Law, Professor
E-mail: mirodiljonborotov@gmail.com
Khakimov Ravshan Tulkunovich,
Chief Researcher of the Institute of State and Law
Academy of Sciences of the Republic of Uzbekistan,
Doctor of Law, Associate Professor
E-mail: ngo_uzail@mail.ru
Akramxodjaev Bori Toxtaxodjaevich,
Senior Researcher of the Institute of State and Law
Academy of Sciences of the Republic of Uzbekistan,
Candidate of Law, Associate Professor
E-mail: 1370017a@gmail.com

ACCESSION OF THE REPUBLIC OF UZBEKISTAN TO THE WORLD TRADE ORGANIZATION AND CURRENT ISSUES OF CYBER PROTECTION OF THE AUTOMOTIVE INDUSTRY OF UZBEKISTAN

For citation: Baratov Mirodiljon Khomudzhonovich, Khakimov Ravshan Tulkunovich, Akramxodjaev Bori Toxtaxodjaevich. ACCESSION OF THE REPUBLIC OF UZBEKISTAN TO THE WORLD TRADE ORGANIZATION AND CURRENT ISSUES OF CYBER PROTECTION OF THE AUTOMOTIVE INDUSTRY OF UZBEKISTAN. Journal of Law Research. 2025, 10 vol., issue 3, pp. 19-25

http://dx.doi.org/10.5281/zenodo.15158589

ANNOTATION

The authors of the article consider the issues of accession of the Republic of Uzbekistan to the World Trade Organization from the position of ensuring the development of the automotive industry, including issues of ensuring cyber protection for such enterprises. The fact is that in international trade, cases of hacker attacks on individual companies specializing in the production of cars have worsened. In this regard, the authors propose to strengthen the cybersecurity of the automotive industry of Uzbekistan.

Keywords: “Uzavtosanoat”, cybersecurity, hacker attacks, WTO, Republic of Uzbekistan, Treves Group, Rosenbauer, Ferrari, Exco Technologies, AlbertZiegler GmbH, SAF - Holland, Rheinmatall, Hyundai Motor, Suzuki Motorcycle India, Laremo GmbH.

Баратов Миродилжон Хомуджонович,
Академия наук Республики Узбекистан, заведующий отделом
Института государства и права, доктор юридических наук, профессор
E-mail: mirodiljonborotov@gmail.com
Хакимов Равшан Тулкунович,
Академия наук Республики Узбекистан, ведущий научный сотрудник
Института государства и права, доктор юридических наук, доцент
E-mail: ngo_uzail@mail.ru
Акрамходжаев Бори Тохтаходжаевич,
Академия наук Республики Узбекистан, старший научный сотрудник
Института государства и права, кандидат юридических наук, доцент
E-mail: 1370017a@gmail.com

ПРИСОЕДИНЕНИЕ РЕСПУБЛИКИ УЗБЕКИСТАН ВО ВСЕМИРНУЮ ТОРГОВУЮ ОРГАНИЗАЦИЮ И АКТУАЛЬНЫЕ ВОПРОСЫ КИБЕРЗАЩИТЫ АВТОМОБИЛЬНОЙ ПРОМЫШЛЕННОСТИ УЗБЕКИСТАНА

АННОТАЦИЯ

Авторы статьи рассматривают вопросы присоединения Республики Узбекистан во Всемирную торговую организацию с позиции обеспечения развития автомобильной промышленности, включающей и вопросы обеспечения киберзащиты такого рода предприятий. Дело в том, что в международной торговле обострились случаи хакерских атак на отдельные компании, специализирующиеся на выпуске автомобилей. Авторы предлагают в этой связи усилить кибербезопасность автомобильной промышленности Узбекистана.

Ключевые слова: «Узавтосаноат», кибербезопасность, хакерские атаки, ВТО, Республика Узбекистан, Treves Group, Rosenbauer, Ferrari, Exco Technologies, AlbertZiegler GmbH, SAF-Holland, Rheinmatall, Hyundai Motor, Suzuki Motorcycle India, Laremo GmbH.

Baratov Mirodiljon Xomudjonovich,
O‘zbekiston Respublikasi Fanlar akademiyasi
Davlat va huquq instituti bo’lim boshligi
yuridik fanlar doktori, professor
E-mail: mirodiljonborotov@gmail.com
Hakimov Ravshan Tulkunovich,
O‘zbekiston Respublikasi Fanlar akademiyasi Davlat va huquq instituti
bosh ilmiy xodimi, yuridik fanlar doktori, dotsent
E-mail: ngo_uzail@mail.ru
Akramxodjayev Bori Toxtaxodjayevich,
O‘zbekiston Respublikasi Fanlar akademiyasi Davlat va huquq instituti
katta ilmiy xodimi, yuridik fanlar nomzodi, dotsent
E-mail: 1370017a@gmail.com

O‘ZBEKISTON RESPUBLIKASINING JAHON SAVDO TASHKILOTIGA QO‘SHILISHI VA O‘ZBEKISTON AVTOMOBIL SANOATINI KIBERXAVFSIZLIGINING DOLZARB MASALALARI

ANNOTATSIYA

Maqola mualliflari O‘zbekiston Respublikasining Jahon savdo tashkilotiga a’zo bo‘lishi masalalarini avtomobilsozlik sanoatining rivojlanishini ta’minlash nuqtai nazaridan, shu jumladan, bunday korxonalarning kiber himoyasini ta’minlash masalalarini ko‘rib chiqadilar. Gap shundaki, xalqaro savdoda avtomobillar ishlab chiqarishga ixtisoslashgan ayrim kompaniyalarga xakerlik hujumlari sodir etish holatlari ko‘paygan. Shu munosabat bilan mualliflar O‘zbekistonda avtomobil sanoatining kiberxavfsizligini kuchaytirishni taklif qilmoqdalar.

Kalit so‘zlar: “O‘zavtosanoat”, kiberxavfsizlik, xakerlik hujumlari, JST, O‘zbekiston Respublikasi, Treves Group, Rosenbauer, Ferrari, Exco Technologies, AlbertZiegler GmbH, SAF-Holland, Rheinmatall, Hyundai Motor, Suzuki Motorcycle India, Laremo GmbH.

In connection with the issues of accession of the Republic of Uzbekistan to the World Trade Organization, issues of docking with the WTO on the implementation of international trade standards in the country's economy are consistently discussed, in particular, the issue of developing the automotive industry of the Republic was discussed. On December 14, 2023, President Shavkat Mirziyoyev got acquainted with the presentation of proposals for the development of automotive and agricultural engineering.

As a result of the economic reforms being implemented in our country, these industries are being consistently modernized. Despite logistical challenges, car production has tripled in recent years, with total volume expected to reach 415,000 units by the end of this year. In order to eradicate the state monopoly and develop competition in the industry, 3 new private automakers and prestigious foreign brands were attracted. Today, 8 factories in the country produce dozens of types of cars, freight and passenger transport, agricultural and special equipment.

In addition, more than 2 thousand enterprises in the industry closely cooperate with each other, and 50% localization of components is ensured.

At the same time, there is still a high demand for cars in the market. Competition among automakers is intensifying both in the domestic and foreign markets. From now on, the Uzavtosanoat joint-stock company must make more efforts to expand the model range, improve quality, reduce production costs, and work in a competitive environment, it was noted at the meeting.

During the presentation, plans and challenges facing the industry were discussed.

In particular, by 2030 it is planned to increase the production of passenger cars in the country to 1 million units. The meeting identified measures that need to be completed within the framework of this task in 2024.

The head of our state emphasized the importance of accelerating the transformation of Uzavtosanoat and reducing costs.

As you know, today the world's leading automakers are switching to the production of electric vehicles. If domestic enterprises are slow to develop this industry, in the future they will face difficulties in occupying a worthy place in the market.

The first projects in this direction have already been started. It is planned that next year a car plants capable of producing 10 thousand electric vehicles per year will be launched.

The President pointed out the importance of special attention to the production of electric vehicles and ordered the production of components for them.

The country's agricultural machinery industry produced more than 3.5 thousand units of equipment this year. By 2030, it is planned to increase this volume to 16 thousand per year.

An agricultural engineering cluster was created in Chirchik. Its annual production capacity is 15 thousand tractors, trailers and other equipment. However, the system for selling them does not meet the requirements of the time.

In this regard, it was emphasized that it is necessary to expand incentives for the purchase of domestic equipment, increase the interest of clusters and farmers, create a portfolio of orders, and additional measures were identified. The task has been set to bring the localization level of domestic tractors to 35 percent, and suspended equipment and trailers to an average of 60 percent [1].

At the same time, globalization and the extremely rapid development of information and communication technologies around the world are causing massive cybersecurity breaches, including in the automotive industry. In the Republic of Uzbekistan, this problem has not yet come to the forefront of discussion, however, sooner or later, economic policy aimed at Uzbekistan’s accession to the WTO will be forced to pay attention to such an urgent and pressing problem.

Let's look at the facts:

Trèves Group was hit by ransomware

Manufacturing, Automotive | Ransomware, ransom demand

French car manufacturer Trèves Group experienced a major cyber-attack over the weekend of February 18 and 19, 2023. To limit the impact of the attack and protect its partners, Trèves Group immediately implemented isolation protocols", according to a company press release . The group worked closely with authorities and promised to take "all necessary measures on this issue". The company has mobilized to ensure continued operations and a return to normal operations as soon as possible. Trèves Group mentioned the Lockbit 3.0 ransomware group as the source of the attack in a press release, which in turn added the company to its list of victims. The company decided not to pay the ransom.

The Rosenbauer group was attacked by ransomware

Manufacturing, Automotive, Fire and Rescue Equipment | IT systems failure | Ransomware

The Rosenbauer Group, an Austrian manufacturer of fire fighting vehicles and firefighting equipment, was the target of a cyber-attack. According to a brief press release published on February 24, 2023, part of the IT infrastructure was taken offline as precautionary measures. The measures taken by the company affected all Rosenbauer locations. A task force was immediately created and external cybersecurity and forensics experts were brought in to safely and quickly restore the systems. According to the company, “neither customer data nor company data was stolen or encrypted.” The relevant authorities were involved in the investigation. A few days after the attack was officially confirmed, the LockBit 3.0 ransomware group included the company in its list of victims.

Ferrari hit by ransomware

Manufacturing, Automotive | Data leak, ransom demand, personal data leak | Ransomware

Italian car manufacturer Ferrari reported a cyber-incident involving ransomware. The attacker demanded that the company pay a ransom for customer data. The company notified its customers of a possible data breach. According to the company's statement, upon receiving the ransom demand, it immediately began an investigation with one of the world's leading cybersecurity companies and notified the relevant authorities. She added that it was company policy that Ferrari would not pay ransoms because such payments finance criminal activity. The company notified its customers and warned them about the possible data breach and the nature of the incident. The company said the ransomware incident had no impact on its operations.

Exco Technologies suffered a cyber-attack

Manufacturing, Automotive | IT systems failure

Canadian multinational foundry tool and auto parts company Exco Technologies announced on January 23, 2023 that three manufacturing facilities within its Casting Group are recovering from a cyber-incident. The company temporarily disabled some computer systems in order to investigate the incident with the involvement of independent experts. The company expected operating activity to largely recover over the next two weeks. The statement did not detail the type of attack, nor did it indicate whether personal or corporate data was stolen.

Ziegler suffered a cyber-attack

Manufacturing, Automotive, Fire Trucks | IT systems failure, delivery stoppage

The German fire truck manufacturer Albert Ziegler GmbH was the victim of a cyber-attack that was discovered on the morning of February 9, 2023. According to the news, all relevant systems were immediately shut down. As a result, all systems were taken offline in all locations, which limited the company's work and email availability. On February 20, 2023, the company released a statement that all systems had been restored, but the company was still available via email with delays. The inventory management system became available again only a few days later. This allowed the campaign to resume product deliveries in Gingen.

SAF-Holland suffered a cyber-attack

Manufacturing, Automotive | Failure of IT systems, stoppage of production: 7-14 days

German trailer and truck chassis manufacturer SAF-Holland [2]was the target of a cyberattack that was announced on March 27, 2023. As a result, the systems were disconnected from the Internet and turned off. The company estimates that the suspension of production at some of its facilities could

last for seven to fourteen days. However, management expected to be able to make up the production backlog over the next three months. The company estimated that it would take three months to restore lost production.

Rheinmetall suffered a cyber-attack

Manufacturing, Automotive | IT systems failure

Rheinmetall, a German automobile and weapons manufacturer headquartered in Düsseldorf , announced that it faced a cyber-attack that occurred on April 14, 2023. The attack affected Rheinmetall's business unit serving industrial customers, particularly in the automotive industry. According to a Rheinmetall representative in an email to Recorded Future News , the company's division that produces military vehicles, weapons and ammunition was unaffected and continues to operate. It is unclear who is behind the attack. It is known that the hacktivist group Killnet published a message on its Telegram channel in March, calling on its followers to launch DoS (denial-of-service) attacks on Rheinmetall.

VSOC — A specialized security center that monitors, detects and responds to cyber threats, especially those affecting vehicles. This is not a new invention. In essence, it is similar to a SOC, which performs the same functions in classic IT: continuous remote monitoring of a large number of parameters in order to automatically detect anomalies and trigger an alarm in the event of threats. Cybersecurity is thus ensured not by completely preventing hacker attacks (this is impossible in networked systems), but by systematically detecting threats at an early stage and taking timely countermeasures to minimize damage. To this end, IT security specialists in Düsseldorf monitor processes and protocols in the control center and respond to security incidents. Given the flood of constantly generated data, this work resembles searching for a needle in a haystack and would not be possible without artificial intelligence, machine learning and automated monitoring processes. With their help, SOC employees can filter out the most important events from the multitude of events that deviate from the normal course of business and focus on these real incidents[3].

The response time to security incidents therefore plays a central role in cyber-attacks. The faster a risk is identified, the faster action can be taken (“incident response”). SOCs and VSOCs differ significantly due to the technical infrastructure: In classic IT systems, the usual procedure for fixing security vulnerabilities is to install software updates, which can be implemented within a few minutes via the network or server. In the automotive sector, this process is much more complex and the response time is significantly longer. Although updates can be delivered to modern vehicles “over the air”, i.e. via the cloud, the manufacturer often does not have access to the software and hardware components of its suppliers, which it does not want to disclose for obvious reasons. In this case, vehicle manufacturers must work with the relevant supplier to find a solution, sometimes through multi-stage supply chains. And not all embedded systems can be accessed via a remote update, so callbacks are necessary. Depending on the length of the communication channels, fixing a security vulnerability can take several weeks. In extreme cases, manufacturers have to ask vehicle owners to temporarily stop using their vehicles or forcibly remove vehicles from service - a real nightmare for owners and manufacturers.

Data theft at Hyundai

Manufacturing, Automotive | Data leak, personal data leak

Car manufacturer Hyundai Motor[4] has notified car owners in France and Italy about unauthorized access to data . The company warned that hackers had illegally accessed the personal information of the company's customers. The leaked data contains phone numbers, email addresses, locations and vehicle chassis numbers (VINs). The alert confirms that while the attackers gained access to Hyundai's database, they did not gain access to customers' financial information or passport details. Hyundai said it had taken its systems offline in response to the attack until further protective measures could be taken. The company has also notified the French and Italian data protection authorities. Hyundai advises its customers to be alert to suspicious emails and unsolicited text messages as they may be an attempt at social engineering.

Suzuki Motorcycle India suffered a cyber-attack

Manufacturing, Automotive | Stopping production

Suzuki Motorcycle India, a subsidiary of Suzuki Motor Corporation, has been the victim of a cyber-attack. Effective May 10, 2023, the company suspended production at its Gurgaon plant, located in the northern Indian state of Haryana. A Suzuki Motorcycle India spokesperson stated that they are aware of the incident and have reported it immediately. At the time the attack was reported, no technical details were provided. The cyber-attack reportedly forced the company to postpone its annual supplier conference, which was scheduled to take place in May.

Laremo was attacked by ransomware

Steel structures | Denial of Service, Data Loss, Data Leak | Ransomware

The German company Laremo GmbH[5], a manufacturer of special equipment for trucks and construction equipment, was attacked using ransomware on February 5, 2023, the company announced this in a public statement on February 22, 2023. According to the statement, the server's storage systems were encrypted so that the data was lost. The attackers gained access to the customer database and financial records. The company contacted the relevant investigative authorities.

The LockBit group claimed responsibility for the attack and uploaded the company's data to their darknet website on February 19, 2023 [6].

Thus, to ensure an adequate level of protection for the automotive safety of new products, a unified methodological approach to the development of vehicle systems and their network interaction is described and applied in the industry. This procedure includes the following process steps:

Identify and assess safety risks

Determine appropriate risk mitigation measures

Ensure and verify the implementation of measures

Testing and approval of implementation

Engineering process [7]

The International Organization for Standardization (ISO) is an international association of standards organizations that develops international standards [8].

SAE International, formerly the Society of Automotive Engineers (SAE), is a non-profit engineering and scientific organization dedicated to advancing mobility technologies.

A similar approach has already proven itself in the field of functional safety through the industry standard ISO 26262 [9]. Similarly, VDA and its members have initiated the standardization of automotive safety engineering systems. In order to achieve a global effect, a joint working group of ISO and SAE standards organizations was created to develop a standard (ISO-SAE AWI 21434 Road vehicles – Cybersecurity engineering) [10]. This standard provides a framework for making automotive safety objectives an integral part of the overall development process of the automotive industry. The relevant aspects of product definition, design, implementation and testing using this standard are described. However, the standard does not prescribe any specific technology.

From an automotive industry perspective, this standard provides a consistent, application-specific, risk-based understanding of safety built into product design and throughout the supply chain.

Thus, the above examples require immediate measures to organize cyber protection of automobile enterprises of the Republic of Uzbekistan, which will subsequently benefit not only the international trade relations of Uzbekistan with the world, but will also benefit the people of Uzbekistan. This policy will cause structural changes in the security forces, in particular in the Ministry of Internal Affairs of the Republic of Uzbekistan, and in this regard it will be very useful to familiarize the police of Uzbekistan with the activities of the relevant cybersecurity specialists in Austria.

References/Иқтибослар/Сноски:

1. Proposals for the development of the automotive industry were considered//https://president.uz/ru/lists/view/6925-2023, December 14.

2. https://safholland.com/us/en/.

3. https://www.security-insider.de/cybersicherheit-automobilbranche-gefahren-loesungen-vsoc-a-6474b3554ea62c9392fffb6f27f5585b/.

4. https://www.hyundaimotorgroup.com/main/mainRecommend.
5. https://www.technikboerse.com/uk/haendler/laremo-gmbh-49162631.
6. First half of 2023 – a brief overview of the main industrial cybersecurity incidents//https://ics-cert.kaspersky.ru/publications/reports/2023/10/05/h1-2023-a-brief-overview-of- main-incidents-in-industrial-cybersecurity.
7. https://www.vda.de/de/themen/digitalisierung/daten/cybersicherheit.
8. Жаҳон савдо ташкилоти: кеча ва бугун / Монография / Б.Т.Акрамходжаев, Ш.А.Ахунов, М.Х.Баратов, О.Оқюлов, Ш.Н.Рўзиназаров, Р.Т.Хакимов. – Тошкент: Kamron press, 2024. 392. 67-б. (World Trade Organization: yesterday and today / Monograph / B.T.Akramkhodjaev, Sh.A.Akhunov, M.Kh.Baratov, O.Okyulov, Sh.N.Rozinazarov, R.T.Khakimov. - Tashkent: Kamron Press, 2024. 392. p. 67.)
9. https://www.iso.org/standard/43464.html.
10. https://www.iso.org/standard/70918.html.

ISSN 2181-9130

Doi Journal 10.26739/2181-9130

ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ

10 ЖИЛД, 3 СОН

ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ

ТОМ 10, НОМЕР 3

JOURNAL OF LAW RESEARCH

VOLUME 10, ISSUE 3

Editorial staff of the journals of www.tadqiqot.uz
Tadqiqot LLC The city of Tashkent,
Amir Temur Street pr.1, House 2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Phone: (+998-94) 404-0000

Контакт редакций журналов. www.tadqiqot.uz
ООО Tadqiqot город Ташкент,
улица Амира Темура пр.1, дом-2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Тел: (+998-94) 404-0000