https://doi.org/10.31489/2025L1/80-86 Received: 1 December 2024 | Accepted: 06 January 2025

UDC 349.8:004(560)

A. Shukan[1*], Ya. Erdogan[2], G.B. Karzhasova[3]

[1]*Karaganda Buketov University, Karaganda, Kazakhstan;*
[2]*Antalya Bilim University, Antalya, Turkey;*
[3] *Karaganda University of Kazakh Consumers' Cooperation, Karaganda, Kazakhstan*
(E-mail: alia_shukan@mail.ru, yavuzerdogan@hotmail.com, Gkb24@mail.ru)

[1]*ORCID ID: https://0009-0001-8725-0955, Scopus Author ID: 57210261515*
[2]*ORCID ID: https://0000-0003-4645-4326, Scopus Author ID: 16238520500*
[3]*ORCID ID: https://0000-0002-0252-3417, Scopus Author ID: 55892744600*

The Experience of the Republic of Turkey in Combating Cybercrime and Issues of Preventing Criminal Offenses in the Field of Information Technologies

Cybercrime is a relatively new type of crime. With the widespread use of the Internet and its integration into all areas of life, this type of crime and the methods of committing it are also evolving. Therefore, the main goal of this article is to explore the establishment of specialized police units and the development of new crime prevention policies in Türkiye to combat cybercrime. In this study, the policies developed by the General Directorate of Security of Türkiye to fight cybercrime are analyzed using the classical approach model within the framework of state policy processes. The institutional analysis method was applied in the research. The study examines the legal regulations issued by Türkiye in combating cybercrime, the technical units established, its personnel policy, and the factors that influenced the development of these policies. Additionally, a comparison is made with the policies in this field in Kazakhstan.The relevance of the topic lies in addressing the importance of measures aimed at protecting information constituting a state secret and legally protected personal data of citizens within Kazakhstan's cyberspace.

Keywords: Combating cybercrime, fraud, cyber police, cyberspace, state system, information terrorism.

Introduction

Considering the transboundary nature of security issues in the field of information technology, we conclude that it is necessary to improve international cooperation in this area in accordance with the principles of equal legal international information exchange.

The development of international legal norms regulating interstate relations in the field of improving cooperation between the law enforcement agencies of the Republic of Kazakhstan and foreign countries in the use of global information infrastructure, as well as in the prevention, detection, suppression, and elimination of the consequences of the use of information and telecommunication technologies for terrorist and other criminal purposes, requires the harmonization of national standards and certification systems in this field with international systems.

* Corresponding author's e-mail: alia_shukan@mail.ru

Methods and materials

In the study of foreign practices in combating criminal activities in the field of information technology, analytical and comparative legal methods were used. Specifically, the analytical method was applied in examining the legislation of the Republic of Turkey on information security, while the comparative legal method was used to study Turkey's experience in implementing legal regulations related to information cybersecurity measures. In addition, the scientific research of domestic and foreign scholars in this field was analyzed.

Discussion

In the direction of organizational-administrative and organizational-technical support, it is required to implement a set of measures to ensure the information security of critically important objects of informatization, to ensure a unified state technical policy in the field of information security, including the system of information protection. To solve this issue, it is necessary to create a unified state system for monitoring the information space, as well as to establish the information system and infrastructure of the operational center for ensuring information security. In addition, it is required to improve the unified information and communication network of state bodies, to create an operational center for ensuring information security to protect critically important infrastructure in the field of information technologies, to develop a unified electronic mail system for state bodies, to establish at least two geographically distributed centers for storing backup databases of state bodies, to develop a national identification system in the cyberspace of the Republic of Kazakhstan, to create cybersecurity hubs, and to improve the quality and reliability of systems ensuring the information security of the "electronic government", aimed at preventing unauthorized access, data loss, and distortion.

In the direction of human resources provision, it is required to improve the system of training personnel in the field of information security and the protection of state secrets, as well as to address the issues of staffing law enforcement agencies, including units dealing with countering information terrorism and information crimes. Enhancing the effectiveness of educational and training programs related to information security and the protection of state secrets is very important. Chief Scientific Researcher of the Academy of Law Enforcement Agencies, Lazzat Temirzhanova, stated: "Currently, employees investigating crimes in the field of information technology lack sufficient qualifications. In this case, in addition to having the appropriate legal knowledge, it is necessary to be proficient in IT technologies. For this reason, a large percentage of criminal cases in this area remain unsolved". In their article, Litvinenko M.V. and Chukova D.I. expressed the following opinion regarding human resources: "Combating cybercrime is a national-level issue. The effectiveness of investigating crimes in the field of computer information is directly related to the preparation of specialists in this field. We believe that training specialists to fight cybercrime will be more effective if the theoretical and methodological foundations for applying deep information and technical knowledge are introduced, and a model for training legal professionals to investigate computer crimes is developed" [1; 59]. We believe that the issue of training qualified specialists is very important for increasing the effectiveness of combating offenses in the field of information technology, and this issue should receive significant attention.

We believe that Kazakhstan should closely collaborate with countries that have extensive experience in combating this type of crime. For example, it is essential to hold regular seminars for exchanging experiences with specialists from countries that have ratified the European Security Convention. Additionally, planned specialized training courses should be organized to enhance qualifications.

The Republic of Turkey's National Security Committee has been conducting measures to combat cybercrime since 1991. However, it can be said that strict and active monitoring of these types of crimes began to be implemented starting from 1997.

Results

The history of the establishment of organizations combating crime in the field of information technology.

Although crimes in the field of information technology were defined in the Turkish Penal Code No. 765 in 1991, it is important to note that it was only six years later that the issue of combating cybercrime was included in the main agenda of the Security Committee. From 1997 to 2011, the National Security Committee established the "Department for Combating Crimes in the Field of Information Technology" under the In-

formation Processing Division. However, initially, this divisions was involved in administrative work, and the staff recruited for the organization had no experience in judicial and criminal procedural areas.

The National Security Committee's significant political step in combating cybercrime was realized on April 18, 1998, during an extraordinary meeting with the creation of the "Computer Crime and Information Security Organizations". On March 1, 1999, a working group on information crimes was organized. The objectives of the organization were also defined: investigating violations in the field of information technology, identifying types of offenses, and establishing the necessary regulations in the relevant authorities' legal acts. As a result of these measures, many international sources were studied, and a system for assessing the threat level of cybercriminals was introduced. Additionally, the department's staff was tasked with continuously conducting exchange programs. In 2006, the department's name was changed to the "Department for Combating Crimes in Information Technology and Systems" [2; 98]. Currently, this department is named "Crimes in Information and High Technology". The Cybercrime Division worked under the department responsible for combating smuggling and organized cybercrime. In addition, provincial units were provided with technical support, and later, this technical department was tasked with investigating electronic evidence, as well as coordinating the "Directorate of Information Security" [2; 98]. In 2006, the department opened its centers in Istanbul, Sakarya, Bursa, Izmir, Antalya, Adana, Van, Diyarbakir, Malatya, Erzurum, Samsun, Ankara, and Kayseri. It is worth noting that the Cybercrime Center in Istanbul stood out for its high level of activity and effectiveness. Since other provincial security units did not have a separate police unit to fight cybercrime, and many companies and institutions working in this field had their headquarters or branches in Istanbul, with the approval of the Ministry of Internal Affairs, the "Counteracting Crime in the Information Space" Directorate was established in Istanbul on April 25, 2007 [2; 99].

In 2011, in order to centralize and consolidate the various departments of departmental agencies and provincial organization branches, prevent the duplication of investments, and ensure the effectiveness of the fight against cybercrime, a decision was made by the Cabinet of Ministers, under Resolution No. 2011/202515, to create a centralized department named "Fight Against Information Crimes" under the Security Department within the framework of an extraordinary meeting of the Cabinet of Ministers. Other goals of this policy included: improving and diversifying the fight against information crimes and crimes committed through communication tools, the need for new structures in combating this crime, saving resources, reducing duplicated services between departments, uniting specialized personnel from different departments under a single organization, and striving to prevent and reduce criminal offenses in the field of information technologies by continuously enhancing their knowledge and qualification levels. Additionally, it aimed to improve the effectiveness of crime investigations. This organization was renamed the Cybercrime Department on February 28, 2013, upon the proposal of the Ministry of Internal Affairs (SSMDB — Siber suçlarla mücadele daire başkanlığı, meaning Cybercrime Combat Division) [2, 99].

The main task of the Cybercrime Department is to provide judicial and informational services and combat crimes related to online fraud, fraud in payment systems, obscene publications, illegal betting, gambling, and cyberterrorism. Therefore, this organization can be considered as an efficient department, staffed with highly qualified specialists capable of providing technical support to other departments and fighting cybercrime. In collaboration with the Cybercrime Department, employees from the Anti-Drug, Financial Crime, Human Trafficking, and Organized Crime Units, as well as the Terrorism and Public Security Departments, are involved in combating theft and fraud. The department also deals with cybercrimes related to copyright infringement, in accordance with Law No. 5846, to protect authorship and creative works. These units are also responsible for investigating cybercrimes within their respective service areas.

The powers of the Turkish Cybersecurity Department can be found on the website www.bugun.com.tr. The list of their activities is as follows:

1. Using informants and undercover investigators during the investigation of criminals to infiltrate criminal organizations and gather evidence.

2. Implementing the use of evidence, expert opinions, services, and statements from individuals or legal entities for the prevention of crimes.

3. Department employees are authorized to listen to any messages and calls, monitor suspects or suspected individuals, and install technical equipment in public places and workplaces of suspects.

4. They have the right to utilize the advantages of emergency services for the benefit of the state and society, to preserve political, social, and cultural security, and to obtain necessary data, audio, and video recordings.

5. Cyberpolice assist in accessing information systems in different geographical locations during important investigations.

The Turkish Cybercrime Department not only performs the function of monitoring information technologies but also operates as a police department carrying out operational police duties. Under the Cybercrime Department, 81 cybercrime units were established across provinces to ensure the security of information technologies. The following departments work within these units: The Forensic Bureau, the Crime Investigation and Search Bureau, the Court Transaction Monitoring Bureau, the Virtual Patrol Monitoring Bureau, and the Operational Support Monitoring Bureau. We can see that the functions of these departments are mainly focused on combating cybercrime. Additionally, the Virtual Patrol Office's activities are also part of this department's duties. These departments emphasize the need to actively use social media platforms for disseminating messages aimed at preventing cybercrime and connecting with the online community. For example, the Cybersecurity Department in the Cyber Bureau, with 2,700 employees, collects information about crimes committed in cyberspace by monitoring the social media of 45 million people in Turkey.

It should be noted that the Ministry of Internal Affairs has established an effective centralized apparatus in Turkey's major cities to combat cybercrime, as most cybercriminal offenses occur in large cities where the internet is widely used. The European Union's Secretariat is contributing to strengthening the potential of law enforcement and judicial authorities by implementing the "Strengthening Cooperation in the Fight Against Information Crimes" project. This project aims to promote cooperation in areas such as combating cybercrime and facilitating information exchange between national and international governments. This cooperation has been ongoing since 2009. The EU Secretariat's efforts in this area are being carried out not only with the Ministry of Internal Affairs but also in collaboration with the Gendarmerie General Command and organizations related to telecommunication services. The project, which began in 2013, is scheduled to conclude in 2019, with plans to hold 138 training sessions and seminars both domestically and internationally. The cost of the project is 4,400,000 euros [3].

The recruitment of civilian employees into the police forces is one of the long-established methods in the Republic of Turkey. There are several reasons for this practice. First and foremost, it is related to financial costs and reward levels, as the salaries of civil servants are calculated to be 20 % lower than those of police officers. Additionally, employees in this department are required to be in civilian clothing when conducting operations, searching for criminals, and making arrests.

Employees in this department must possess the skills and capabilities to investigate crimes committed using electronic technologies, as well as any crimes related to electronic evidence. Furthermore, security department personnel combating cybercrime must continuously improve their professional skills, such as learning foreign languages. Knowledge of foreign languages is necessary to work effectively with foreign partners. Additionally, employees must be proficient in using information technologies for cybercrime detection. Specifically, they need to be able to identify methods for finding cyber-criminal evidence required for expert analysis. Since evidence in cybercrimes resides in information technologies, expert specialists are needed to gather and report such evidence. For this reason, law enforcement agencies that collect evidence must develop their technical and administrative capabilities [4].

Turkey, therefore, still requires additional expert specialists in the judicial-investigation sector dealing with cybercrimes. A global issue is the lack of potential, capabilities, and resources in police departments for combating cybercrime. It should also be noted that only cases reported by the victims are taken into consideration, and investigative work is conducted based on those reports. In other words, the judicial-information services aimed at obtaining electronic traces and evidence used in criminal investigations and cybercrime cases, as well as collaborating with the necessary sector organizations to prevent crimes, enhance the effectiveness of the fight against cybercrime. The strategy of continuous education for personnel fighting cybercrime should be a strategic priority. The principles of this work are as follows: conducting forensic examinations for criminal cases, providing assistance to other institutions, and introducing a continuous training strategy for local law enforcement employees to improve the qualifications of specialists in the field of cybercrime investigations for network security; organizing continuous training on electronic evidence collection not only for specialized units but also for all law enforcement agencies; increasing the number of employees capable of conducting high-level research and digital analytical reviews due to the constantly evolving nature of cybercrimes and the rapid growth of crime in this field. Since training new specialists to fight cybercrime is expensive, measures to improve the qualifications of existing employees are implemented regularly.

Within the framework of KOMDB (Committee for Combating Organized and International Crime), the following seminars and trainings were conducted: “Methods and Forensics of Recovering Computer and Internet Criminal Evidence”, “Seminar on Crime Analysis”, “Seminar on Finding Cybercrime Traces”, “Conducting Research on Electronic Evidence”, “Seminar on Crimes on the Internet”, “Confidential Course on Electronic and Computer Crimes”, “Course on Recovering Criminal Evidence,» and «Methodology of Investigating and Investigating Crimes in Information Technologies”.

After the establishment of SSMDB (Committee for Combating Cybercrime), the training of personnel in this field was transferred to the authority of the mentioned committee.

Since 2014, every year, between 909 and 1500 trainees, in line with the basic and advanced training needs of employees, have been learning to effectively and successfully work with various types of cybercrime and criminal organizations related to information technology. The Security Committee has been conducting training for cybercrime units at foreign police organizations. Between 2014 and 2016, about 100 employees, within the framework of an international relations project in Kosovo, Georgia, Kazakhstan, Bosnia, and Herzegovina, participated in training seminars on methods of combating cybercrimes over six semesters [5].

Due to the international nature of cybercrime, cooperation and information exchange with other countries are crucial. In this regard, Turkish police have made bilateral agreements with the security organizations of 39 countries, and they plan to hold training sessions related to conducting international operations against cybercrime until 2019.

Moreover, Turkey had announced in 2021 its intention to train nearly 21,000 professionals who will monitor offenders in the field of information technology. Therefore, from the information provided above, we can observe that Turkey is actively pursuing its cybersecurity policy both in the military and civilian security sectors. In the current era of information technology, it is well-known that conducting an active security policy in this area is a key guarantee of internal stability within countries.

Above, the analysis reveals that in Kazakhstan’s information technology network, there is poor coordination of measures for protecting legally protected data and information, as well as systemic fragmentation in ensuring the integrity and confidentiality of information. This lack of a unified system negatively impacts the protection of legally protected data sources and critical information.

The issue of a shortage of qualified personnel in the information and communication sector, including in information security, remains a critical issue. The preparation of specialists and the enhancement of their qualifications in this field are highly relevant issues.

Additionally, the relatively low level of legal and information culture, as well as the skills needed for the safe use of cyberspace in Kazakh society, poses a significant risk. The low level of citizens’ literacy regarding cybersecurity is also a contributing factor to the issue. Moreover, cybersecurity measures should not only be implemented by the government but also by individuals. For instance, citizens should ensure they keep their personal information, details about their relatives, home addresses, places of work or study, and bank card numbers confidential, and avoid disclosing them to others. By adhering to this simple algorithm, individuals can contribute to preventing cybercrimes.

Conclusions

Considering the information security policies implemented in Turkey regarding the protection and preservation of information technologies, the following conclusions can be made:

1. The legal provision of the information sector in our country is significantly behind the needs of time. Legal mechanisms regulating information-legal relations arising during the search, acquisition, and consumption of various types of information, information resources, information products, and information services are developed insufficiently.

2. The current state of ensuring action against cybercrimes is characterized by the insufficient coordination of the legal mechanisms in use, fragmentation of efforts to develop and improve them, lack of effectiveness, contradictions in legal norms, and underdevelopment of legal statistics.

3. The problems mentioned above clearly indicate that they pose a significant threat to the country’s information security in the context of legal provision in the information sector.

4. In Kazakhstan, establishing a network of centralized and streamlined institutions, along with creating a central monitoring body dedicated to ensuring cybersecurity, is highly relevant and would yield effective results.

References

1 Чукова Д.И. Модель формирования компетенций специалиста в сфере расследования компьютерных преступлений / Д.И. Чукова, Д.А. Медведев, М.В. Литвиненко // Вопросы кибербезопасности. Серия Право. — 2019. — № 3(31). — С. 57–62.

2 Shukan A. Issues of Information Technology Crime Control in The Republic Of Turkey / A. Shukan, A. Abdizhami, G. Ospanova, D. Abdakimova // Digital Investigation. — 2019. — Vol. 30. — P. 94–100.

3 Taşçı U. Türkiye'de polisin siber suçlarla mücadele politikasi: 1997–2014 [Electronic resource] / U. Taşçı, A. Can // Fırat Üniversitesi Sosyal Bilimler Dergisi. — 2015. — Vol. 25. — № . 2. — P. 229–248. — Access mode: https://dergipark.org.tr/tr/download/article-file/157433

4 «Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы» Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы. — [Электрондық ресурс]. — Қолжетімділігі: https://adilet.zan.kz/kaz/docs/P1700000407 (Қарау уақыты: 11.12.2024 ж.).

5 «Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің компьютерлік ақпарат саласындағы қылмысқа қарсы күрестегі ынтымақтастығы туралы келісімді бекіту туралы» Қазақстан Республикасы Президентінің 2002 жылғы 25 маусымдағы № 897 Жарлығы. — [Электрондық ресурс]. — Қолжетімділігі: http://adilet.zan.kz/kaz/docs/U020000897_ (Қарау уақыты: 18.11.2024 ж.).

А. Шукан, Я. Ердоган, Г.Б. Каржасова

Түркия Республикасының киберқылмыспен күресу тәжірибиесі және ақпараттық технологиялар саласындағы қылмыстық құқық бұзушылықтардан алдын алу мәселелері

Киберқылмыс — қылмыстың салыстырмалы түрде жаңа түрі. Әсіресе, ғаламторды кеңінен қолдану және оның өмірдің әр саласына енуіне байланысты қылмыстың бұл түрі мен оны жасау жолдары да өзгеруде. Мақаланың негізгі мақсаты — мамандандырылған полиция бөлімшелерін құруды және киберқылмыспен күресу үшін Түркиядағы қылмыстың алдын алудың жаңа саясатын әзірлеуді зерттеу. Бұл зерттеуде Түркияның Бас қауіпсіздік басқармасы киберқылмыспен күресу үшін әзірлеген саясат мемлекеттік саясат процестері шеңберінде классикалық тәсіл моделін қолдану арқылы талданған. Зерттеуде институционалдық талдау әдісі қолданылды. Сондай-ақ Түркияның киберқылмыспен күрес саласындағы құқықтық нормалары, құрылған техникалық бөлімшелер, кадрлық саясаты, сондай-ақ осы саясаттың дамуына әсер еткен факторлар да қарастырылған. Қазақстандағы осы саладағы саясатпен қосымша салыстыру жүргізілді. Тақырыптың өзектілігі мынада: мемлекеттік құпияны құрайтын ақпаратты және Қазақстанның киберкеңістігінде азаматтардың заңмен қорғалатын дербес деректерін қорғауға бағытталған шаралардың маңыздылығын зерделеу.

Кілт сөздер: киберқылмыспен күрес, алаяқтық, киберполиция, кибер кеңістік, мемлекеттік жүйе, ақпараттық терроризм.

А. Шукан, Я. Ердоган, Г.Б. Каржасова

Опыт Турецкой Республики в борьбе с киберпреступностью и вопросы профилактики уголовных правонарушений в сфере информационных технологий

Киберпреступность — относительно новый вид правонарушений. С широким распространением интернета и его интеграцией во все сферы жизни эволюционирует как этот вид преступлений, так и способы его совершения. Поэтому основная цель этой статьи — изучить создание специализированных полицейских подразделений и разработку новой политики предотвращения преступности в Турции для борьбы с киберпреступностью. В данной статье политика, разработанная Генеральным управлением безопасности Турции для борьбы с киберпреступностью, анализируется с помощью модели классического подхода в рамках процессов государственной политики. В исследовании был применен метод институционального анализа, рассматриваются правовые нормы, изданные Турцией в области борьбы с киберпреступностью, созданные технические подразделения, кадровая политика, а также факторы, повлиявшие на ее разработку. Дополнительно проводится сравнение этой области с политикой Казахстана. Актуальность темы заключается в рассмотрении важности мер, направленных на защиту информации, составляющей государственную тайну, а также охраняемых законом персональных данных граждан в киберпространстве Казахстана.

Ключевые слова: борьба с киберпреступностью, мошенничество, киберполиция, киберпространство, государственная система, информационный терроризм.

References

1 Chukova, D.I., Medvedev, D.A., & Litvinenko, M.V. (2019). Model formirovaniia kompetentsii spetsialista v sfere rassledovaniia kompiuternykh prestuplenii [Model of Competency Formation for Specialists in the Field of Investigating Computer Crimes]. *Voprosy kiberbezopasnosti. Seriia Pravo — Issues of Cybersecurity. Law Series,* 3(31), 57–62 [in Russian].

2 Shukan, A., Abdizhami, A., Ospanova, G., & Abdakimova, D. (2019). Issues of Information Technology Crime Control in The Republic of Turkey. *Digital Investigation, 30*, 94–100.

3 Ufuk, Taşci, & Ali, Can. (2015). Türkiye'de polisin siber suçlarla mücadele politikasi: 1997–2014. *Fırat Üniversitesi Sosyal Bilimler Dergisi, 25*, 2, 229–248. Retrieved from https://dergipark.org.tr/tr/download/article-file/157433

4 Kiberqauipsizdik tuzhyrymdamasyn («Qazaqstannyn kiverqalqany») bekitu turaly» Qazaqstan Respublikasy Ukimetinin 2017 zhylgy 30 mausymdagy No 407 qaulysy [Decree on the Approval of the Concept of Cybersecurity ("Kazakhstan's Cyber Shield")]. *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/kaz/docs/P1700000407 [in Kazakh].

5 «Tauelsiz Memleketter Dostastygyna qatysushy memleketterdin kompiuterlik aqparat salasyndagy qylmysqa qarsy kurestegi yntymaqtastygy turaly kelisimdi bekitu turaly» Qazaqstan Respublikasy Prezidentinin 2002 zhylgy 25 mausymdagy No 897 Zharlygy [The Decree No. 897 of the President of the Republic of Kazakhstan on the Ratification of the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Computer Crimes in the Field of Computer Information, dated June 25, 2002]. (2002, 25 June). *adilet.zan.kz* Retrieved from http://adilet.zan.kz/kaz/docs/U020000897_ [in Kazakh].

Information about the authors

Shukan Aliya — PhD, Karaganda Buketov University, Karaganda, Kazakhstan, e-mail: alia_shukan@mail.ru;

Erdogan Yavuz — PhD, Antalya Bilim University, Antalya, Turkey, e-mail: yavuzerdogan@hotmail.com;

Karzhasova Guldana Batyrbaevna — PhD, Karaganda University of Kazakh Consumers' Cooperation, Karaganda, Kazakhstan, e-mail: Gkb24@mail.ru.