AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Technology and Applied Sciences
ISSN (E): 2832-1766 Volume 46, March - 2026

FOREIGN EXPERIENCE IN PREVENTING CRIMES COMMITTED IN INFORMATION TECHNOLOGIES

Djamatov Mustafa Khatamovich
Senior Lecturer, Department of Digital Technologies and Information Security,
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Mamanazarov Dilshod Yashin o‘g‘li
Cadet, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

ABSTRACT

This article analyzes the experience of Germany, Israel, South Korea, and other countries in preventing crimes committed in the field of information technologies. The institutional and regulatory-legal foundations of combating cybercrime in countries with highly developed digital infrastructure, as well as the activities of specialized cybersecurity centers, are described. In addition, the effectiveness of mechanisms such as early detection of cyberattacks, prevention of unauthorized access to computer systems, ensuring the security of personal data, and strengthening cooperation between the public and private sectors is analyzed. It is emphasized that the foreign approaches to modern technology-based monitoring systems, digital literacy programs, and international cooperation are of significant importance for adaptation to Uzbekistan’s practice. At the end of the article, proposals and recommendations are presented based on the experience of South Korea and Singapore in preventing cybercrime.

KEYWORDS

Cyber fraud, social networks, cybersecurity policy, prevention of cyberattacks, digital security, international cooperation, information technology crimes, foreign experience.

Introduction

Today, preventing crimes committed in information technologies remains an urgent issue. In this area, the experience of several states—particularly South Korea, Israel, Germany, and other countries—serves as an international example in preventing such crimes. At present, cybercrimes—ransomware, phishing, data theft, and DDoS attacks—cause more than USD 14.5 trillion in annual losses to the global economy, and this figure is forecast to increase further by 2027. At the international level, the Budapest Convention (Convention on Cybercrime) serves as the foundational instrument for combating cybercrime. In the United States and European countries, penalties for types of cybercrime (phishing, hacking, data theft) are continuously updated, and law enforcement agencies are granted broad powers to collect digital evidence.

Methodology

In Israel and Türkiye, there is strong integration between cybersecurity standards and state security services. The state has established platforms for rapid information exchange on cyberattacks among state banks and IT companies. It has developed strict legal and technical systems to combat cybercrime. Below are the main measures being implemented by these states by 2026:

Israel's "Cyber Shield" strategy: Israel has one of the strongest cyber defense systems in the world. Its approach is based on the following:

– National Cyber Directorate (INCD):

Coordinates all cyber defense nationwide. Through the short number "119", citizens and companies can report cyberattacks 24/7.

The national cyber defense law for 2026 establishes mandatory security standards for critical infrastructure (energy, water, healthcare). For violations, a fine of up to 300,000 NIS or imprisonment of up to 2 years is предусмотрено (envisaged/provided).

Regarding cyber insurance, the private sector actively uses insurance mechanisms against cyber threats, which compels companies to continuously update their security.

Turkey considers combating cybercrime an integral part of national security. According to the new cybersecurity legislation for 2026: Turkey has strengthened criminal liability for cybercrimes. Strict requirements were introduced regarding data encryption and processing.

USOM (Cyber Incident Response Center) operates at the national level to detect cyberattacks and respond rapidly.

Turkey is making major investments in developing domestic antivirus and firewall systems to reduce dependence on foreign software.

Turkey is making major investments in developing domestic antivirus and firewall systems to reduce dependence on foreign software.

In the United Kingdom, the National Cyber Security Centre (NCSC) develops free protective tools and recommendations both for private businesses and for the general public.

In Estonia, as a model "digital state," children are taught cybersecurity basics and rules of online behavior starting from kindergarten and school age.

Discussion and Results

Germany has one of the most advanced systems in the world for preventing and combating crimes in the field of information technology (IT). This experience is based on an institutional structure, strategic cooperation, and strict legislation.

1. Institutional system and specialized agencies

In Germany, combating cybercrime is coordinated by agencies at several levels:

BKA (Bundeskriminalamt) – the Federal Criminal Police Office is the central body for investigating cybercrimes. It includes a "Cybercrime" (CC) unit specializing in complex crimes directed against the Internet and IT systems;

BSI (Bundesamt für Sicherheit in der Informationstechnik) – the Federal Office for Information Security. It develops IT security standards for the public and private sectors and analyzes cyberattacks;

NCAZ (Nationales Cyber-Abwehrzentrum) – the National Cyber Defense Center, which serves as a platform for information exchange and rapid response to cyberattacks among intelligence, police, and IT security agencies.

2. Strategic and legal foundations

According to the Cybersecurity Strategy, Germany's cybersecurity strategy (Cyber-Sicherheitsstrategie) identifies the protection of critical infrastructure (energy, transport, communications) as a priority task;

According to legislation, the German Criminal Code contains specific provisions for cybercrimes (e.g., Section 202a—unlawful acquisition of data; Section 303b—computer sabotage). Even preparing to commit a crime (creating malicious software) may entail criminal liability;

According to the Budapest Convention, Germany has harmonized international law in line with the Budapest Convention on Cybercrime.

3. Prevention methods (preventive measures)

According to public–private cooperation – the police work closely with the private sector and IT companies. Special portals have been established to exchange information about cyberattacks;

Regarding public training, continuous cyber hygiene training programs and warning systems (e.g., BSI for Citizens) have been introduced for citizens and small businesses. Continuous monitoring is conducted. Each year, the Federal Police publishes the "National Situation Report on Cybercrime" (Bundeslagebild Cybercrime), providing analytical information on emerging threats and offender methods.

From Germany's experience, it is possible to use elements such as establishing a centralized analytical unit to counter cybercrime or introducing mandatory standards for protecting critical infrastructure.

In the European Union, "Cybersecurity Month" is held every October to increase public knowledge on protection from phishing and fraud.

Conclusion

The conducted analyses indicate that preventing crimes committed in the field of information technologies has become an integral component of global security today. The experience of leading foreign countries in combating cybercrime is based on a comprehensive, institutional, and systemic approach.

In particular, Germany's experience demonstrates a centralized management system for combating cybercrimes through specialized federal agencies and strict regulatory-legal mechanisms. In Israel's practice, the activities of the National Cyber Directorate, mandatory security standards for critical infrastructure, and a rapid information exchange system ensure high effectiveness. The experience of South Korea and Singapore shows that preventive mechanisms can be strengthened through digital monitoring, public–private sector cooperation, and increasing the population's digital literacy.

References

1. European Union. EU Cybersecurity Strategy for the Digital Decade. Brussels, 2020.
2. Рустам Хабибуллаевич Махамадов, & Мустафа Хатамович Джаматов (2022). КИБЕРЖИНОЯТЧИЛИК ВА КИБЕРТЕРРОРИЗМ ТАҲДИДЛАРИГА ҚАРШИ КУРАШ. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), 2 (5), 103-108.
3. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime. Vienna, 2013.
4. OECD. Digital Security Risk Management Recommendation. Paris, 2015.
5. Makhamadov Rustam Khabibullayevich, & Djamatov Mustafa Khatamovich. (2025). Modern intellectual systems: status, functions, technologies and development tendencies. American Journal of Applied Science and Technology, 5(02), 52–55. https://doi.org/10.37547/ajast/Volume05Issue02-13
6. European Union Agency for Law Enforcement Cooperation (Europol). Internet Organised Crime Threat Assessment (IOCTA). The Hague, yillik hisobot.
7. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF 2.0). Gaithersburg, 2024.
8. United Nations General Assembly. Resolution on Countering the Use of ICTs for Criminal Purposes. New York, 2022.
9. Cyber Security Agency of Singapore (CSA). Singapore Cybersecurity Strategy 2021.
10. Rustam Maxamadov, & Mustafa Djamatov. (2025). Harbiy ta’lim muassasalarida mashg‘ulotlarni tashkil etishda intellektual o‘qitish tizimlarining roli. «Muhandislik Va Iqtisodiyot» Jurnali, 3(9), 6–12. https://doi.org/10.5281/zenodo.17117077