CYBERCRIME: NEW VECTORS OF DEVELOPMENT AND WAYS TO FIGHT THEM

Simonov Sergey Gennadievich, Tyumen Industrial University
Khamatkhanova Makka Alaudinovna, Tyumen Industrial University
Lysenko Igor Vyacheslavovich, Tyumen Industrial University

ABSTRACT

The purpose of the article is to identify and analyze modern vectors of development, localization and prevention of cybercrime. The statistics of cybercrime in our country and abroad in recent years have been studied. The sectoral landscape of cybercrimes in the Russian Federation for 2023 is presented. Attention is focused on phishing by the method of distribution, which today poses the greatest danger to Russian companies. The main resources forged by hackers during phishing attacks have been identified. Spoofing as a new vector of cybercrime development, its types and negative consequences for business are investigated. The problems of cybersecurity of "second-tier" business structures are touched upon, most of which are financially and organizationally not ready to purchase information security services and have low demand for vulnerability search services in software, web applications and corporate IT infrastructure. The stages of achieving minimum standards for combating cybercrime are proposed in the form of stages of implementing simple organizational and methodological recommendations for the prevention of cybercrime and minimizing their consequences for small and medium-sized businesses.

Keywords: cybercrime, phishing, spoofing, hacker attack, information security, cyber threats and vulnerabilities, second-tier business.

INTRODUCTION

In recent years, the rapid progress of cybersecurity has been constantly accompanied by new challenges due to the emergence and spread of innovative technologies, services, applications, and devices. The development of the Internet of Things (IoT), artificial intelligence (AI), mobile gadgets, cloud storage, messengers, social networks, electronic and cryptocurrency, blockchain, and machine learning (ML) occurs against the backdrop of ongoing hacker attacks and cybercrimes. For example, IoT devices are infected with malware that is used to create botnets, conduct DDoS attacks, or spy (24,14). Cloud services become compromised if hackers gain access to credentials, keys, or tokens (7). Mobile devices are subject to phishing, theft, loss, and hacking. Social networks are used by fraudsters to spread disinformation, manipulation, cyberbullying, or identity theft. Cryptocurrencies and blockchain are becoming targets for attacks through fake transactions, double spending, wallet hacking or mining. Using artificial intelligence (AI) and machine learning (ML), criminals create fake images, videos, audio or texts to mislead, deceive or blackmail corporate users (32).

At the same time, we note that the above-mentioned innovative technologies, services, applications and devices, although they are promising and influential trends in the field of

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

combating cybercrime, are capable of both increasing and decreasing the level of security of information and information systems of a business structure.

Today, such a popular messenger as Telegram significantly lowers the threshold for entry into the world of cybercrime. Condescending moderation conditions and a high level of anonymity have turned it, according to the figurative expression of Guardio Labs experts, into a "hotbed of modern phishing operations" (31). Even novice cyber fraudsters have the opportunity to gain free access to ready-made tools for carrying out hacker attacks or hire a personal hacker.

Telegram is now used to distribute malware and phishing kits, open public channels where hackers advertise their services and provide advice, and create special chatbots that can fully automate the cyberattack process for a modest fee. Hence, as information security researchers note, anyone can launch a cybercriminal campaign and make money from it.

Cybersecurity experts are concerned about this development vector, as it generates an increase in the number of hacker attacks, a sense of impunity among attackers, and puts business structures of various formats, their personnel, and ordinary citizens at risk. One cannot discount the fact that interaction with Telegram is difficult and, in practice, does not occur due to the location of the company's server equipment and the legal entity itself outside the Russian Federation (15).

RESEARCH METHODS

In this article, methods such as secondary data analysis, expert assessment, and questionnaires were used to collect the empirical material underlying the study of the problem of combating cybercrime.

The first of these methods is to initially study in detail the materials on the topic under study by scientists from both domestic and foreign countries. The next stage involves analysis, verification of the data obtained, and interpretation of the result obtained. This method also makes it possible to lay the foundations for building a typical internal cybersecurity monitoring center (SOC - Security Operation Center), as a structural unit of a medium or small-sized company, which is responsible for the prompt study of the IT environment and response to cyber incidents.

The study was conducted using the expert assessment method among two groups of experts: middle and senior managers of various economic entities who took part in the federal program “Labor Productivity and Employment Support,” for the implementation of which the Tyumen Region was chosen as a pilot territory; representatives of various non-profit territorial bodies and structures that do not directly carry out commercial activities. Including representatives of government bodies, scientific and public organizations, and others.

By using this method, it was possible to obtain an idea of the industry landscape of the request of economic entities in the studied region for services to search for vulnerabilities in software, web applications and IT infrastructure of companies. Finally, a research method such as a questionnaire allowed us to identify changes in the attitude of Russian businesses to the problem of cybersecurity, as well as to find out which main corporate resources hackers forge when carrying out their attacks.

RESULTS AND DISCUSSION

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

International statistics show that cybercrime in many countries continues to gain momentum, changing its landscape and quality. This also applies to our country, which currently ranks eighth in the world ranking with 5.3% of the total number of cyberattacks in the world. The top three in this list are as follows: the USA (16.2%), India (12.8%) and China (10.4%) (26).

It also became clear that today Russian business has changed its attitude towards cybersecurity. This was confirmed by a survey of representatives of 100 companies from various sectors of the domestic economy conducted in 2023 by K2Tech (Figure 1).

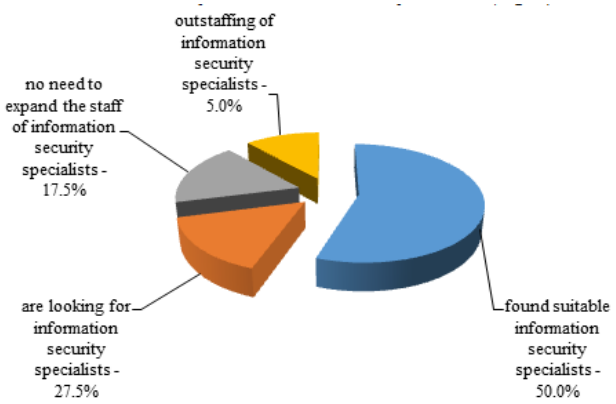

FIGURE 1
RESULTS OF RESPONSES TO THE QUESTION: "WHAT CHANGES IN THE STAFFING OF INFORMATION SECURITY SPECIALISTS ARE YOU PLANNING IN LIGHT OF INCREASING CYBER THREATS?"

From Fig. 1 it is clear that half of the representatives of the surveyed business structures have already found suitable employees to combat cybercrime (50.0%), more than a quarter of them (27.5%) are in the search stage, and the remaining 5% use outstaffing, borrowing information security specialists from other companies.

There have also been significant shifts in the sectoral landscape of cybercrimes in Russia (Table 1).

Table 1
SECTORAL LANDSCAPE OF CYBERCRIME IN RUSSIA IN 2023 (28).

No.	Names of the most attractive vectors of cyber attacks on Russian business structures	Distribution of the most attractive vectors of cyber-attacks on Russian business structures in descending order of share (in %)
1	Public sector	37
2	Finance sector	23
3	Telecommunications sector	18
4	Energy sector	7
5	Oil sector	5
6	Other sectors	10

It should be noted that the increase in the total number of cyberattacks on domestic business structures for the period 2022-2023 amounted to 28% (17). At the same time, phishing remains the initial vector of hacker attacks, which has received new vectors of its development in the form of the distribution of ransomware, infostealers and other modifications of malware aimed at

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

stealing valuable information and gaining access to the IT infrastructure of companies. The most vulnerable link for them remains small and medium-sized business entities that are unable to protect themselves from cybercriminals who quickly change their schemes. For example, in 2023, one of the most popular hacker schemes was email distribution, which turned out to be quite effective and less expensive for them. In the first quarter alone, over 800 ransomware attacks with infection through malicious mailings were recorded. By the end of Q2 2023, the total number of phishing attacks increased by 4.6 times, with each company encountering phishing 24% more often (5).

In modern scientific literature devoted to cybersecurity issues, scientists classify phishing by the method of data collection and by the method of distribution. The classification of phishing by the first criterion is already recognized as traditional, where two main types are distinguished: fake site. Here hackers use the same interface as the original, as well as similar domains, so that the user does not realize that he has accessed a duplicate site. In the email address of such a site, the data changes insignificantly, literally by one character. Most often, they change letters that look the same. For example, the uppercase I and lowercase L. Aliexpress.com and AIiexpress.com are different domains, although they do not differ visually; malicious file. Typically, this is a .rar archive that, when opened, infects the device with a virus, which then begins to engage in business espionage, collect corporate data and send it to devices of cybercriminals.

The classification of phishing by the second criterion – by the method of distribution – is considered innovative today, since it reflects new trends in the development of cybercrime and in recent years has presented the greatest danger to business in the form of: fake websites sent via email or instant messengers in the form of a letter or message and sent allegedly on behalf of a certain business structure. Inside, they contain a picture or table disguised as a document, malware, a link to a website created by cybercriminals, a demand to transfer money to a specified account or phone number, etc. Employees of the victim company, unaware of the deception, follow the link and provide the hackers with the necessary data. In the Eurasian economic space, such a negative practice was first discovered in 2020 in Kazakhstan, where letters were sent on behalf of the Minister of Health of the Republic. In them, hackers informed local business structures about the opportunity to receive free protective equipment as part of state aid. To do this, the website offered Kazakhstani entrepreneurs a simple action: fill out a simple form and send it to the specified address. The letter to the entrepreneurs contained documents attached, upon opening which a virus program from the Loki PWS family was introduced onto the user's computer. The purpose of this program is simple, but extremely dangerous: stealing logins and passwords from a computer (3); fake websites that appear in search results. Cybercriminals are highly active on the eve of events associated with consumer or sports-mass excitement (start of sales of new iPhone models, online sales, professional holidays, sports and entertainment events, etc.), when, on the eve of a corporate party, business management, employees or members of their families make spontaneous online purchases, make ill-considered and hasty decisions regarding their budget expenditures, without noticing the catch. For example, In 2020, ahead of the massive Black Friday sales, Group-IB experts identified almost half a thousand fake pages that copied the popular AliExpress marketplace, as well as about two hundred clone sites of online stores. At the same time, online fraudsters used similar resource names to fraudulently sell customers low-quality, non-original goods, unlicensed goods and other low-quality products. In addition, the work of these sites is aimed at

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

stealing personal data, passwords, information about bank cards and accounts and other confidential information of users. Also, switching to fake sites exposes users to the risk of infecting electronic devices with viruses.

In our opinion, the primary problem associated with phishing at present is that there is no software that would fully protect a business structure and its employees. Ultimately, everything depends on how careful the latter will be when going to certain sites or using certain programs, whether they will be able to determine that a certain page is fake or a double, duplicating the original sites of real online stores, streaming services, social networks. Cybercriminals are guided by the fact that representatives of the business community and ordinary users will not be able to recognize a slight difference in the address or appearance of the site and, trusting the open page, will enter the information necessary for theft of funds: logins, passwords, bank account and card numbers, code words and other personal confidential information that will allow the attackers to realize their criminal intentions.

According to modern business practice, most often Cybercriminals counterfeit websites of financial organizations and institutions, mail, payment and online services, cloud storage, and bookmakers (Fig. 2).

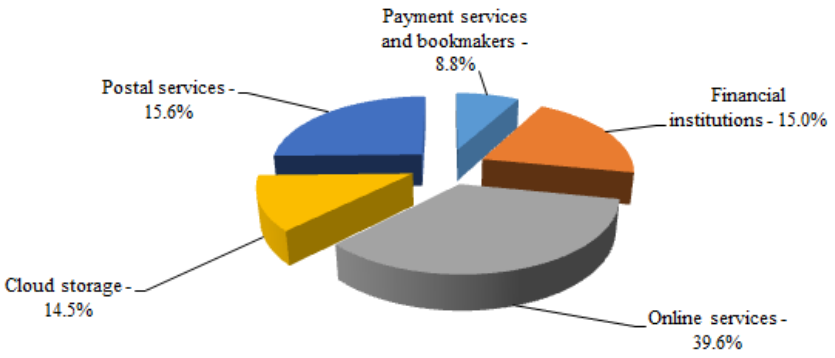

FIGURE 2
THE MAIN RESOURCES COUNTERFEITED BY CYBERCRIMINALS DURING PHISHING ATTACKS

Recently, there have been more frequent cases when, during phishing attacks, attackers blackmailed victim companies and demanded money in exchange for not publishing corporate and personal data online. For example, in 2023 , the Sneaking Leprechaun hacker group used a new extortion scheme, which affected more than 30 Russian and Belarusian business structures . engaged in software development and integration (10).

The Sneaking Leprechaun criminal group, guided by financial motives, chose those business entities that were willing to pay for the safety of their corporate data. As a result, industrial, logistics, financial and medical companies and even government agencies became victims of its phishing attacks. Hackers from the Sneaking Leprechaun group took advantage of vulnerabilities in outdated versions of Confluence, Bitrix and Webmin on Linux servers to gain access to the internal networks of business structures in Russia and Belarus. They uploaded their malware and gained a foothold in the system, gaining the necessary access to confidential company data. Remaining undetected, the fraudsters manually analyzed corporate data and copied those they

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

considered valuable. They then blackmailed business entities with the information they had stolen and demanded a substantial ransom, threatening to otherwise post it in the public domain.

In our opinion, it is much more difficult for businesses today to combat the multi-stage Letscall phishing attack, where modern vishing technologies are complemented by other malicious tools.

Vishing (from English voice phishing - voice phishing) is a type of fraudulent activity in which attackers , using phone calls and voice messages, often using psychological pressure, force company employees to hand over important confidential corporate information or transfer financial resources to the fraudsters' accounts. In combination with voice phishing, malware is distributed through a fake website that is a copy of the official Google Play app store. After installing such software, every call from the business structure's office is redirected to a hacker call center, where members of a cybercriminal group represented by Android developers, backend masters and call operators use pre-recorded bait messages and voice traffic routing. Such routing is carried out using IP telephony and WebRTC.

In addition, cybercriminals have Session protocols in their arsenal Traversal Utilities for NAT and Traversal Using Relays around NAT , which allows them to maintain high-quality communications and bypass NAT restrictions (19) .

Towards new vectors of development cybercrime should include spoofing - a new type of hacker attack, in which the criminal disguises himself as an official computer network or device and, in the form of a double, penetrates the legal information space of various entities, thus gaining access to confidential data or launching DoS attacks (denial of service attacks). Acting as a technique for falsifying electronic data by hackers and distorting information about themselves, spoofing helps to forge senders' email addresses and other parameters of corporate and personal mail. As a result, the true origin of the email is hidden, and the spoofed emails that replace it are sent to steal personal or corporate information, distribute malicious attachments and other cyberattacks.

As noted in the scientific community, there are many types of spoofing, among which the most popular today are: Email spoofing , which allows you to forge the real address of the company sending the letter and create the appearance that it came from another legal entity or individual. In the "From" field, the recipient of such a message will see the name of a reliable sender, although in fact it will be a cyber fraudster; IP address spoofing — distortion of IP addresses in corporate data packets transmitted to the target server. This type of spoofing is used to hide the hacker's true location on the Internet; DNS spoofing — substitution of a domain name (filling the DNS cache with fake corporate or personal data) to redirect the user to a false site. The goals here may be obtaining confidential information or spreading viruses; ARP spoofing - interception and substitution of corporate or personal data that is transmitted between two devices; Caller ID spoofing - substitution of a telephone number, as a result of which, when a call comes in, the number displayed on the screen will not be the one from which the call is actually coming; GPS/GNSS spoofing — transmission of a false signal to a GPS receiver, which is used to adjust the data on the actual geolocation of an object in the direction desired by the cybercriminal; Geolocation spoofing - substitution of geolocation, forcing the network to believe that the user's device is located in another country (for example, using VPN services) (2).

In our opinion, spoofing, as a new type of hacker attack on business, can cause considerable harm to companies:

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

a) *lead to blocking of IP and domains. After sending spam, these IP addresses end up on blacklists*
b) *Reduce the volume of corporate information delivery, since filters block legitimate emails due to the damaged reputation of the sending company. In turn, mass blocking and low deliverability lead to significant financial losses;*
c) *damage the brand image, because when cyber fraudsters send out spam, phishing emails and viruses on behalf of a business entity, the trust of customers in the latter will be undermined;*
d) *Distribute software to steal internal and client data of a business structure, which leads to the leakage of confidential information and will also negatively affect the brand's reputation.*

The specialists of the BI.ZONE company presented statistics in the field of combating potentially dangerous email distributions. According to them, in the first half of 2023 alone, 600 thousand illegitimate emails containing spoofing were blocked (22) .

The Russian state, which has been under the burden of Western economic sanctions (23) in recent decades, like a number of other countries in the world (Iran, Venezuela, Syria, Nicaragua, Cuba, North Korea, etc.), in our opinion, has had no time for the problem of ensuring the cybersecurity of domestic businesses and the country's population. However, today, official bodies represented by the country's leadership, representatives of the State Duma, the Ministry of Digital Development, Communications, Mass Media, the State Supervision Service, the Federal Service for Technical and Export Control, and Rosfinmonitoring are doing everything possible to counter new vectors of cybercrime development (phishing modifications, spoofing, modern ransomware, etc.) . First of all, we note the signing on June 13, 2023, by the President of Russia of the Federal Law providing for the confiscation of property and money from cybercriminals that were obtained through illegal activities. Amendments have already been made to the Criminal Code, and the law has acquired legal force. Among other significant steps taken at the state level, the following should be highlighted: preparation by the Ministry of Digital Development, Communications and Mass Media, together with relevant departments, of amendments to RF Government Resolutions No. 325 and No. 1236 concerning the register of domestic software, which has been in operation for over eight years. In particular, the list of requirements necessary to receive all the benefits due will change. The new rules are expected to come into force in 2024 (20) ; introducing a bill to the State Duma on the legalization of "white" hackers (pentesters), which will enable them to conduct their activities legally, subject to certain conditions. One of the main conditions for the legal work of a pentester is that he is obliged to provide the results of his activities to the copyright holder within five days (11); FSTEC's demand that domestic software developers speed up fixing vulnerabilities in software of Russian origin, threatening to revoke their licenses. They currently spend twice as much time fixing errors as their foreign competitors, who are banned from our country's market (16) ; Rosfinmonitoring is concerned that Russians are increasingly becoming droppers (front men), helping criminals to cash out stolen money through illegal schemes to withdraw funds from Russians' bank cards. The most common scheme is to issue a bank card and transfer it to third parties for a fee (29) ; the initiative of the Ministry of Digital Development, Communications and Mass Media, approved by the Russian government, on monetary compensation for corporate and personal users who suffered as a result of a leak of confidential information . Such a step by a business structure will be considered as a mitigating circumstance when determining the punishment provided for by the law on turnover fines. The decision on whether a business structure deserves leniency will be made by the affected users, who can reject the compensation if it does not suit them (12); introduction of new cybersecurity regulations for hosting providers by the state. Changes and additions were made to the Law "On Information", which established that hosting providers are required to connect to the FSB GosSOPKA cyberattack counteraction

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

system, and they are also required to block those resources and domains that are noticed as sources of cyberattacks. Hosting providers must transfer information about detected malicious sites and resources to the specified FSB GosSOPKA system. Companies will also have to take part in exercises to disconnect the Runet from the global network (25) ;

- a recommendation from the head of the government commission on crime prevention to the Investigative Committee of the Russian Federation, together with the Ministry of Internal Affairs of Russia, to amend the Criminal Code of the Russian Federation by December 1, 2024, classifying crimes committed with the help of IT technologies as aggravating circumstances (13).

Of course, this is far from a complete list of government measures to support and protect domestic businesses and the population of our country from the growing activity of hackers. But already in 2023, it became obvious that these measures eliminate, rather, various consequences, rather than the causes of high cybercrime. Such elimination primarily works for large businesses, which have recovered to a certain extent from the indirect impact of Western economic sanctions and adapted to new cybersecurity challenges (18.30). We add that businesses of any format should not rely solely on such “framework” government measures to ensure cybersecurity, since the latter orient them, especially small and medium-sized companies, to use only moderate partnership (“adoption”) and “passive protection” strategies (4.8).

Thus, it is impossible to solve the problem of combating cybercrime in modern Russia without consolidating the efforts of the government, business and the population.

The consolidated participation of domestic business found its expression in the creation of the joint-stock company F.C.C.T. Today , having separated from Group - IB , it has become Russian from the legal and resource points of view, where its own vendors have replaced Western ones.

The most important areas of activity of the F.C.C.T. company in the information security market at present include: search and collection of information about hacker attacks aimed at a specific business structure, optimization of existing mechanisms for protection against them using cyber intelligence data (Unified Risk Platform); proactive analysis of cyber threats, maximum protection efficiency and prevention of hacker attacks by understanding the methods, tools and intentions of attackers (Threat Intelligence); combating online fraud; protecting businesses and their customers from digital risks, preventing fraud in real time and protecting the user's digital identity (Fraud Protection); identify and eliminate cyber threats; prevent attacks in real time for hosts, network, infrastructure and email (Managed XDR); cyber attack vector management, continuous detection of digital assets to eliminate information risks and prevent leaks and incidents (Attak Surface Management); brand and digital asset protection ; AI platform for protecting digital assets, the company's brand and its customers, as well as for identifying and eliminating digital risks (Digital Risk Protection); blocking hacker attacks in email; proactively detecting and preventing complex targeted attacks in email using patented technology to protect against detonation of any malicious objects in mail (Business Email Protection) etc.

The timeliness of the creation of the joint-stock company F. C. C. T. is confirmed by the results of its effective work already in the first financial year: the number of clients increased by 1/3, sales volume and revenue increased by 60% and 35 % respectively. Moreover, 80% of revenue came to the company through such a channel as the regional partner development program (33).

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

At the same time, it should be noted that the services provided to domestic businesses by the joint - stock company F.C.C.T. are quite expensive by Russian standards. Taking into account the current high differentiation of domestic business structures by the size of their assets, it should be recognized that many small and medium-sized business entities, especially in the regions, are not ready to acquire information security services, both financially and organizationally. Until now, at best, they have done a pentest once a year, there is no talk of any full diagnostics (check - up), there is a clear lack of qualified personnel to counter cyber threats, etc.

In this regard, we studied the industry landscape of the request of second-tier entrepreneurs in the Tyumen region for services to search for vulnerabilities in software, web applications and the company's IT infrastructure (Fig. 3).

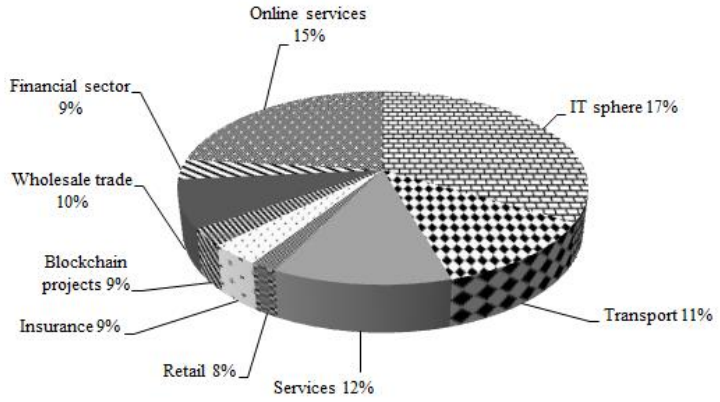

FIGURE 3
INDUSTRY LANDSCAPE OF REQUESTS FROM SMALL AND MEDIUM-SIZED ENTREPRENEURS IN THE REGION FOR VULNERABILITY SEARCH SERVICES IN SOFTWARE, WEB APPLICATIONS AND THE COMPANY'S IT INFRASTRUCTURE.

It follows from Fig. 3 that in all the considered industries of the Tyumen region, the demand of entrepreneurs for vulnerability search services in software, web applications and IT infrastructure of the company is very low, averaging about 11%. In our opinion, this is not only a matter of the relative high cost of cyber services, but also the fact that no financial resources are allocated for the provision of the latter from regional programs to support small and medium-sized businesses. Therefore, "second-tier" business entities have to rely only on their own efforts in this matter. In this regard , the position of S. Bhargavi is of some practical interest. Analyzing the Fortinet report on business gaps in cybersecurity skills in 2022, he suggests that "second-tier" business entities take advantage of the best courses and methods for combating hackers developed by the EU Council (9). Today, a lack of cybercrime skills accounts for 80% of hacks, and 64% of companies experience cybersecurity breaches, leading to lost revenue and fines (1).

Returning to the issue of small and medium-sized businesses using cybersecurity courses and methods proposed by the EU Council, we would like to point out that this is entirely possible, since they include:

Free entry-level cybersecurity courses (zero experience in cybersecurity) on:

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

I. Basics of network security (N|DE);
II. The basics of ethical hacking (E|HE);
III. Fundamentals of Digital Forensics (D|FE);

Relatively inexpensive courses to develop entry-level skills leading to a Cybersecurity Technician (C|CT) certification (6).

CONCLUSION

The good news in the context of the problem under consideration is that at the end of 2023, in a number of regions of the Russian Federation, some small and medium-sized business entities began to invest in the development of their own information security level in terms of building internal cybersecurity monitoring centers (SOC - Security Operation Center). The latter are a structural unit of a business structure responsible for the prompt study of the IT environment and response to cyber incidents.

And although the budgets of "second-tier" companies are quite modest, in our opinion, they may be sufficient to lay the foundation for building a typical SOC that meets the most minimal standards . combating cybercrime. The process of achieving such minimum standards is a sequence of stages of implementing simple organizational and methodological recommendations for preventing cybercrime and minimizing its consequences (Fig. 4).

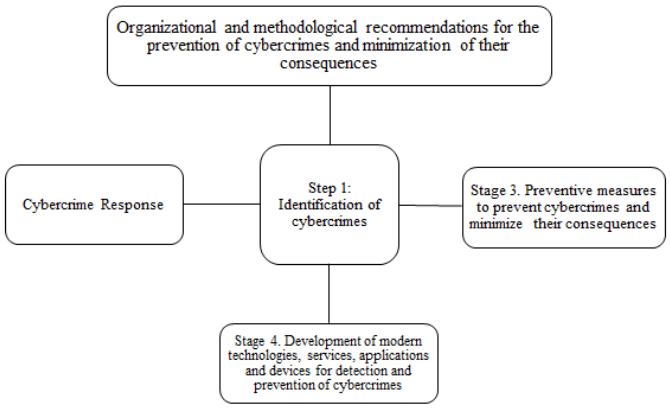

FIGURE 4
Stages of achieving minimum standards for combating cybercrime when building a typical SOC

Stage 1. Detection, registration and classification of cybercrimes is the first step towards solving the task. To achieve this task, various tools for such identification are used , in particular:

network traffic monitoring . This tool is a process of observing and analyzing information and data that are transmitted over the network. During this monitoring, suspicious actions, atypical traffic or violations of cybersecurity policy are identified. Such monitoring is carried out using specialized software or equipment (sniffers, proxy servers, firewalls, etc.);

express analysis of logs and protocols, considered as a process of studying and interpreting records created by information systems, applications or devices during various operations, events or actions. It makes it possible to identify cybercrimes (failed login attempts, unauthorized access, modification or deletion of corporate or personal data, violation of access rules, etc.); intrusion detection and prevention systems (IDS/IPS) in the form of software or hardware

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

solutions that "monitor" network traffic, logs, and protocols and compare them with a database of threats, vulnerabilities, or behavioral patterns. Intrusion detection systems (IDS) are designed to notify company management about cybercrimes, block them, or suspend them. Note that IDS/IPS systems can be deployed at different network levels (e.g., host, network level, application level).

Stage 2: A systematic approach to combating cybercrime requires clear implementation of agreed response procedures that define how to act if they are detected. Such procedures include: the process of creating a document containing the goals, policies, roles, responsibilities, processes and resources that are necessary to respond to cybercrimes. It should be noted that this process ends with the preparation of a response plan, which should be developed in advance, taking into account various scenarios, threats, vulnerabilities, and also regularly updated and tested; the process of notifying and coordinating stakeholders (company management, its staff, clients, partners, suppliers, law enforcement agencies, etc.) upon detection of a cybercrime about its characteristics, such as time, place, source, target, vector, effect, etc. These messages also include analysis, assessment, priorities, assignment, execution and control of actions aimed at preventing cybercrimes and their consequences; the process of returning information and information systems to a normal state after a cybercrime, identifying the causes, details and rank of its significance. This also includes the development of proposals and conclusions aimed at preventing cybercrimes and the material and financial damage caused by them.

Stage 3. Preventive measures to prevent cybercrimes and minimize their consequences include the following actions: the process of training and informing the company's employees, its clients and business partners about the principles, policies, standards and practices of cybersecurity, about the types, methods and consequences of risk events, etc. Training of personnel and raising their awareness of potential cybercrimes can be carried out using various forms and methods (lectures, seminars, webinars, trainings, brochures, posters, e-mails, etc.); the process of creating and implementing in practice the company's cybersecurity policy, which is a set of rules, tools, organizational approaches and activities on how and in what order the company's information systems should be protected, used, managed and supported. The company's cyber policy is intended to be based on the analysis of economic, information and social risks, consistent with business goals and requirements, observed by all interested parties, and also documented, distributed, controlled and updated; the process of checking the status and assessing the effectiveness of cybersecurity, identifying and eliminating threats and vulnerabilities, and breaches in information systems. Regular audits of risk events and their consequences can be carried out both by specialists of the business structure itself and on the basis of outstaffing using a variety of methods and tools (for example, testing, scanning, observation, interviews, questionnaires, etc.).

Stage 4. The continuing expansion of the spectrum of cyber threats, vectors of hacker attacks and leaks of corporate and personal data suggests that today, preventive measures alone to prevent cybercrimes and minimize their consequences are clearly not enough. The development of modern technologies, services, applications and devices for detecting and preventing cybercrimes is becoming objectively necessary. For example, blockchain and cryptography can be used to create secure systems for storing, transmitting and verifying confidential data of a company and its employees. Biometrics and behavioral analytics can strengthen user authentication and authorization, as well as detect potential threats and vulnerabilities, and therefore prevent cybercrimes. The use of quantum computing and quantum

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

cryptography contributes to the creation of more reliable encryption and decryption systems corporate and personal data.

As for artificial intelligence (AI) and machine learning (ML), they are currently promising and influential technologies in the field of cybersecurity. They make it possible to analyze large volumes of business data, identify anomalies, learn normal and abnormal business behavior, automate and optimize cybercrime response processes, etc.

Let's be honest: the final fourth stage of building a typical SOC goes beyond the minimum standards for combating cybercrime at the level of small and business structures. But hypothetically allowing it, we prescribe the trajectory of a long-term strategy for the development of a typical SOC from the very beginning to its transformation into a complete socio-economic system.

REFERENCES

Admon, M. Top skills required to start a career in cybersecurity / M. Admon. - Text : electronic. - URL: https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/top-skills-start-career-in-cybersecurity/ (дата обращения: 17.07.2023).

Current Spoofing Methods These Days - Text: electronic // Hacker: electronic journal. - URL : / Hacker. ru / 2023/10/16/ relevant - spuffing / (date accessed: 23.07.2023).

Akhrorova, A.D. Factors of economic space and business network in increasing economic security of businessb / A.D. Akhrorova, Z.K. Smagulova, S.K. Zhanuzakova - Текст: непосредственный // Bulletin of the Innovative University of Eurasia. - 2021. - № 2. - P. 56-63.

Approaches to the assessment of economic security of subjects small and medium business in the Eurasian economic union / Simonov S.G., Lysenko I.V., Khamatkhanova M.A. [et al.] - Text: direct // Mediterranean Journal of Social Sciences. - 2015. - T. 6. - № 4. - P. 509-515.

Acronis' mid-year cyberthreats report reveals 464% increase in email attacks : press release - Text : electronic. - URL : https://www.acronis.com/en-us/pr/2023/ (дата обращения: 29.06.2023).

A complete guide to best cybersecurity courses: beginners, advanced, & specializations. - Text : electronic. - URL : https://infocerts.com/ (accessed: 23.07.2023).

Azure AD Microsoft Bug Allowed hackers to breach over two dozen organizations via forged Azure AD tokens: press release. - Text : electronic. - URL : https://thehackernews.com/2023/07/microsoft-bug-allowed-hackers-to-breach.html (дата обращения: 23.07.2023).

Business in the era of global change: monograph / S.G. Simonov, E.V. Kurushina, E.A. Koryakina [et al.]. - Tyumen: TIU, 2023. - 210 p.: - ISBN 978-5-9961-3163-1/ - Text: direct.

Bhargavi, S. Fortinet releases its 2022 cybersecurity skills gap report / S. Bhargavi. - Text: electronic. - URL: https://channelpostmea.com/2022/05/09/ (date appeals : 25.07.2023).

Voloshin, E. BI . ZONE has discovered unusual ransomware attacks on dozens of companies in Russia and Belarus / E. Voloshin. – Text: electronic. - URL :

https://bi.zone/news/ (date accessed: 23.05.2023).

A bill on legalizing "white" hackers has been submitted to the State Duma. – Text: electronic. - URL : https://ria.ru/20231212/zakonoproekt-1915369737.html (date of access: 12.12.2023).

The Government has approved compensation for those affected by leaks. – Text: electronic. - URL : https://t.me/mintsifry/1990 (date of access: 09/26/2023).

In Russia, crimes using IT will be classified as aggravating circumstances in the Criminal Code . - Text : electronic. - URL : https :// iz . ru /1661129/2024-03-07/ (date of access: 07.03.2024).

DDoS botnets hijacking zyxel devices to launch devastating attacks . – Text: electronic . - URL: https://thehackernews.com/2023/07/ddos-botnets-hijacking-zyxel-devices-to.html (date accesses : 22.03.2023)

Erokhin, S. The Ministry of Internal Affairs called Telegram the main tool for criminals in the IT sphere / S. Erokhin. – Text: electronic. - URL : https://tass.ru/obschestvo/19984855 (date of access: 14.02.2024).

There is no shortage of protection. – Text : electronic. - URL : https://www.kommersant.ru/doc/6266589 (date of access: 10.10.2023).

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.

Ivanov, S. Cybercrime is exploding Russia: the number of hacker attacks has grown by a third in six months / S. Ivanov. – Text: electronic. - URL : https://newsorel.ru/fn_1403697.html (date of access: 08.11.2023).

Koryakina, E. A. Social interaction of large businesses as a security condition of its operation and development in the Northern region / E. A. Koryakina, N. P. Sheveleva, N. S. Kulakova. - DOI https://doi.org/10.18510/hssr.2019.74100. - Text : electronic // Humanities & Social Sciences Reviews. – 2019. - Vol 7. - № 4. - Pp. 773-780.

Letscall – new sophisticated Vishing toolset - Text : electronic. - URL: https://www.threatfabric.com/blogs/ (date accessed : 07.07.2023).

Lyubavina, A. The registry of domestic software will be divided into Russian software of the first and second grade / A. Lyubavina. - Text: electronic. - URL : https://www.cnews.ru/news/top/2023-12-04_pravila_vneseniya_v_reestr (date of access: 04.12.2023).

Markov, D. What is phishing: how not to become a victim of hackers / D. Markov. - Text: electronic. - URL : https://trends.rbc.ru/trends/industry/602e9fe79a7947a4bd611504 (date of access: 07.02.2023).

Medzhlumov, M. 75% of incoming letters pose a danger to Russian companies / M. Medzhlumov. - Text: electronic. - URL : https://infobezopasnost.ru/blog/news/ (date of access: 25.07.2023).

Mulder, N. The economic weapon: the rise of sanctions as a tool of modern war / N. Mulder. – Text : direct. - Yale University Press, 2022. - 448 p.

Moraes, M.T. The importance of iot security: understanding and addressing core security issues / M. Moraes. - Text : electronic. - URL : https://infocerts.com/ (дата обращения: 23.07.2023).

Providers are preparing for shutdowns. - Text : electronic. - URL : https :// www . kommersant . ru / doc / 6212718 (date of access: 15.09.2023).

Russia enters top 10 in number of cyber attacks - Text : electronic. - URL : https://infobezopasnost.ru/blog/news/ (date accessed: 05.07.2023).

Russian companies are concerned about their security. - Text: electronic - URL: https://cisoclub.ru/rossijskie-kompanii-ozabotilis-svoej-bezopasnostju/ (date of access: 31.05.2023).

Russia is among the top ten countries in the world most attacked by hackers. - Text: electronic. - URL : https://lenta.ru/news/2023/07/05/ddos/ (date accessed: 07/05/2023).

Rosfinmonitoring: Many citizens do not realize that fraudsters make them accomplices to crimes. - Text : electronic. - URL : https://cisoclub.ru/ (date of access: 02.11.2023).

Simonov, SG Theoretical and methodological approaches to the assessment of the economic security level of the Russian major oil and gas companies / SG Simonov , VV Efremova, MA Khamatkhanova . - Text: direct // Modern Journal of Language Teaching Methods, 2019. - Vol. 9. - Issue 1, January. - Pp.619-624.

Telegram breeds cybercriminals. - Text : electronic. - URL : https://telegra.ph/Telegram-plodit-kiberprestupnikov-02-01 (accessed: 01.02.2024).

The risks and preventions of ai in business: safeguarding against potential pitfalls/ - Text : electronic. - URL: https://thehackernews.com/2023/07/the-risks-and-preventions-of-ai-in.html (date accessed : 12.07.2023).

Shabanov, I. Valery Baulin: Shareholders of F . A . S . S . T . see huge development potential in Russia / I. Shabanov. - Text: electronic - URL : https://www.anti-malware.ru/interviews/2023-07-14/41565 (access date: 14.07.2023).

Received: 15-Jan-2025, Manuscript No. AEJ-25-15881; **Editor assigned**: 20-Jan-2025, PreQC No. AEJ-25-15881(PQ); **Reviewed:** 30-Jan-2025, QC No. AEJ-25-15881; **Revised**: 04-Feb-2025, Manuscript No. AEJ-25-15881(R); **Published:** 11-Feb-2025

Citation Information: Gennadievich, S S., Alaudinovna, K M., Vyacheslavovich, L I. (2025). Cybercrime: New Vectors of Development and Ways to Fight them. *Academy of Entrepreneurship Journal, 31*(1), 1-13.