ROADMAP – CYBER SECURITY IN RUSSIA

ROOT LEVEL RESOURCES

It is virtually impossible to imagine modern society without thinking of information and telecommunication technologies. This, however, comes with the downside of new types of crimes.

According to a federal government body, FKU, which is recognized as the main information and analytical centre of the Ministry of Internal Affairs of Russia, between the months of January and September 2019, 205.1 thousand crimes related to information and telecommunication technologies were registered. This is a 69.2% year-on-year increase. The proportion of these types of crimes when compared to the total number of crimes committed also increased from 8.1% to 13.5%, from January to September 2018.

Almost all such crimes (98.3%) were detected by the bodies of internal affairs.

Almost half of the crimes (48.3%) or 99,000 fall into the categories of grave and especially grave. More than half (52.9%) or 108,500 were committed with the help of the Internet, more than a third (38,8%) or 78,500 - with the help of mobile devices.

Three quarters of such crimes (78,6%) involved theft or fraud: 161,300, which is a 84.9% increase on the year prior. Almost one in eleven crimes (8,7%) were carried out for the purposes of illicit production, sale or distribution of drugs, psychotropic substances or their analogues: 17,900, which is a 34,7% year-on-year increase.

The Prosecutor General's Office of the Russian Federation characterizes cybercrime growth as "very substantial." When compared with the data the agency gathers on other types of crimes, the growth rate in this segment is the highest.

Number of crimes registered between the months of January and September 2019

205 116

Including grave and especially grave

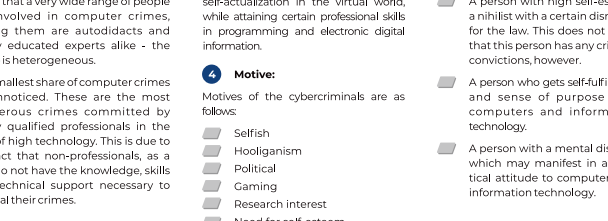
99 040

Including those committed using:

23 259 Payment (plastic) cars	**726** Fictitious payments
14 267 Computer hardware	**108 540** Internet
4 494 Software tools	**78 479** Mobiles

158 CC RF – Theft	**61 074**
159 CC RF – Swindling	**83 333**
159[3] CC RF – Payment card fraud	**10 371**
159[6] CC RF – Computer information fraud	**533**
171[2] CC RF – Illegal gambling	**685**
205[2] CC RF – Public calls for committing of terrorist activity or public justification of terrorism	**161**
228[1] CC RF – Illegal production, sale or distribution of narcotic drugs, psychotropic substances or their analogues, as well as illegal sale or distribution of plants containing narcotics or psychotropic substances, or their parts containing narcotics or psychotropic substances	**17 871**
242, 242[1], 242[2] CC RF – Production of pornographic materials	**1 485**
280 CC RF – Public calls for extremist activity	**210**
Crimes in the sphere of computer information Chapter **28 of the Criminal Code of the RF**	**2 044**
272 CC RF –Illegal access to computer information	**1 683**
273 CC RF – Creation, use and dissemination of harmful computer programmes	**354**
274 CC RF – Violation of the operation rules of computer information storage, transmittance and processing facilities or those of information telecommunication networks	**–**
274[1] CC RF – Negative impact on the critical infrastructure of the Russian Federation	**–**

***CC RF** - Article of the Criminal code of the Russian Federation*



Total number of criminal cases solved in the reporting period

Total number of unresolved cases in the reporting period:

Total number of criminal cases sent to court with indictments and in relation to which charges have been made

Regions of the Russian Federation with the highest and lowest growth rate of registered crimes

The percentage of crimes committed using information and telecommunication technologies (general breakdown of the crimes)

Regions of the Russian Federation with the highest and lowest proportion of registered crimes

Khanty-Mansi AO-Yugra **26,1%**	Jewish Autonomous Region **8,8%**
Yamalo-Nenets AO **25,9%**	Transbaikal region **8%**
Chuvash Republic **25,8%**	Republic of North Ossetia-Alania **7,8%**
Penza region **22,5%**	The Republic of Buryatia **6,8%**
Komi Republic **22,2%**	Tyva Republic **5,9%**
Murmansk region **21,5%**	Moscow region **4,9%**
Kirov region **20,1%**	Saint Petersburg **4%**
Mari El Republic **20%**	The Republic of Ingushetia **3,5%**
The Republic of Mordovia **19,6%**	The Republic of Dagestan **3,2%**
Vologodskaya Oblast **19,2%**	Chechen Republic **1,7%**

Regions of the Russian Federation with the highest and lowest crime detection rate

The Republic of Dagestan **71,5%**	Yamalo-Nenets AO **19,5%**
The Republic of Ingushetia **59,4%**	Voronezh region **18,9%**
Chukotka Autonomous Okrug **54,7%**	Kaluga region **17,7%**
Orenburg region **51,6%**	Leningrad region **17,5%**
Chechen Republic **47,7%**	Stavropol region **17,1%**
Moscow region **46,9%**	Krasnodar region **17,1%**
Pskov region **46,5%**	Murmansk region **16,9%**
The Republic of Sakha (Yakutia) **43,8%**	Republic of Tatarstan **16,8%**
Republic of Adygea **43,7%**	Moscow **15,5%**
Ulyanovsk region **43,6%**	Tver region **13,6%**

Cybercriminal in the Russian Federation - Who is It?

ROOT LEVEL RESOURCES

Today almost anyone can launch a cyber attack. However, in most cases, the modern-day cybercriminal is part of a group; there are virtually no individual actors carrying out attacks independently from start to finish. This can be explained by the fact that attacks have grown in complexity - attackers now need to cooperate. So a successful cybercriminal is someone who is a good leader and who has created a team, this person may not be a computer programmer at all. This tends to complicate matters when it comes to accountability for attacks during the investigative process, and it increases the total number of parties involved in cybercriminal activity. Nevertheless, based on the most current data available, a portrait of a cybercriminal is as follows:

1 Degree:

The level of educational attainment of individuals committing this type of crime is an important indicator of the criminals' intelligence and it is often linked to the nature of their criminal acts.

It is often thought that cybercriminals are highly qualified professionals with higher education degrees in the fields of science or law. However, research reveals that cybercriminals typically have technical secondary education, incomplete higher education or higher education, whereas specialized third level education is less common. In criminological literature, cybercriminals are commonly described as talented, curious people with a high level of intelligence who are likely to be self-taught. However, it should be noted that a very wide range of people are involved in computer crimes, among them are autodidacts and highly educated experts alike - the group is heterogeneous.

The smallest share of computer crimes go unnoticed. These are the most dangerous crimes committed by highly qualified professionals in the field of high technology. This is due to the fact that non-professionals, as a rule, do not have the knowledge, skills and technical support necessary to conceal their crimes.

2 By age:

The age of cybercriminals ranges from 18 to 35. There are few cyber criminals who are older than that, since, in the Russian Federation, computer technology started to be widely used in the late 90s, and it is more difficult for older people to master it. The modern-day cyber criminal skews even younger because children and adolescents are introduced to computer equipment and network information technologies early on. According to some researchers, the age of cyber criminals now ranges from 15 to 45.

3 Gender:

Most researchers agree that it is men who commit the vast majority of such crimes. However, recently there has been documented an uptick in the number of women committing cyber crimes. Most of the time, when women are involved, they tend to be partners in the crime.

A person who does not look very attractive and faces difficulties in social settings, especially with peers of the opposite sex, someone who is seeking self-actualization in the virtual world, while attaining certain professional skills in programming and electronic digital information.

4 Motive:

Motives of the cybercriminals are as follows:

- Selfish
- Hooliganism
- Political
- Gaming
- Research interest
- Need for self-esteem
- Revenge
- Those associated with mental disorders
- Self-esteem
- Desire for fame.

5 Appearance and psychological aspects of personality:

Usually it is:

- A person who does not look that attractive and faces difficulties in communication with peers of the opposite sex, seeking self-realization in the virtual world, while achieving certain professional skill in programming and using electronic digital information.
- Reserved, secretive person.
- A person striving for self-esteem, wishing to gain fame and authority in his social circle.
- A bright and clever person capable of making responsible decisions.
- A person with high self-esteem, a nihilist with a certain disregard for the law. This does not mean that this person has any criminal convictions, however.
- A person who gets self-fulfillment and sense of purpose from computers and information technology.
- A person with a mental disorder which may manifest in a fanatical attitude to computers and information technology.

To understand the dynamics of cyber crime, it is important to research the personality type of cyber criminals and update this knowledge base regularly. This can not only have a positive impact on the process of uncovering and investigation of these crimes, but it may also help in their development of future preventive measures.

It is worth pointing out that it is now very advantageous to be a cyber criminal from a financial point of view. As a result, cybercrime may also attract opportunistic, adventurous and even charismatic people who seek to profit off of criminal activity while avoiding criminal penalty.

What is at stake?

ROOT LEVEL RESOURCES

Due to the speed of development of information technologies, the types of cybercrimes being carried out are rapidly evolving. The schemes used to profit from illegal activity are becoming more advanced every year. As of now, the following types of cybercrimes can be identified:

Data Theft

Competitive espionage, phishing, theft of intellectual property, trade secrets, credentials and other confidential information.

Financial Crimes

Theft of cryptocurrency, fraud involving online and mobile banking systems, attacks on ATMs, card processing systems, SWIFT, payment templates.

Attacks on Critical Infrastructure

Attacks on water supply systems, transport infrastructure, process control systems in the sector of energy, oil and gas.

Malware Attacks

Production, distribution and control of malware, botnets, fraudulent email newsletters, ransomware and spyware.

Information Wars

Extortion, undermining of reputation, distribution of negative information, online harassment and identity theft.

Insider Threats

Abuse of authority, competitive espionage, data leakage, account theft.

DDoS Attacks

Customized and targeted attacks on web service providers with the objective of interruption or disruption of the normal traffic of a web-property.

Intellectual property theft

Misappropriation of source code, software and other information products.

Who is next on the list? Everyone is a target:

ROOT LEVEL RESOURCES

As a rule, cyber criminals perform targeted attacks on enterprises that process or store information they can profit from. Frequently, cyber criminals in the Russian Federation attack:

1

Objects of Critical Information Infrastructure (CII). In 2018, there were detected close to 4.3 billion cyber attacks on the critical infrastructure of the Russian Federation. Among the attacked entities were Rosneft and two dozen other large Russian organizations, including those in the strategic sectors of oil, gas, chemicals, agriculture and so on. Attackers also targeted several large Russian exchanges.

2

Financial institutions, especially banks where the use of information technologies is widespread, should be distinguished and examined separately from CIL. Criminals attack servers or banking networks to gain access to data and carry out illegal transfers of funds from customers' bank accounts. However, theft is not the worst thing that can happen to a financial institution. Banks were among the targets of government-backed hacker groups who specialize in sabotage. A cyber attack carried out by such a group, if successful, can result in the financial institution's liquidation and can lead to a total collapse of a national financial system.

3

Billing Companies. When targeting a billing company, criminals try to gain access to user accounts or steal valuable information such as customer databases, financial information or other data.

Why is the insurance industry in no hurry to offer cyber insurance coverage?

The main issue in the Russian Federation is that customers lack an understanding of this type of insurance coverage. Furthermore, insurance companies are unwilling to introduce new insurance products. Note the following:

Notable factors in the Russian insurance legislation:

1. Threat of intensity growth
2. Threat of concentration
3. Difficulties in development and evaluation of risk models
4. Lack of infrastructure for the settlement of insurance claims
5. Risk-averse companies reluctant to take on new threats
6. Complex and costly underwriting
7. Technical difficulties of organising and settling insurance claims

What do consumers need?

ROOT LEVEL RESOURCES

The cyber insurance market in Russia is currently at its nascent stages. However, over time it can turn into a useful tool for ensuring information security and protection against cyber threats. The market potential is huge: any bank, company or organization handling valuable data and information is at risk.

Overview of the laws governing the issues of legal protection of network security in the Russian Federation

ROOT LEVEL RESOURCES

Constitution of the Russian Federation of 12.12.1993: http://www.consultant.ru/document/cons_doc_LAW_28399/

Codified rules and regulations:

- The Civil Code of the Russian Federation dated 30.11.1994 №51-FZ in 4 parts :
  1) http://www.consultant.ru/document/cons_doc_LAW_5142/,
  2) http://www.consultant.ru/document/cons_doc_LAW_9027/#dst0,
  3) http://www.consultant.ru/document/cons_doc_LAW_34154/#dst0,
  4) http://www.consultant.ru/document/cons_doc_LAW_64629/#dst0
- The Code of Administrative Offenses of the Russian Federation dated 30.12.2001 №195-FZ : http://www.consultant.ru/document/cons_doc_LAW_34661/
- The Criminal Code of the Russian Federation dated 13.06.1996 №63-FZ: http://www.consultant.ru/document/cons_doc_LAW_10699/
- The Labor Code of the Russian Federation dated 30.11.2001 №197-FZ, http://www.consultant.ru/document/cons_doc_LAW_34683/
- The Tax Code of the Russian Federation dated 31.07.1998 №146-FZ: http://www.consultant.ru/document/cons_doc_LAW_19671/

Federal laws of the Russian Federation and other:

- Law on Information, Information Technologies and the Protection of Information dated 27.07.2006 №149-ФЗ : http://www.consultant.ru/document/cons_doc_LAW_61798/
- Law on State Secrets dated 21.07.1993 №5485-1: http://www.consultant.ru/document/cons_doc_LAW_2481/#dst0
- Law on Commercial Secret dated 29.07.2004 №98-FZ: http://www.consultant.ru/document/cons_doc_LAW_48699/#dst0
- Law on Banks and Banking Activities dated 02.12.1990 №365-1: http://www.consultant.ru/document/cons_doc_LAW_5842/
- Law on Insurance Household Deposits in the Banks of the Russian Federation dated 23.11.2003 №177-FZ: http://www.consultant.ru/document/cons_doc_LAW_45769/
- Law on Licensing Specific Types of Activity dated 04.05.20111 №99-FZ: http://www.consultant.ru/document/cons_doc_LAW_113658/
- Law on Personal Data dated 27.27.2006 №152-FZ: http://www.consultant.ru/document/cons_doc_LAW_61801/
- Law on Securities Market dated 22.04.1996-FZ: http://www.consultant.ru/document/cons_doc_LAW_10148/
- Law on Communications dated 07.07.2009 №126-FZ: http://www.consultant.ru/document/cons_doc_LAW_43224/
- Law on Technical Regulation dated 27.12.2002 №184-FZ: http://www.consultant.ru/document/cons_doc_LAW_40241/
- Law on the Security of the Critical Information Infrastructure of the Russian Federation dated 26.07.2017 №187- FZ: http://www.consultant.ru/document/cons_doc_LAW_220885/
- Law on Customs Regulation in the Russian Federation dated 03.08.2018: http://www.consultant.ru/document/cons_doc_LAW_304093/
- On Approval of Doctrine of Information Security of the Russian Federation dated 05.12.2016 №646: http://www.consultant.ru/document/cons_doc_LAW_208191/
- On National Security Strategy of the Russian Federation dated 31.12.2015 №683: http://www.consultant.ru/document/cons_doc_LAW_191669/
- GOST 34.0003-90. Interstate standard. Information Technology. Set of Standards for Automated Systems dated 12.27.1990 No. 2299 27.12.1990 №2299: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=STR&n=10020#007375066912518613