Moscow, January 14, 2022

The Issues of Informational Safety – New Threats for Office Printing Devices and the Corresponding Countermeasures

Moscow, January 14, 2022* — *Information Agency "Business-Inform" together with the Association of Quality Consumables Manufacturers and Suppliers presented the new results of the vulnerability research for office printing devices and the recommendations for removing the vulnerabilities.

Information Agency "**Business-Inform**" together with the Association of Quality Consumables Manufacturers and Suppliers (**AQCMS**), on 14th of January, this year, held the Conference **"The Issues of Informational Safety – New Threats for Office Printing Devices and the Corresponding Countermeasures".** During the Conference the results of the research were shown concerning the new vulnerabilities found in office printing devices in Russian and International organizations in 2021, as well as the recommendations on how to remove them. A special attention, during the Conference, was paid towards the modern policies of informational protection of businesses' corporate networks, and above all towards the policy of the "Zero Trust", as well as towards the issues related to the practice of workflow system usage (IT-outsourcing, MPS, the usage of remanufactured cartridges and newly-built cartridges). The Conference saw the participation of representatives from 162 Russian businesses and organizations, as well as from the leading Russian and International experts in the field of information safety.

During the Conference 3 reports were heard:

- **"Printers, MFPs and Cartridges – the Sources of Vulnerabilities. Audit of Printing Devices in Russian Organizations in 2021: the Results, Conclusions and Recommendations"** (speaker – Stanislav Malinskiy, Russian University of Transport)

The report theses: Office printing and its managing: legal, administrative and program-technical aspects; microprogram, system and applied software: vulnerabilities (evident and hidden), methods of passive and active protection; the leading manufacturing brands of printing devices and their policy in the field of informational safety provision; HP and branded microprogram FutureSmart software: vulnerabilities CVE-2021-39237 (CVSS score: 7.1) and CVE-2021-39238 (CVSS score: 9.3), and how to defend oneself against them; the month has passed – and there are new surprises: CVE-2021-44228, CVE-2021-45046, CVE-2021-4104, CVE-2021-45105, CVE-2021-44832 and their impacts. Konica Minolta and the vulnerabilities it discovered - CVE-2021-20868, CVE-2021-20869, CVE-2021-20870, CVE-2021-20871, CVE-2021-20872: how to defend oneself against them, and is it really necessary?; Brother, Canon, Lexmark, Ricoh, Xerox printing devices – vaccination does not provide the defense against viruses; Up-To-Date topic: is it necessary to develop new vaccines and be vaccinated?; passive and active defense methods and legislative limitations of their use; the audit of printing devices in Russian organizations in 2021: main results and conclusions; the stingy pays twice, the stupid pays thrice, the idiot the whole life; to protect one's health at least basic hygiene is necessary, or why one shouldn't turn the new MFP on and start printing right away.

- **"Zero Trust Model – Implementation Recommendations and Possible Issues"** (speaker – Stanislav Malinskiy, Russian University of Transport)

The report theses: The growth of crime rates during the COVID-19 pandemic; Zero Trust – is a safety model implying the total absence of trust towards any user, device or application; the main components of the zero trust architecture according to "NIST Special Publication 800-207: Zero Trust Architecture"; 7 principles of Zero Trust and the features of their implementation within the modern systems of automated workflow; minimal Zero Trust control requirements; recommendations on Zero Trust implementation; the issues related to practical implementation of Zero Trust:the requirements of Zero Trust towards the operational systems and input/output devices and their functions; software updates as a new source of vulnerabilities; OEM and non-OEM cartridges carry new threats; preventive protection measures; the necessity to continuously monitor the network; if a data-theft is inevitable, the cryptographyand the steganography may help; corrections of existing information safety policies are inevitable; the tendencies of the development of the Russian office printing market in the existing conditions.

This report received the Diploma as "The Best Scientific Report" on the All-Russia Science and Theory Conference "The Theory and Practice in Providing Informational Safety TPPIS-2021" in its section "Cryptographic Algorithms and Network Safety"

- **"Printers, MFPs and Cartridges – the Sources of Vulnerabilities; the Recommendation on Procurement, Usage and Disposal in 2022; the Responsibility of Suppliers and Users According to the Russian Legislation"** (speakers – Alexander Semenov, "Business-Inform" Legal Agency, Alina Savinova, Information Agency "Business-Inform")

The report theses:
Office printing and its managing: software-technical aspects; the "holes" in system and application software; patches and their role for hackers and information safety specialists; printers and MFPs as sources of vulnerabilities; the solutions from the manufacturers of printing devices, are they to be trusted; certificates on information safety of printing devices and how can they be related to the Russian market; firmware and its upgrades; what are the aims of manufacturers; remote

working places bringing new problems; cartridges (OEM, remanufactured, newly-built) and chips – one more group of information safety issues; what is chip doing: the statements of manufacturers and the opinion of information safety researchers; the spying devices and what is stated on the topic in criminal and administrative codes of the Russian Federation; the overview of court proceedings sings August 13, 2019; the responsibility of suppliers and the responsibility of users; the issues of disposal of printing devices and supplies from information safety specialists' perspective: the overview of wrong solutions and practical recommendations for 2022.

The participants of the Conference discussed together with the speakers the provided information, the results of the research on the vulnerabilities found in office printing devices in Russian and International organizations in 2021, as well as recommendations on their removal. A special attention of the Conference participants was paid towards the modern policies of data protection of corporate networks, as well as towards the issues related to the practice of workflow system usage (IT-outsourcing, MPS, the usage of remanufactured cartridges and newly-built cartridges). The participants of the Conference congratulated on of the speakers – Stanislav Malinskiy – with receiving the Diploma "The Best Scientific Report" on the All-Russia Science and Theory Conference "The Theory and Practice in Providing Informational Safety TPPIS-2021" in its section "Cryptographic Algorithms and Network Safety".

As a nice surprise for all the Conference participants came the new issue of BUSINESS-INFORM Review magazine (issue #33, 2021) and its appendix "Testing and Quality" (December, 2021).

AQCMS: **info@aqcmsrus.ru**, **https://aqcmsrus.ru/**
BUSINESS-INFORM: bizinform@list.ru, **http://sforp.ru/**