КОД ИБ ИТОГИ
МОСКВА 05 ДЕК'19

Что случилось с кибербезопасностью АСУ ТП?

Антон ШИПУЛИН
CISSP, CEH, CSSA
Kaspersky

Обо мне

kaspersky

Industrial Cybersecurity Center

RUSCADASEC

- Развитие бизнеса промышленной кибербезопасности в **Kaspersky**
- Руководитель программного комитета **Kaspersky Industrial Cybersecurity Conference**
- Координатор международного **Industrial Cybersecurity Center** (**CCI**)
- Сооснователь сообщества специалистов по кибербезопасности АСУ ТП / **RUSCADASEC**
- Certified SCADA Security Architect (**CSSA**), **CISSP**, **CEH**
- @shipulin_anton

Глобальная стандартизация **(O-PAS) v1.0**

Организация Open Process Automation Forum (OPAF) выпустила предварительную версию своего стандарта open process automation standard (O-PAS) v1.0, целью которого является унификация вендоронезависимой архитектуры промышленной автоматизации. Стандарт смогут использовать промышленные компании при работе с поставщиками систем автоматизации.

O-PAS Part 1 – Technical Architecture Overview
O-PAS Part 2 – Security (62443)
O-PAS Part 3 – Profiles
O-PAS Part 4 – Connectivity Framework (OCF)
O-PAS Part 5 – System Management

OPAF будет использовать систему сертификации ISASecure (на базе ISA/IEC 62443) для оценки безопасности прототипов компонент совместимых со стандартом O-PAS

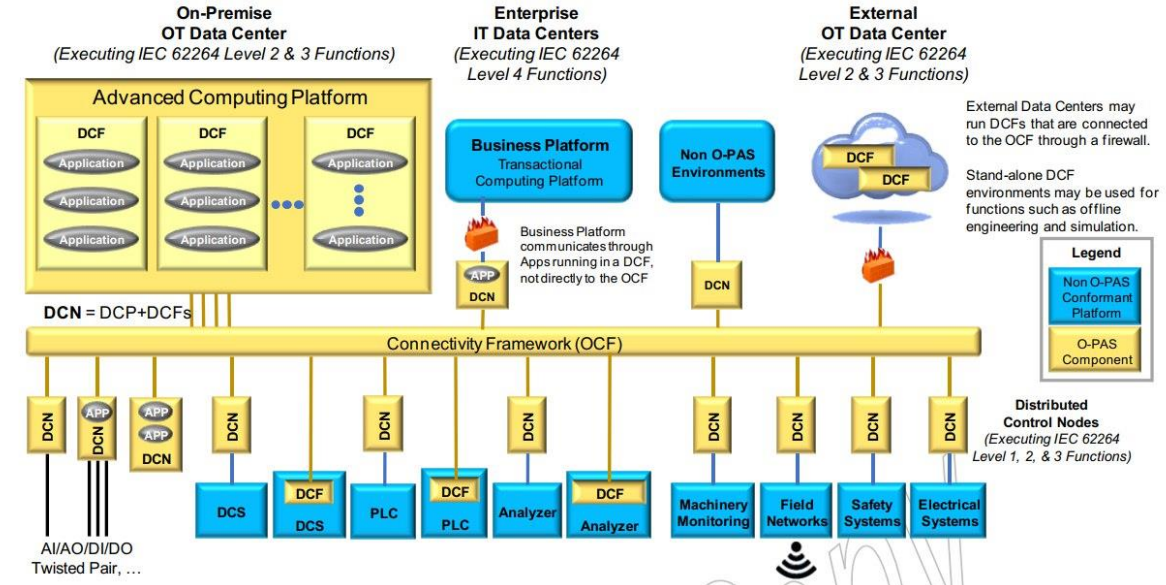


Figure 1: Concept Diagram of a Process Automation System of O-PAS Components

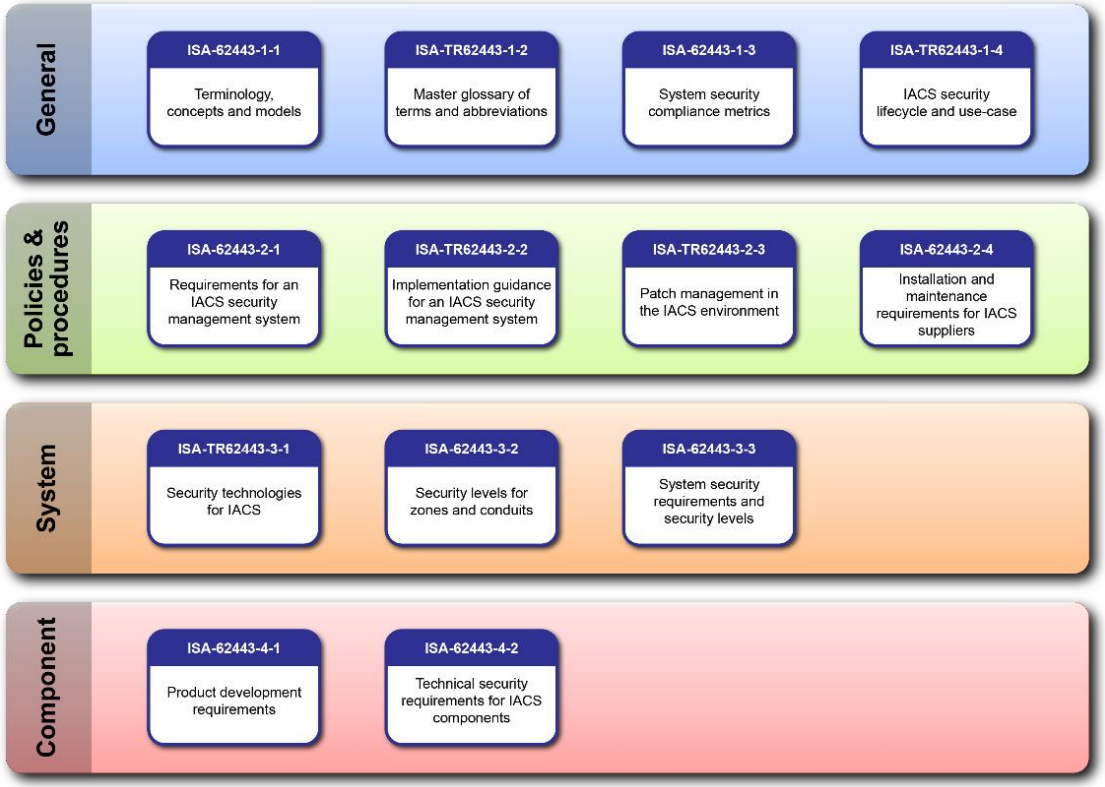
https://publications.opengroup.org/i190
https://www.isasecure.org/en-US/News-Events/OPAF-partners-with-ISA-to-use-ISASecure%C2%AE-specifica

IEC 62443 – Глобальный стандарт

UNECE / Европейская экономическая комиссия ООН (включает Россию) заявила о планах интегрировать серию стандартов по кибербезопасности промышленных систем ISA/IEC 62443 в Common Regulatory Framework on Cybersecurity (CRF), предназначенный для создания единого законодательного базиса по кибербезопасности внутри европейского союза

UNECE

ISA™



Альянсы промышленной кибербезопасности

Charter of Trust

https://new.siemens.com/global/en/company/topic-areas/cybersecurity.html

ISA GLOBAL CYBERSECURITY ALLIANCE

https://isaautomation.isa.org/cybersecurity-alliance/

OT CSA

https://otcsalliance.org/

SIEMENS

Schneider Electric

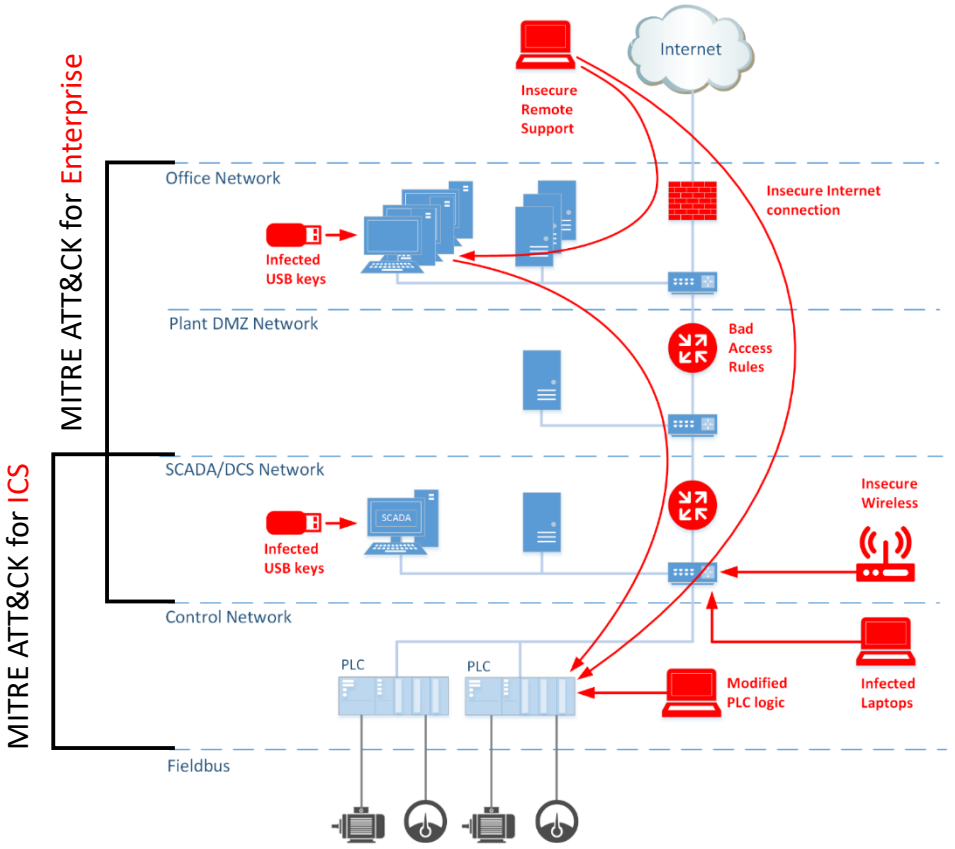
ABB

Rockwell Automation

Honeywell

MITRE ATT&CK

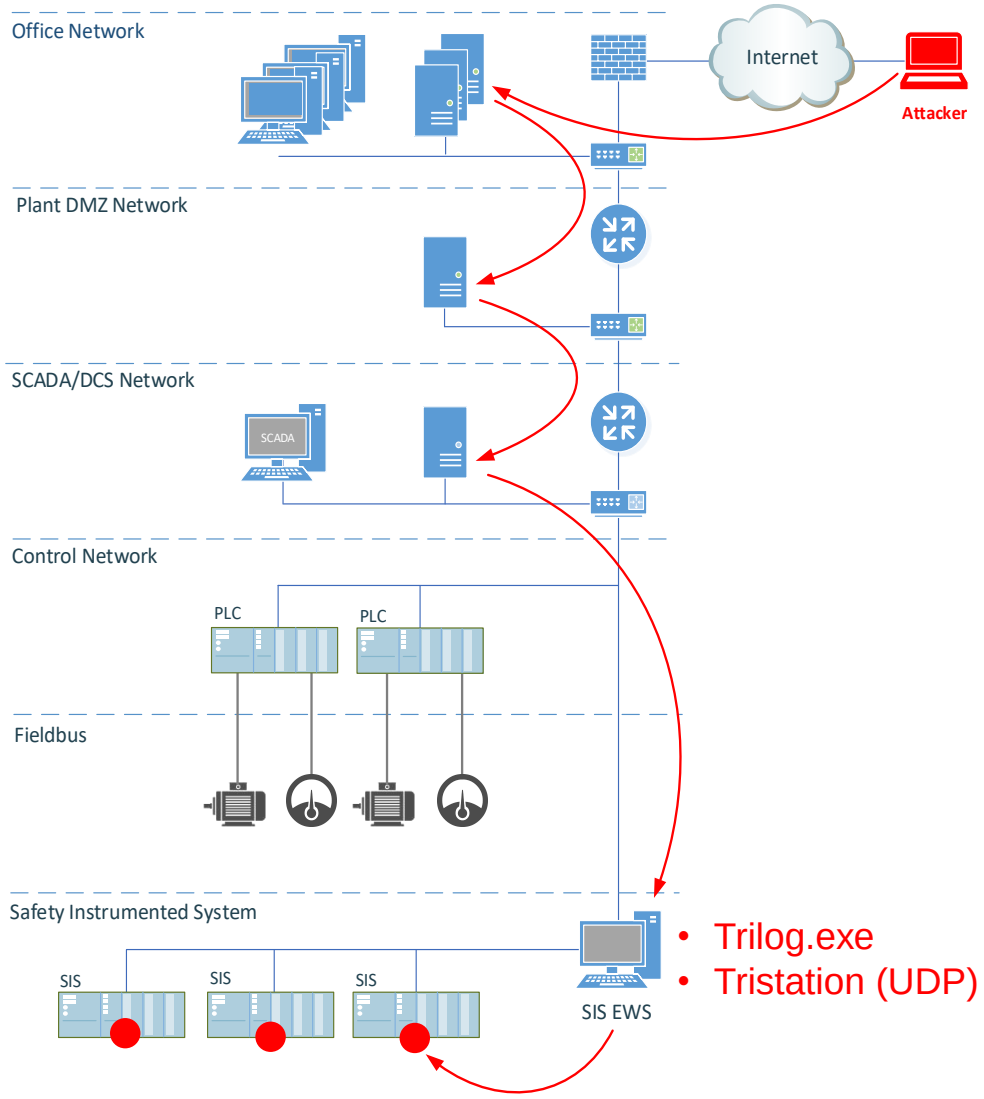
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery	Object Model	Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain		Pass the Ticket	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	Security Software Discovery	Replication Through Removable Media	Trap	Screen Capture	Exfiltration Over Other Network Medium	
Dylib Hijacking		Space after Filename	Bash History		Windows Admin Shares	Source	Data Staged		Communication Through Removable Media
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Connections Discovery	Remote Desktop Protocol	Launchctl	Input Capture	Exfiltration Over Alternative Protocol	
AppInit DLLs		HISTCONTROL	Account Manipulation		Pass the Hash	Space after Filename	Data from Network Shared Drive		Multilayer Encryption
Web Shell		Hidden Users	Replication Through Removable Media	System Owner/User Discovery	Exploitation of Vulnerability	Execution through Module Load		Data Transfer Size Limits	Standard Application Layer Protocol
Service Registry Permissions Weakness		Clear Command History	Input Capture	System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Data from Local System	Data Compressed	Commonly Used Port
Scheduled Task		Gatekeeper Bypass	Network Sniffing		Logon Scripts	InstallUtil	Data from Removable Media		Standard Cryptographic Protocol
New Service		Hidden Window	Credential Dumping	Application Window Discovery	Remote Services	Regsvr32			
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Brute Force		Application Deployment Software	Execution through API			Custom Cryptographic Protocol
Path Interception		Trusted Developer Utilities	Credentials in Files	Network Service Scanning	Remote File Copy	PowerShell			
Accessibility Features		Regsvcs/Regasm		Query Registry	Taint Shared Content	Rundll32			Data Obfuscation
Port Monitors		Exploitation of Vulnerability		Remote System Discovery		Scripting			Custom Command and Control Protocol
Screensaver		Extra Window Memory Injection		Permission Groups Discovery		Graphical User Interface			Connection Proxy
LSASS Driver		Access Token Manipulation				Command-Line Interface			Uncommonly Used Port
Browser Extensions		Bypass User Account Control		Process Discovery		Scheduled Task			Multiband Communication
Local Job Scheduling		Process Injection		System Service Discovery		Windows Management Instrumentation			Fallback Channels
Re-opened Applications		SID-History Injection				Trusted Developer Utilities			
Rc.common		Sudo				Service Execution			
Login Item		Setuid and Setgid							
LC_LOAD_DYLIB Addition									
Launch Agent									
Hidden Files and Directories									
.bash_profile and .bashrc									
Trap									
Launchctl									
Office Application Startup									
Create Account									
External Remote Services									
Authentication Package									
Netsh Helper DLL									
Component Object Model Hijacking									
Redundant Access									
Security Support Provider									
Windows Management Instrumentation Event Subscription									
Registry Run Keys / Start Folder									
Change Default File Association									
Component Firmware									
Bootkit									
Hypervisor									
Logon Scripts									
Modify Existing Service									
		Component Object Model Hijacking							
		InstallUtil							
		Regsvr32							
		Code Signing							
		Modify Registry							
		Component Firmware							
		Redundant Access							
		File Deletion							
		Timestomp							
		NTFS Extended Attributes							
		Process Hollowing							
		Disabling Security Tools							
		Rundll32							
		DLL Side-Loading							
		Indicator Removal on Host							
		Indicator Removal from Tools							
		Indicator Blocking							
		Software Packing							
		Masquerading							
		Obfuscated Files or Information							
		Binary Padding							
		Install Root Certificate							
		Network Share Connection Removal							
		Rootkit							
		Scripting							

https://www.youtube.com/watch?v=a9-p4tMsp14
https://www.youtube.com/watch?v=QU1ZR0c5x6A

Подробности поведения **Triton** в **Petro Rabigh**



TOOL	COMPONENTS	PURPOSE	ATTACK LIFECYCLE STAGE						
			Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
SecHack	KB77846376.exe	Credential harvesting			x	x			
	KB77846376.exe.x64								
NetExec	NetExec.exe	Remote command execution					x		
	runsvc.exe	NetExec runner							
Cryptcat-based backdoor	cryptcat.exe cryptsvc.exe svchostpla.exe	Backdoor		x					
	compattelprerunner.exe	C&C domain name generator							
	ProgramDataUpdater.xml	Scheduled task file (persistence mechanism)							
PLINK-based backdoor	napupdatedb.exe	Backdoor		x				x	
Bitvise-based backdoor	alg.exe userinit.exe csrss.exe	Backdoor					x	x	
	tquery.dll txflog.dll cryptopp.dll DEFAULT DEFAULT.BAK	Backdoor components							
OpenSSH-based backdoor	spl32.exe WinSAT.exe csrss.exe	Backdoor					x	x	
	clusapi.dll PolicMan.dll verifier2.dll misc.mof setup.ini	Backdoor components							
WebShell	logoff.aspx	Modified legitimate Outlook Web Access Component				x		x	
	flogon.js	Modified legitimate Outlook Web Access Component							
	ftpexts.tlb	Output file containing credentials harvested by logoff.aspx							

https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

Атаки шифровальщиков и майнеров

- **Norsk Hydro ASA,** норвежская нефтегазовая и металлургическая компания
- **Pilz**, немецкий производитель систем промышленной автоматизации
- **Hoya**, японский производитель оптического оборудования
- **Nyrstar**, бельгийский горно-металлургический комбинат
- **ASCO**, бельгийский производитель авиационных деталей
- **Hexion**, американская химическая компания
- **Momentive**, американская химическая компания
- **Demant**, датский производитель слуховых аппаратов
- **Rheinmetal**, немецкий производитель военной техники
- **Aebi Schmidt**, европейская машиностроительная компания
- …

Атака **Norks Hydro**

Norsk Hydro ASA — норвежская нефтегазовая и металлургическая компания. 40 стран, 35000 человек

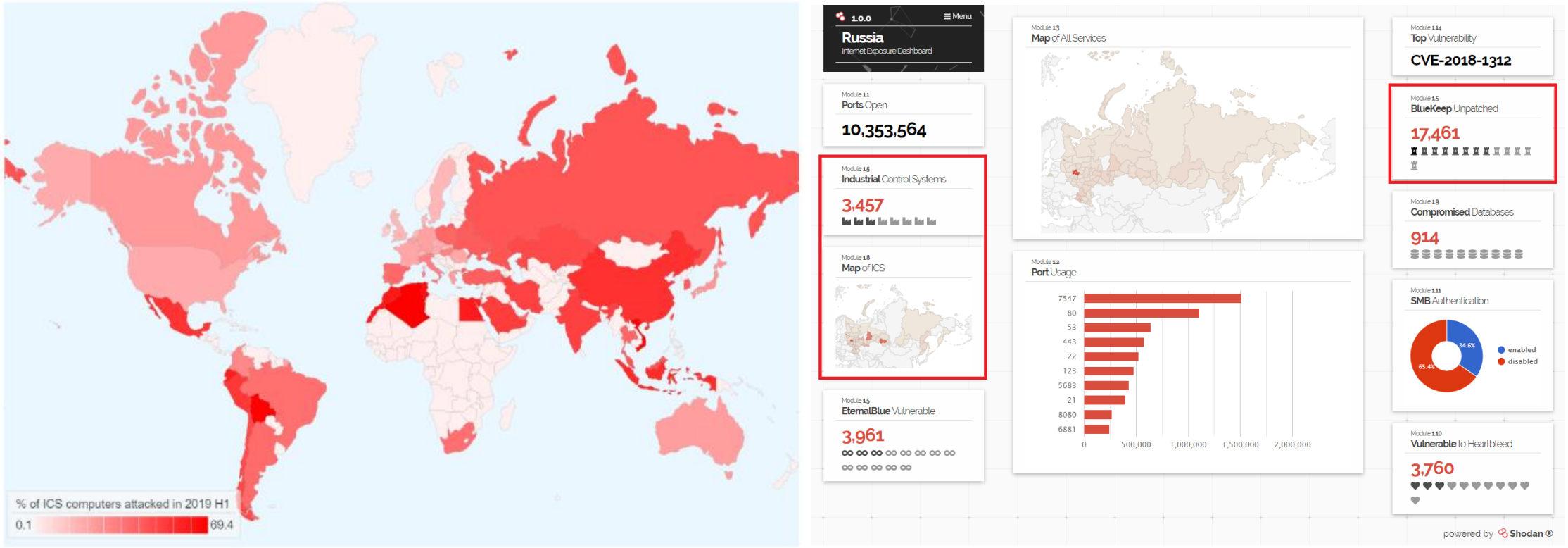
Март, 2019, Атака шифровальщика LockerGoga

Последствия:

- Заражено 11 000, зашифровано 2 700 ПК
- Заражено 1000, зашифровано 500 серверов
- Заводы переведены на ручное управление
- Ущерб: Q1: $40 млн, Q2: $30 млн

Страховое возмещение: $3,6 млн

Заражения ВПО в АСУ ТП



География атак на системы промышленной автоматизации, первое полугодие 2019*

** процент компьютеров АСУ, на которых были заблокированы вредоносные объекты*

https://exposure.shodan.io/#/RU

https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/

Политические заявления о кибератаках

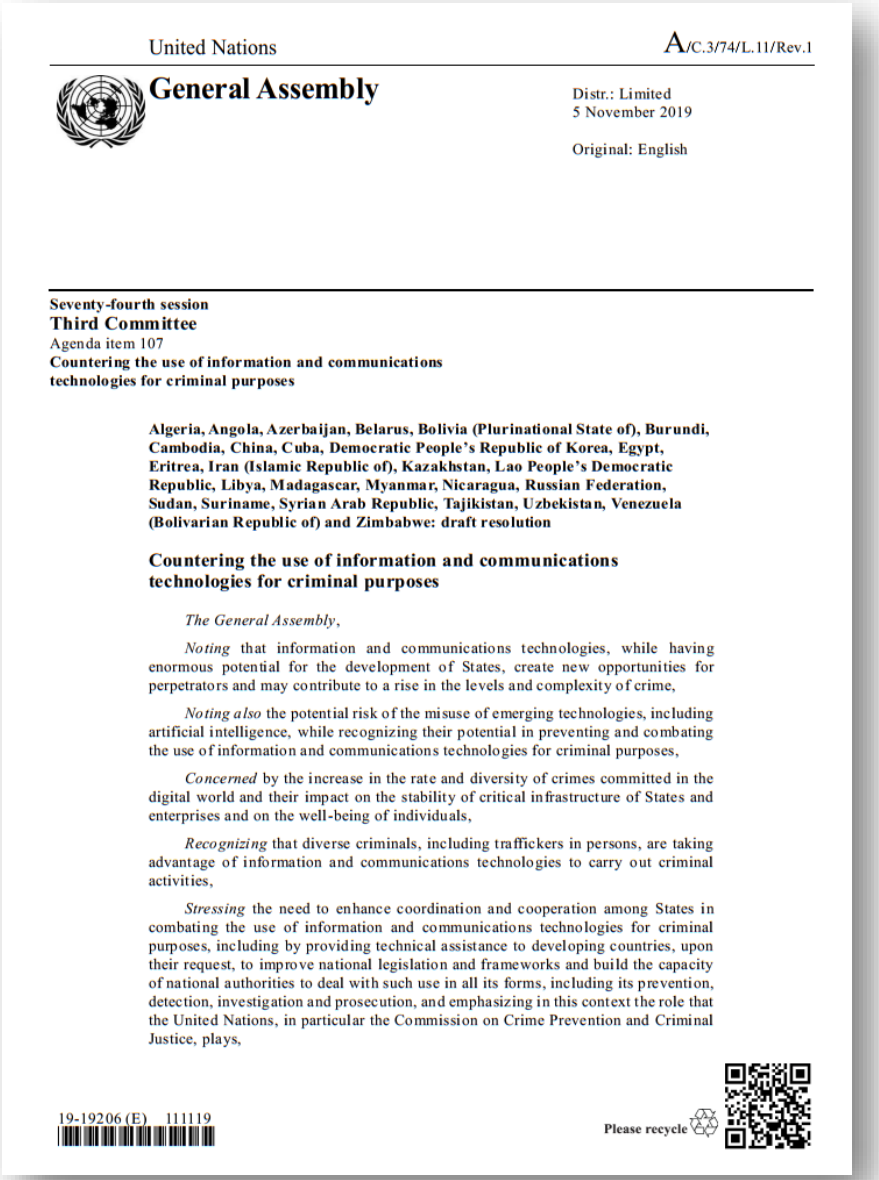



- Заявления США о готовности атаковать критическую инфрастукруту России (New York Times)
- Заявления США о Российских атаках на к критическую инфраструктуру США (DHS/CISA)
- Заявления Венесуэлы о кибератаках США на энергетику страны (США опровергает)
- Заявления США о кибератаках на системы управлением вооружением Ирана (Иран опровергает)
- …

Глобальное регулирование

Генассамблея ООН приняла резолюцию России по “Противодействию использованию информационно-коммуникационных технологий в преступных целях”

Целью является в том числе и решение вопросов с кибератаками с территории государств в том числе и направленных на критическую инфраструктуру



United Nations A/C.3/74/L.11/Rev.1

General Assembly

Distr.: Limited
5 November 2019

Original: English

Seventy-fourth session
Third Committee
Agenda item 107
Countering the use of information and communications technologies for criminal purposes

Algeria, Angola, Azerbaijan, Belarus, Bolivia (Plurinational State of), Burundi, Cambodia, China, Cuba, Democratic People's Republic of Korea, Egypt, Eritrea, Iran (Islamic Republic of), Kazakhstan, Lao People's Democratic Republic, Libya, Madagascar, Myanmar, Nicaragua, Russian Federation, Sudan, Suriname, Syrian Arab Republic, Tajikistan, Uzbekistan, Venezuela (Bolivarian Republic of) and Zimbabwe: draft resolution

Countering the use of information and communications technologies for criminal purposes

The General Assembly,

Noting that information and communications technologies, while having enormous potential for the development of States, create new opportunities for perpetrators and may contribute to a rise in the levels and complexity of crime,

Noting also the potential risk of the misuse of emerging technologies, including artificial intelligence, while recognizing their potential in preventing and combating the use of information and communications technologies for criminal purposes,

Concerned by the increase in the rate and diversity of crimes committed in the digital world and their impact on the stability of critical infrastructure of States and enterprises and on the well-being of individuals,

Recognizing that diverse criminals, including traffickers in persons, are taking advantage of information and communications technologies to carry out criminal activities,

Stressing the need to enhance coordination and cooperation among States in combating the use of information and communications technologies for criminal purposes, including by providing technical assistance to developing countries, upon their request, to improve national legislation and frameworks and build the capacity of national authorities to deal with such use in all its forms, including its prevention, detection, investigation and prosecution, and emphasizing in this context the role that the United Nations, in particular the Commission on Crime Prevention and Criminal Justice, plays,

19-19206 (E) 111119

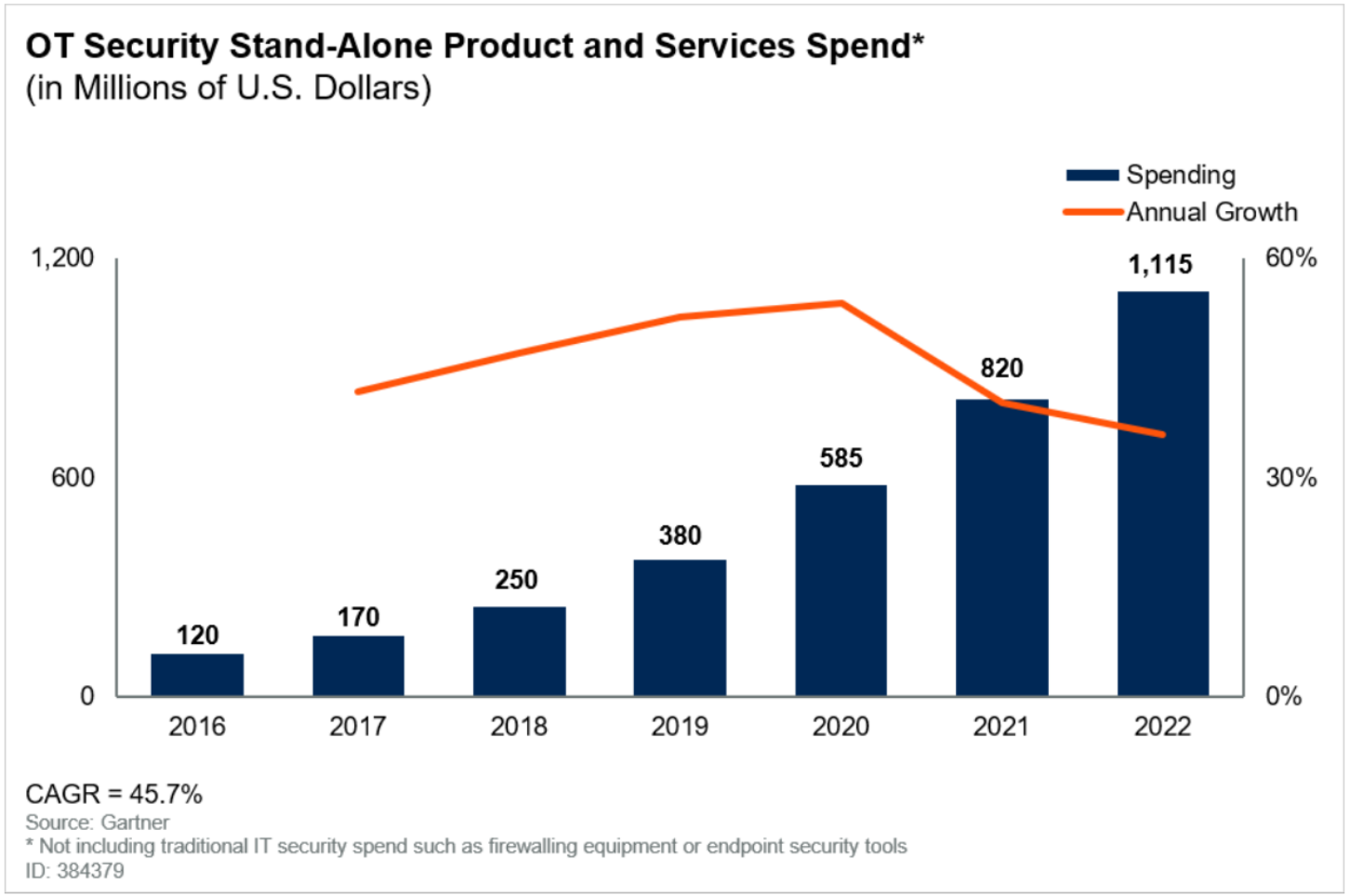
Please recycle

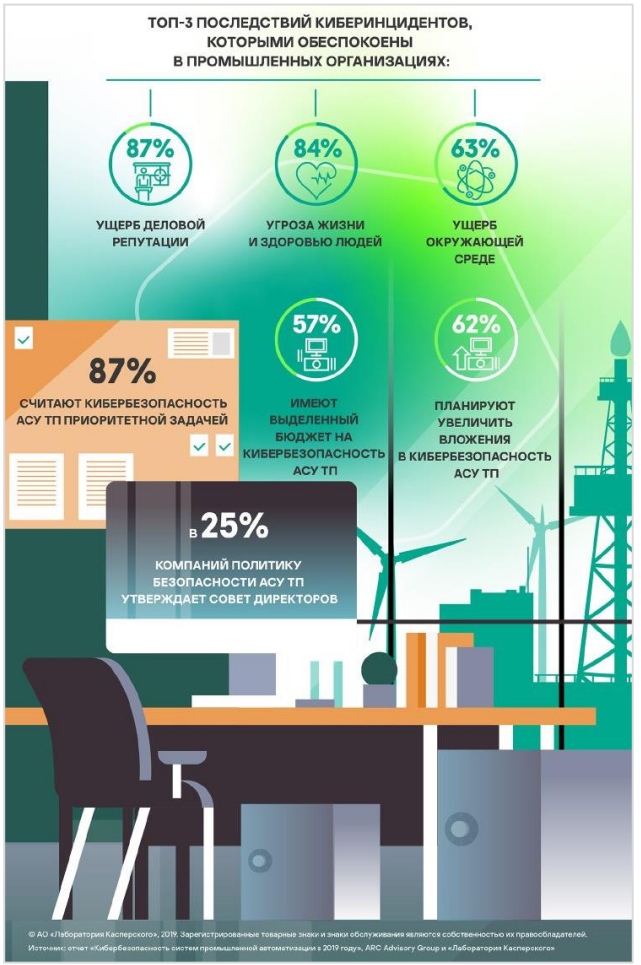
Масштабные ежегодные кибер учения

- NATO Cyber Coalition
- NATO CCDCOE Locked Shields
- NERC’s Grid Security Exercise (GridEx)
- SANS Cyber Situational Training Exercise (Cyber STX)
- Singapore (CISS) Critical Infrastructure Security Showdown
- The Standoff

Мировые расходы на кибербезопасность АСУ ТП

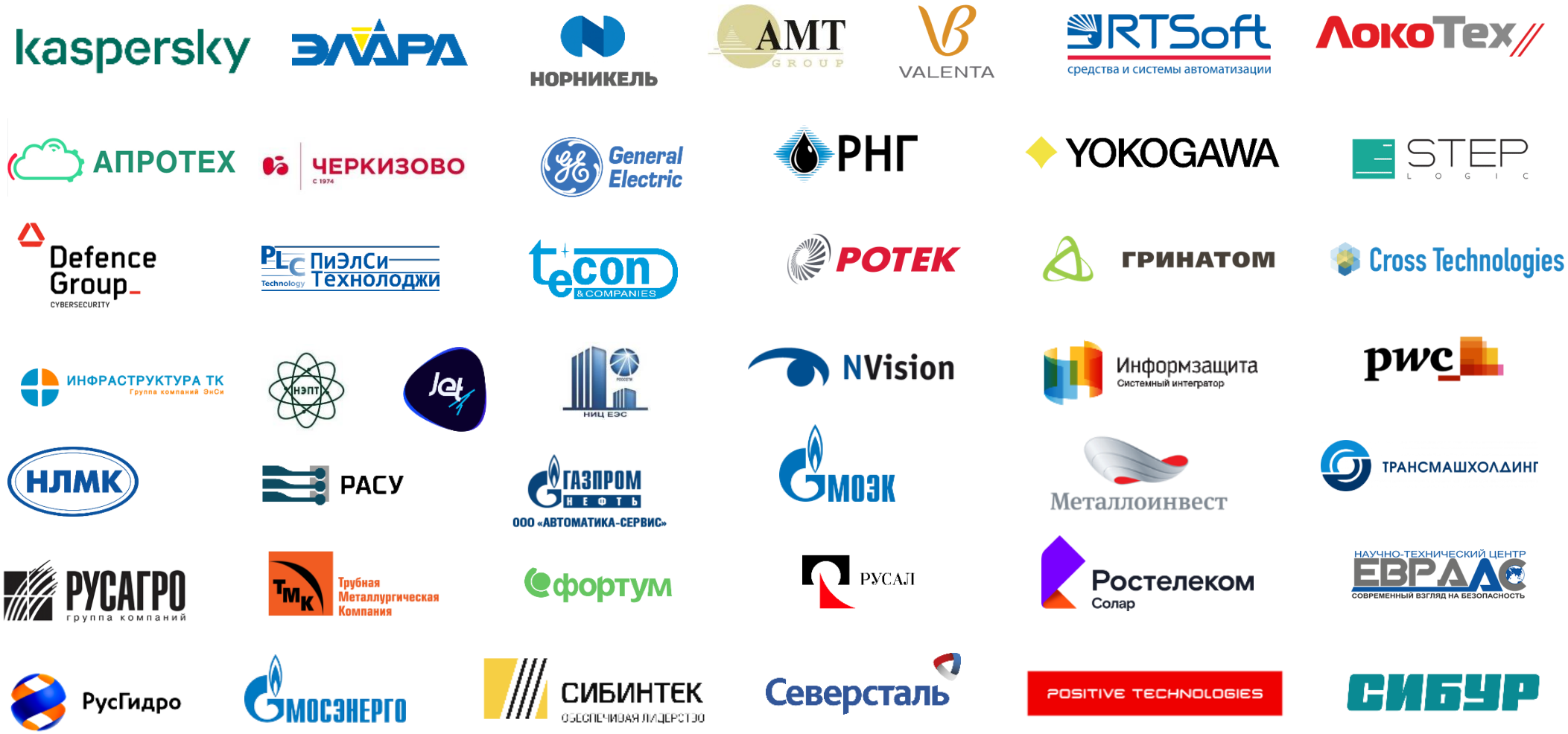
Figure 1. OT Security Stand-Alone Products and Services Spend (in Millions of U.S. Dollars)





https://www.gartner.com/en/documents/3956240 https://ics.kaspersky.ru/the-state-of-industrial-cybersecurity-2019/

Востребованность специалистов ИБ АСУ ТП в **2019**



https://t.me/RUSCADASEC

RUSCADASEC Con 2020

Практическая конференция профессионального сообщества специалистов по промышленной кибербезопасности

Апрель 2020, г. Москва

con.ruscadasec.ru

Организаторы

RUSCADASEC

АВАНГАРД медиа группа

kaspersky

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТОГИ

Спасибо!

Антон Шипулин

CISSP, CEH, CSSA

Менеджер по развитию решений по безопасности критической инфраструктуры

Kaspersky HQ

39A/3 Leningradskoe Shosse, Moscow

T: +7 (495) 797 8700 #1746

Anton.Shipulin@kaspersky.com

@shipulin_anton

ics.kaspersky.ru