



# Топ угроз ИБ в корпоративных сетях в 2019 году

Результаты анализа сетевого трафика  
в крупных компаниях в России и СНГ

Авезова Яна, аналитик

# Network Traffic Analysis



## NTA (Network Traffic Analysis) — системы анализа трафика:

- Анализируют трафик как на периметре, так и в инфраструктуре
- Выявляют атаки с помощью комбинации способов детекта
- Предоставляют информацию, необходимую для расследования инцидентов

**Многие клиенты Gartner** рассказали, что NTA инструменты выявили подозрительную активность в трафике, которую пропустили периметровые решения

Market Guide for Network Traffic Analysis, Gartner, 2019

**NTA входит в топ** технологий для выявления угроз, работой которых довольны в SOC

Common and Best Practices for Security Operations Centers:  
Results of the 2019 SOC Survey, SANS Institute 2019

# Об исследовании

РТ

**Как анализировали:** NTA-система  
PT Network Attack Discovery (PT NAD)

**Чей трафик:** 36 компаний со штатом  
>1000 чел.

**Когда анализировали:** 2019 год

**Цель:** выявить наиболее  
распространенные угрозы ИБ  
в корпоративных сетях



**31%**  
Госучреждения



**25%**  
Промышленность



**19%**  
ТЭК



**11%**  
Телекоммуникации



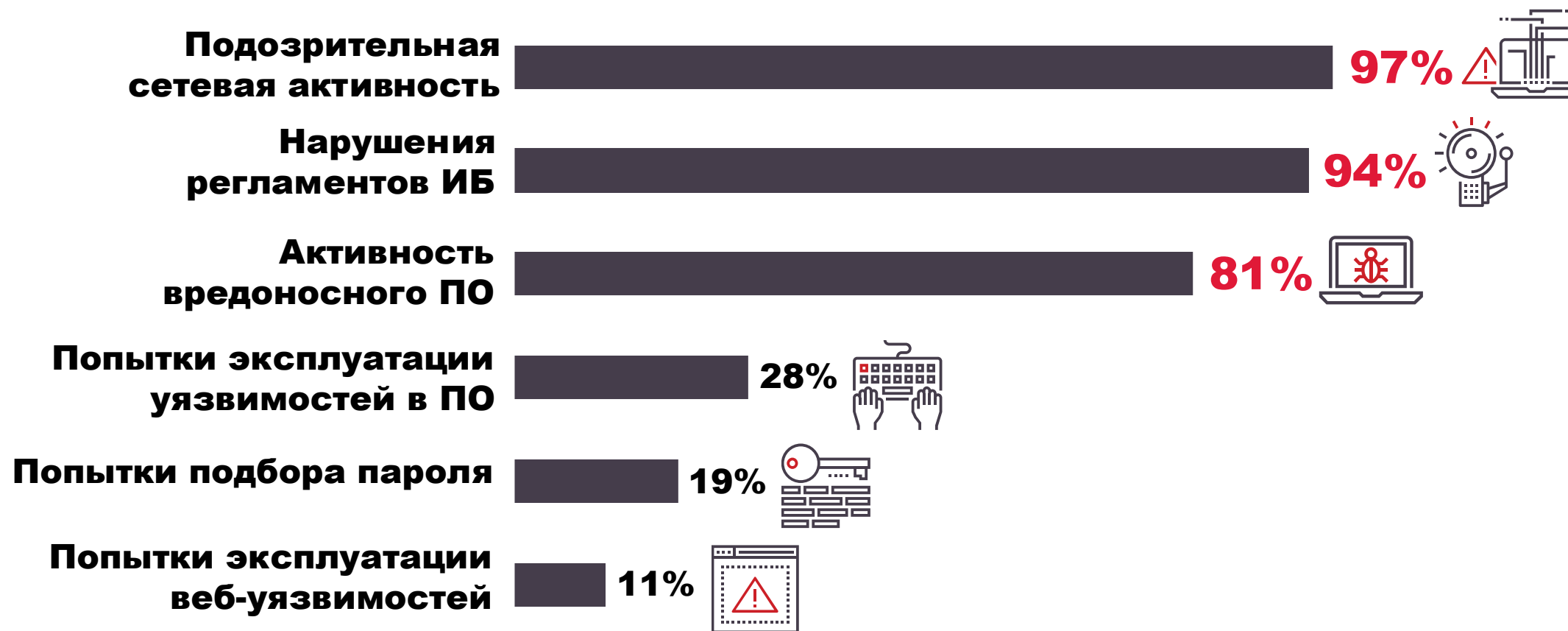
**8%**  
Финансовая  
отрасль



**6%**  
Другие

# Что удалось найти

РТ

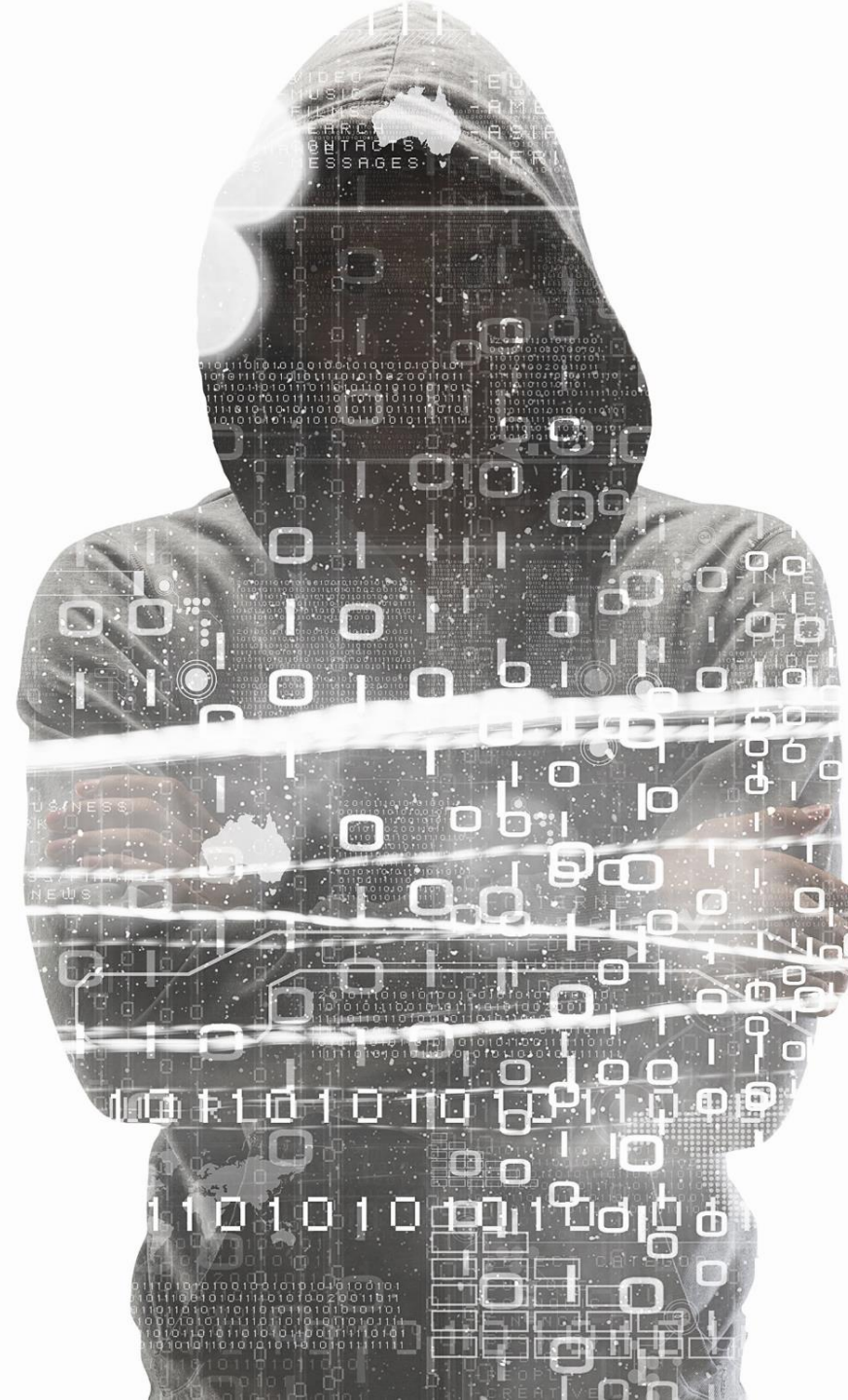


Категории выявленных угроз (доли компаний)



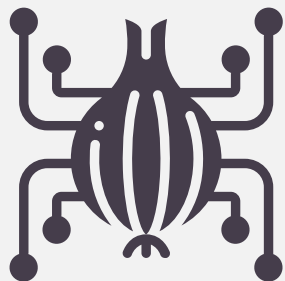
# Подозрительная сетевая активность

[ptsecurity.com](https://ptsecurity.com)



# Tor, proxy, VPN

PT



Tor, proxy, VPN

в **64%**  
компаний

+ Анонимность  
Шифрование

---

**Возможная  
компрометация**

Примеры ВПО:  
SystemBC, RTM, Ursnif

Вебинар «Как выявлять активность злоумышленников в зашифрованном трафике»:  
[ptsecurity.com/ru-ru/research/webinar/298091/](https://ptsecurity.com/ru-ru/research/webinar/298091/)

# Инструменты двойного назначения

PT



в **28%**  
компаний

выявлены инструменты,  
которые могут использоваться  
для проведения атак

Psexec, Net, Nmap, Kali Linux...

## Общие сведения

Протоко... [smb, tcp](#)

Начало 22 января 2019, 07:09:12

Конец 22 января 2019, 07:59:35

Длитель... 50 минут 22 секунды

Отправл... 15 кБ, 112 пакетов

Получено 14 кБ, 104 пакета

Отправи...

[Windows: 7 or 8](#)

Получат...

[Windows: 7 or 8](#)

## Атаки

[ET POLICY SMB2 NT Create AndX Request For an Executable File](#)

Potentially Bad Traffic

[ATTACK \[PTsecurity\] SMB2 Create PSEXESVC.EXE](#)

A Suspicious Filename was Detected

[ATTACK AD \[PTsecurity\] SMB ADMIN\\$ Share Access Denied](#)

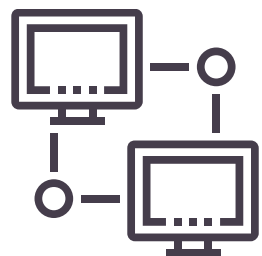
Attempted Administrator Privilege Gain

[Еще 11 атак](#) ▾

Неудачная попытка удаленного подключения для выполнения команд с помощью утилиты PsExec

# Что еще подозрительно

РТ



**39%**

Сканирования



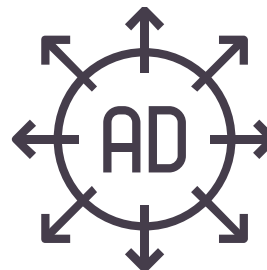
**19%**

Сбор информации об  
активных сессиях на узлах



**25%**

Попытки удаленного  
запуска процесса



**19%**

Сбор информации с  
контроллера домена

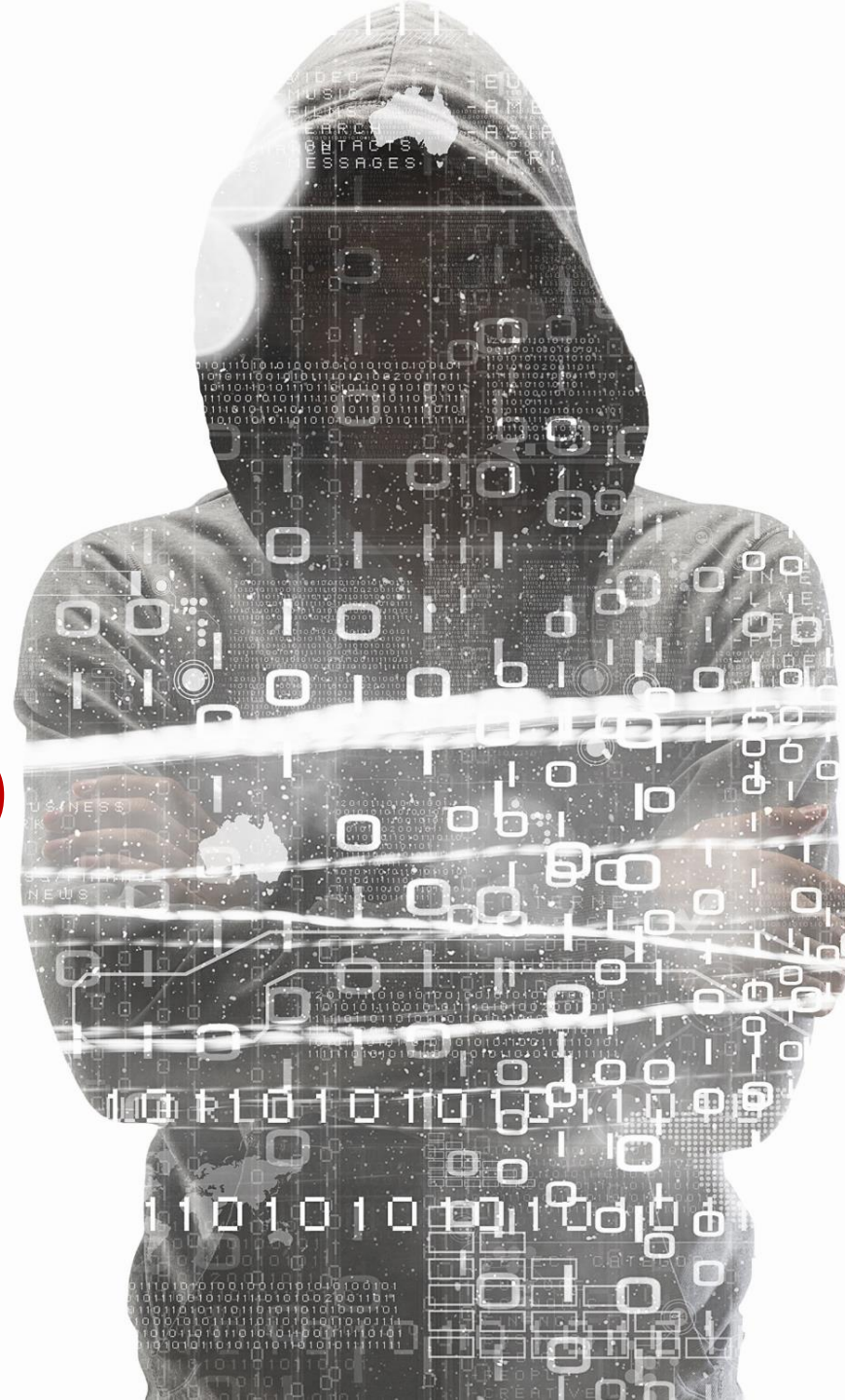
Указаны доли компаний





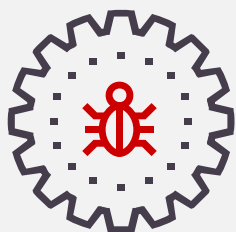
# Активность вредоносного ПО

ptsecurity.com



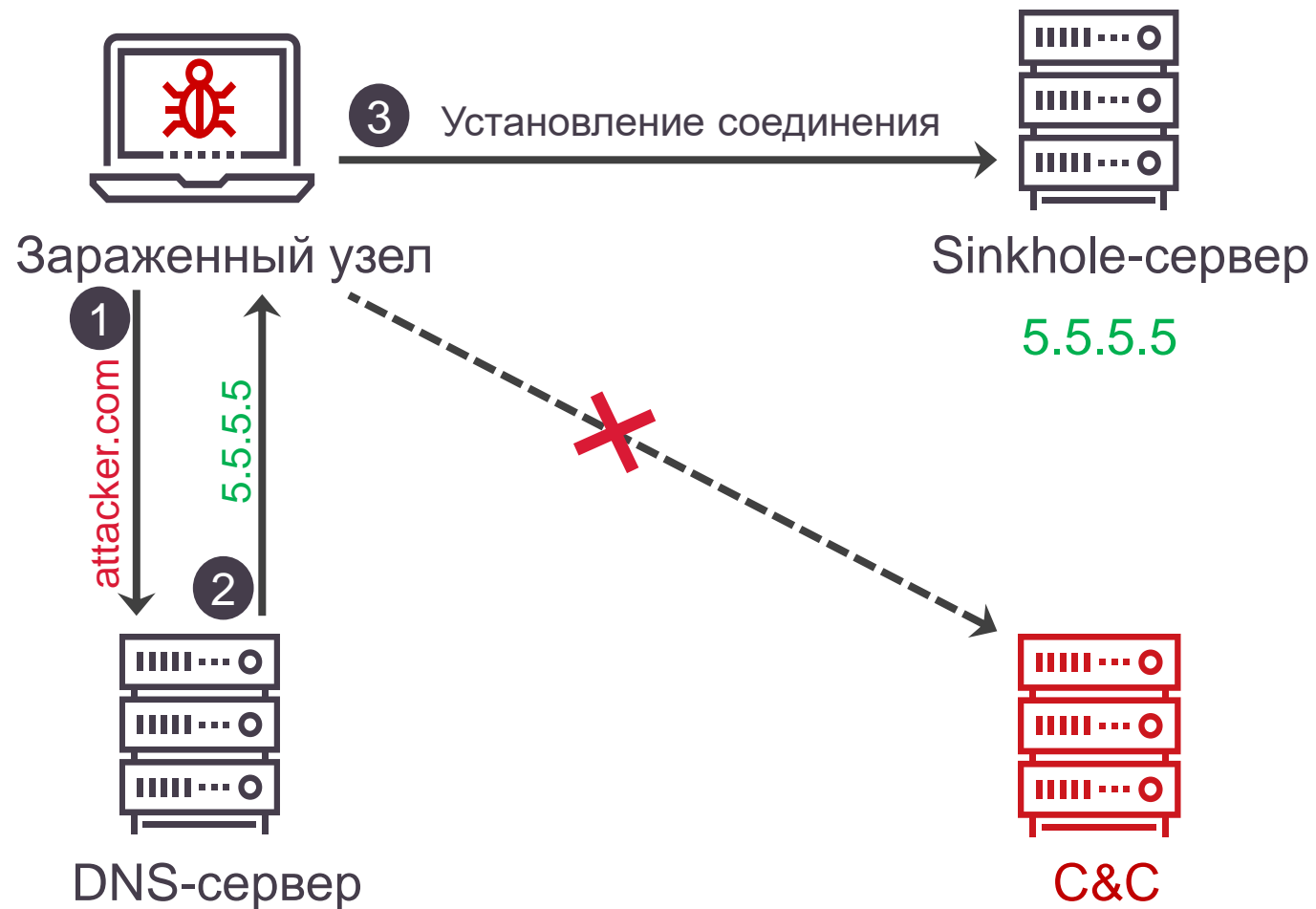
# Sinkhole

РТ

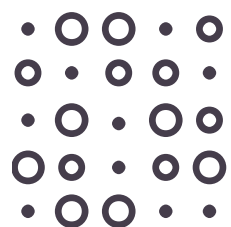


в **39%**  
компаний

выявлены попытки  
подключения к  
засинкхолованным доменам



# DGA-домены



Примеры ВПО:  
Sality, Zeus, Conficker

Доменные имена серверов по числу запросов	
Имя сервера	Количество запросов ▾
z5h64q92x9.net	105
ptitjnmfnjh.club	22
djchfgacdfaaadfdc.ru	19
d4knadd23t.ru	12
bce924fa02fa.ru	11
ghfgjehjbiehfbjaef.ru	10
w697oiiqsbmp.ru	3
0416.bkr13mxs.top	1
efbvrlg6dnjyllx.ru	1
lhvmt5et8vq0.ru	1
2wswg32trqa2.ru	1

DGA-домены

Обнаружение DGA-доменов: [habr.com/ru/company/pt/blog/282349/](http://habr.com/ru/company/pt/blog/282349/)

DGA — Domain generation algorithms

# Типы вредоносного ПО

РТ

**Майнеры** 55%

**Рекламное ПО** 28%

**Шпионское ПО** 24%

**Шифровальщик WannaCry** 21%

**Потенциально  
нежелательное ПО** 17%

В **47%** организаций

выявлено вредоносное  
ПО нескольких типов

Топ-5 вредоносного ПО (доли зараженных компаний)

# Как детектировать

PT

DNS-записи по числу запросов		
DNS-запись	Количе...	
zec.nanopool.org	4535	
dwarfpool.com	3656	
ypool.net	1896	
webminepool.com	8	
nanopool.org	6	

Запросы на майнинг-пулы

Атаки	
ADWARE [PTsecurity] Win32.Downloader (Sogou/Chindo)	
Misc activity	

Атаки	
MALWARE [PTsecurity] Win32/Spy.RTM.N	
A Network Trojan was Detected	

Срабатывания правил

DNS					
www.iuqerfsodp9ifjaposdfjhgosu... DGA	A	NOERROR	flags: RA, RD		
		Non-authoritative	www.iuqerfsodp9ifjaposdfjhgosuri...	CNAME	iuqerfsodp9ifjaposdfjhgosurijfaew... TTL: 11378
			iuqerfsodp9ifjaposdfjhgosurijfaew...	A	72.52.179.175 TTL: 11378

Killswitch-адреса WannaCry

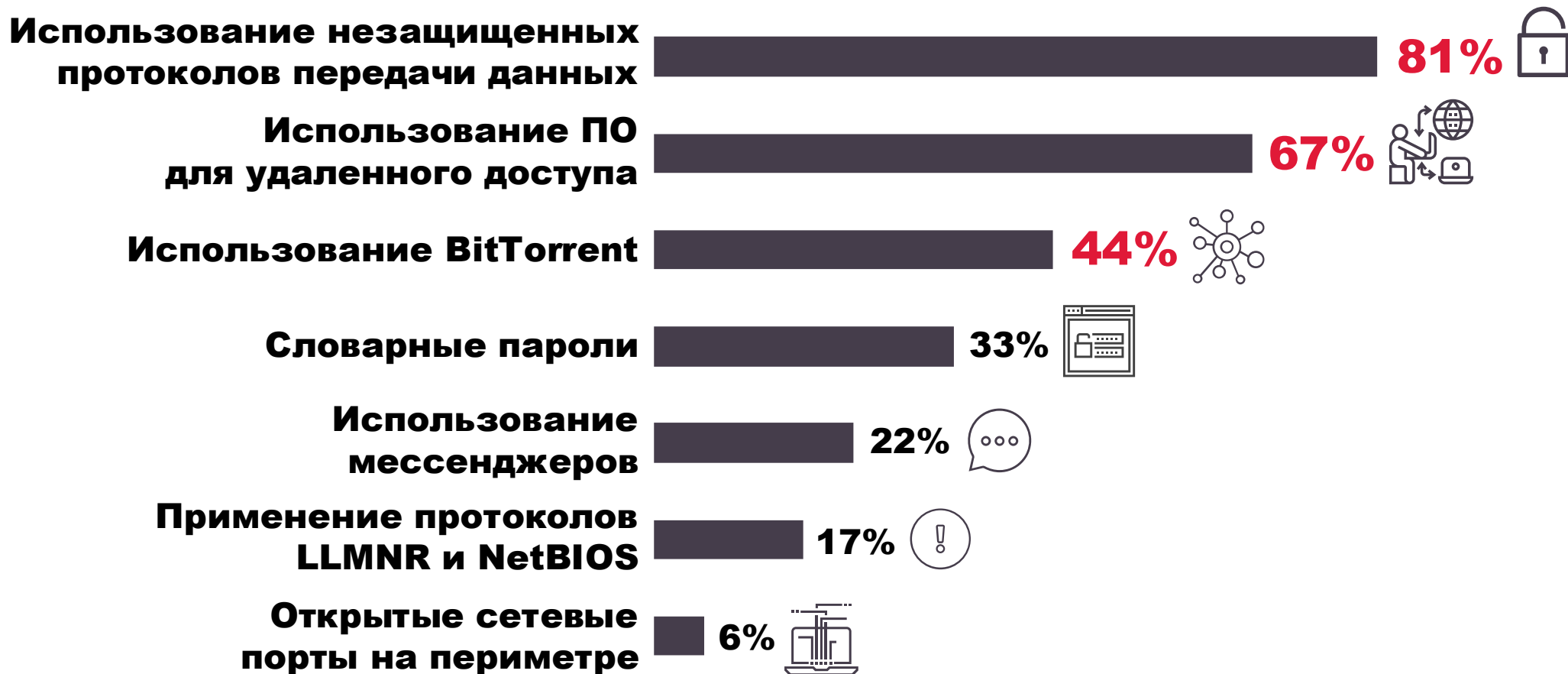


# Нарушения регламентов ИБ

[ptsecurity.com](https://ptsecurity.com)

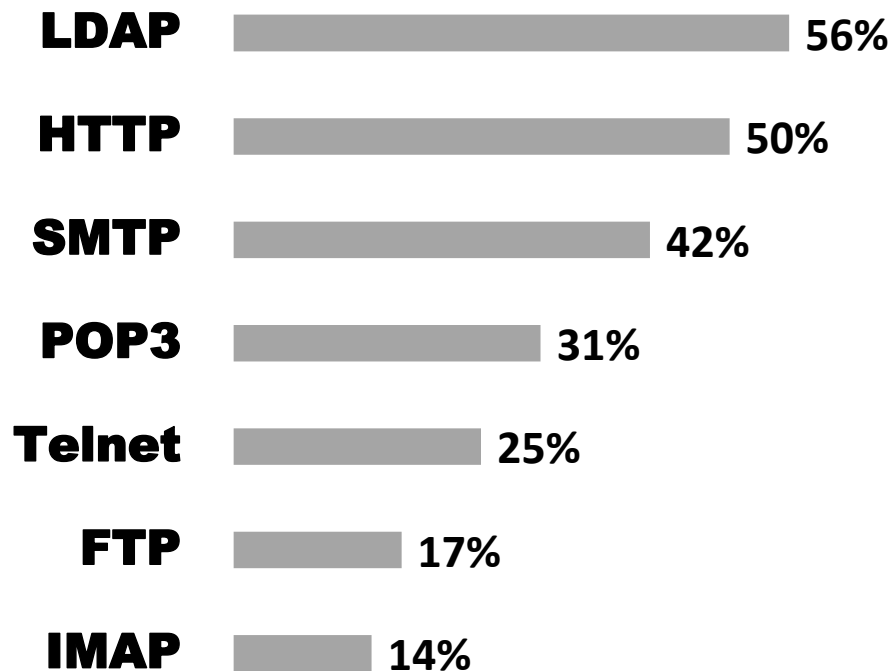
# Какие нарушения выявили

РТ



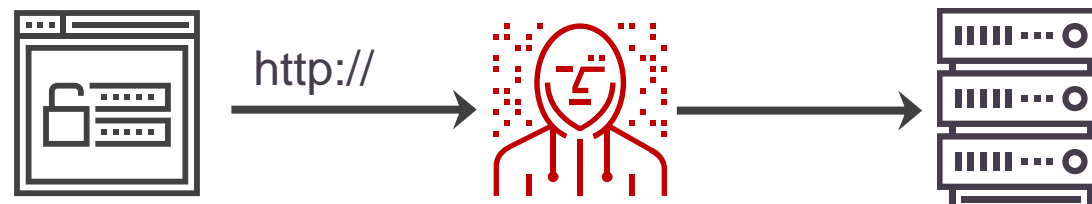
Топ-7 нарушений регламентов ИБ (доли компаний)

# Передача чувствительных данных в открытом виде



Использование незащищенных протоколов передачи данных (доли компаний)

```
request=&name=user&password=user&autologin=1&enter=Sign+inHTTP/1.1 302 Found  
Date: Sun, 10 Nov 2016 13:30:51 GMT  
Server: Apache/2.2.15 (CentOS)  
X-Powered-By: PHP/5.3.3
```



The screenshot shows the Zabbix web interface. The 'Scripts' tab is selected. The configuration for a script named 'positive' is displayed. The 'Type' is set to 'Script'. The 'Execute on' dropdown is set to 'Zabbix server (proxy)'. The 'Commands' field contains the command 'id;uname -a;/sbin/ifconfig -a'.



# Словарные пароли

РТ

Общие сведения

Протоколы [http, tcp](#)

Начало 13 июня 2019, 11:37:00

Конец 13 июня 2019, 11:37:00

Длительность 0 секунд

Отправлено 2 кБ, 12 пакетов

Получено 2 кБ, 12 пакетов

Отправитель

Получатель

Файлы

[services\\_state.cgi](#) 162 Б

↓ /admin/ajax/

Учетные записи

✓ admin 1234

HTTP

13.06.19 11:31:27	GET	/admin/ajax/services_state.cgi?...	0 Б	OK 200
----------------------	-----	------------------------------------	-----	-----------

Host

Accept-[en-US,en;q=0.5](#)

Language

Connection [keep-alive](#)

Authorization [Basic YWRtaW46MTIzNA==](#)

User-Agent [Mozilla/5.0 \(Windows NT 10.0; Win64; x64; rv:56.0\) Gecko/20100101 Firef](#)

HTTP Basic



в **33%**  
компаний

используют  
словарные пароли

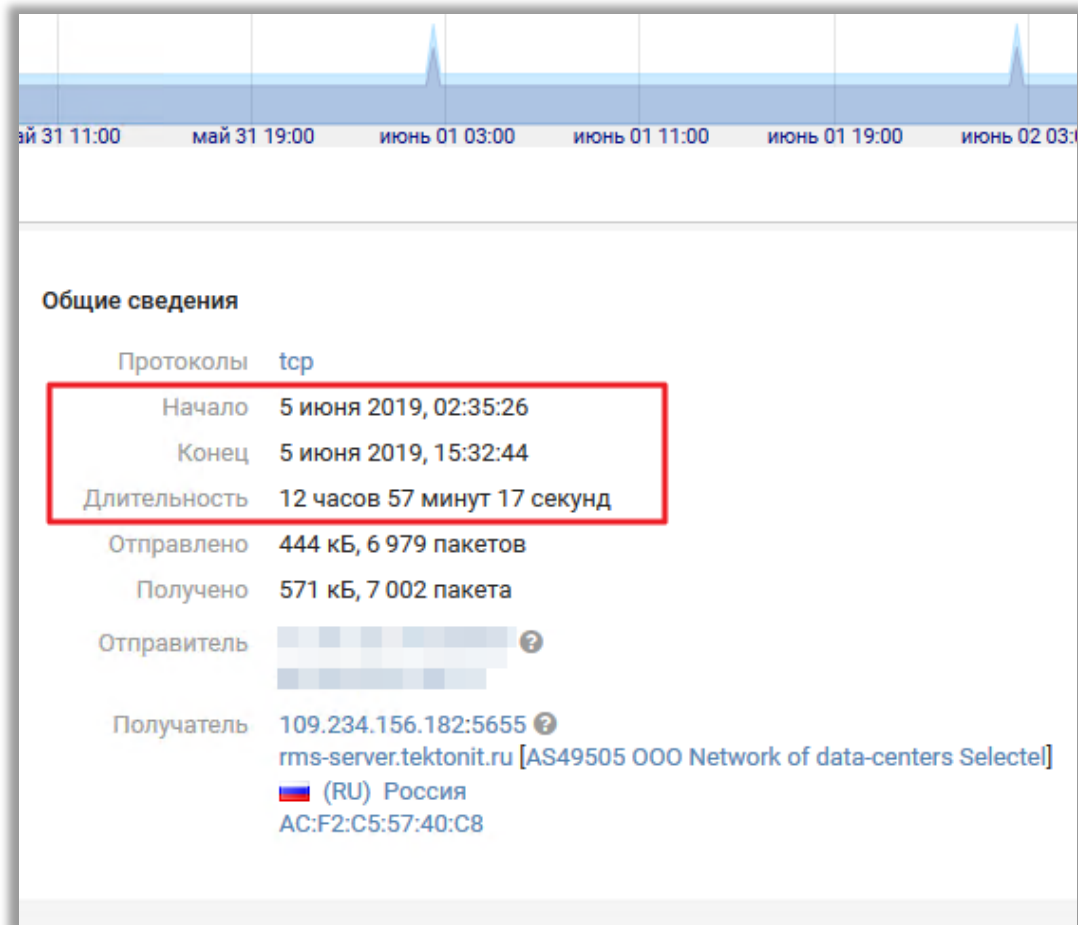
Пары "логин — пароль" по числу сессий

Логин	Пароль	Количество се...
admin	Password	14642
admin	admin	514
Bob	alice	393
Alice	bob	204
proxy	secret123!	129
tg	123qwerty	102
proxyuser	superpassword	74
tlouser	KWidiochsh8**6dewif	64

Виджет с учетными данными

# RAT: в чем риск

PT



Аномально длительное подключение по RMS

TeamViewer **58%**

RMS **14%**

Ammyy Admin **11%**

RAdmin **8%**

В **28%**  
организаций

используются  
несколько программ  
для удаленного доступа

## Атаки

- REMOTE [PTsecurity] Ammyy  
Potential Corporate Privacy Violation
- REMOTE [PTsecurity] FlawedAmmyy.RAT Checkin  
A Network Trojan was Detected

# Как защититься

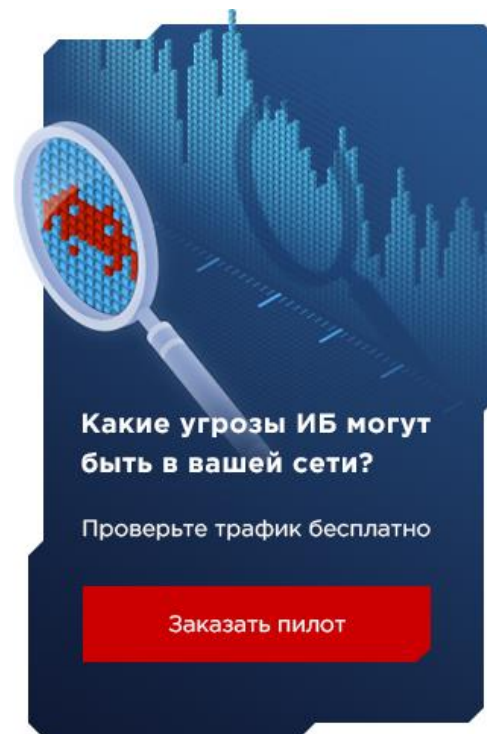
- Используйте защищенные протоколы: HTTPS, SLDAP, SFTP, FTPS, SSH.
- Настройте почтовые клиенты и серверы на использование TLS.
- Исключите словарные пароли и пароли по умолчанию.
- Разграничивайте права локальных пользователей.
- Настройте белые списки для ПО (в этом поможет AppLocker).
- Проводите глубокий анализ сетевого трафика, чтобы своевременно выявлять скрытые угрозы.

# Материалы по теме вебинара



**Полный текст исследования:**

[ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2020/](https://ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2020/)



**Проверить сеть компании бесплатно:**

[ptsecurity.com/ru-ru/products/network-attack-discovery/#free-demo](https://ptsecurity.com/ru-ru/products/network-attack-discovery/#free-demo)

Обсуждение темы  
анализа трафика,  
вопросы  
об исследовании  
и PT NAD

[t.me/PTNADChat](https://t.me/PTNADChat)

# Ещё больше интересных исследований



**Аналитика:** [ptsecurity.com/ru-ru/research/analytics/](https://ptsecurity.com/ru-ru/research/analytics/)

**Вебинары:** [ptsecurity.com/ru-ru/research/webinar/](https://ptsecurity.com/ru-ru/research/webinar/)

Про контроль сетевого комплаенса: [ptsecurity.com/ru-ru/research/webinar/298584/](https://ptsecurity.com/ru-ru/research/webinar/298584/)

Про выявление малварей в зашифрованном трафике: [ptsecurity.com/ru-ru/research/webinar/298091/](https://ptsecurity.com/ru-ru/research/webinar/298091/)

Про обнаружение атак на AD: [ptsecurity.com/ru-ru/research/webinar/290582/](https://ptsecurity.com/ru-ru/research/webinar/290582/)

Кейсы threat hunting с PT NAD: [ptsecurity.com/ru-ru/research/webinar/302112/](https://ptsecurity.com/ru-ru/research/webinar/302112/)

Кейс расследования атаки через дочку: [ptsecurity.com/ru-ru/research/webinar/303415/](https://ptsecurity.com/ru-ru/research/webinar/303415/)

**Блог:** [habr.com/ru/company/pt/blog/](https://habr.com/ru/company/pt/blog/)



**Спасибо**

**за внимание!**

[ptsecurity.com](http://ptsecurity.com)