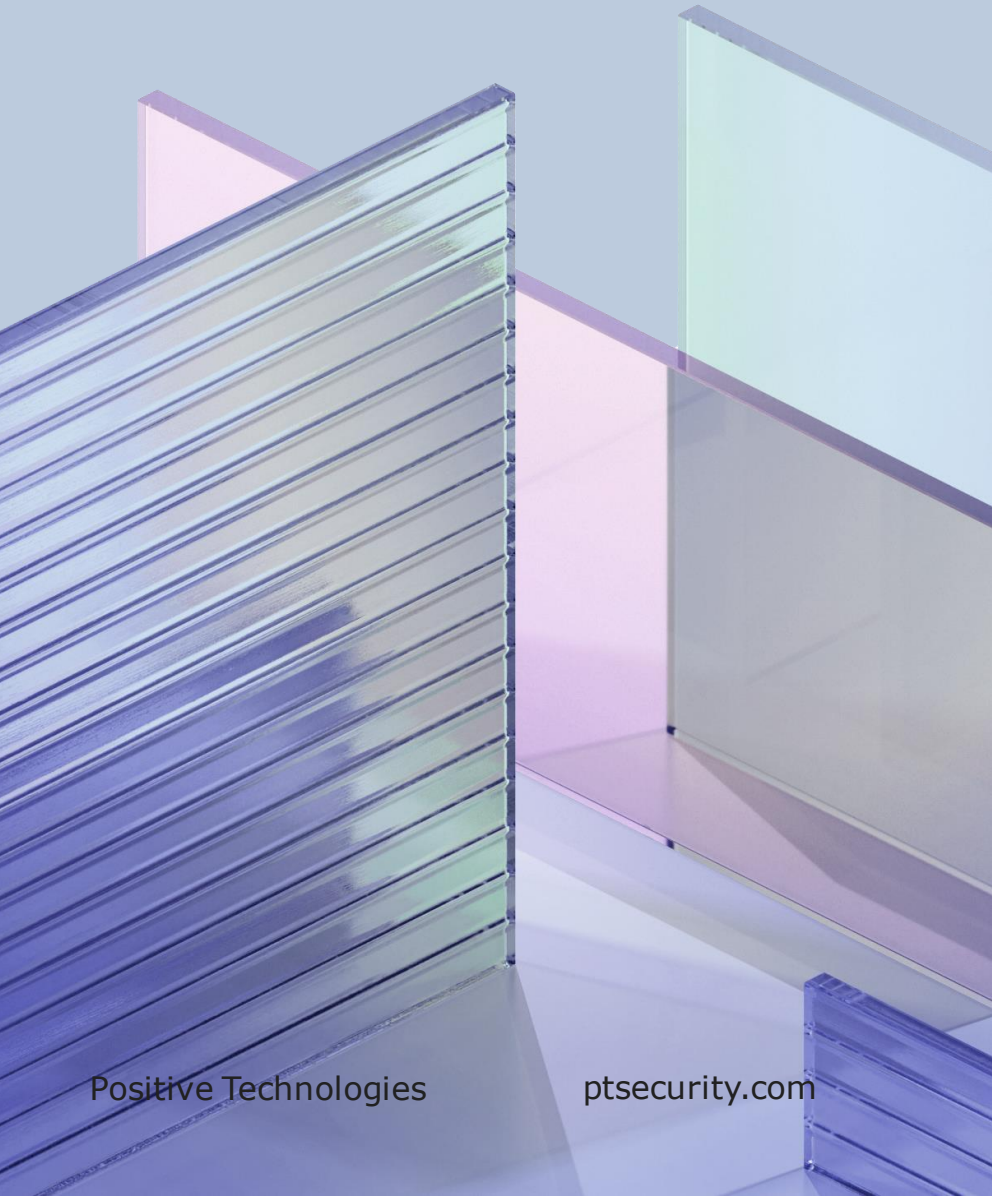
Как учесть рекомендации НКЦКИ в работе с уязвимостями

ptsecurity.com



Содержание

1. 

Зафиксированы случаи **внедрения недокументированных возможностей** в ПО иностранного производства

2. 

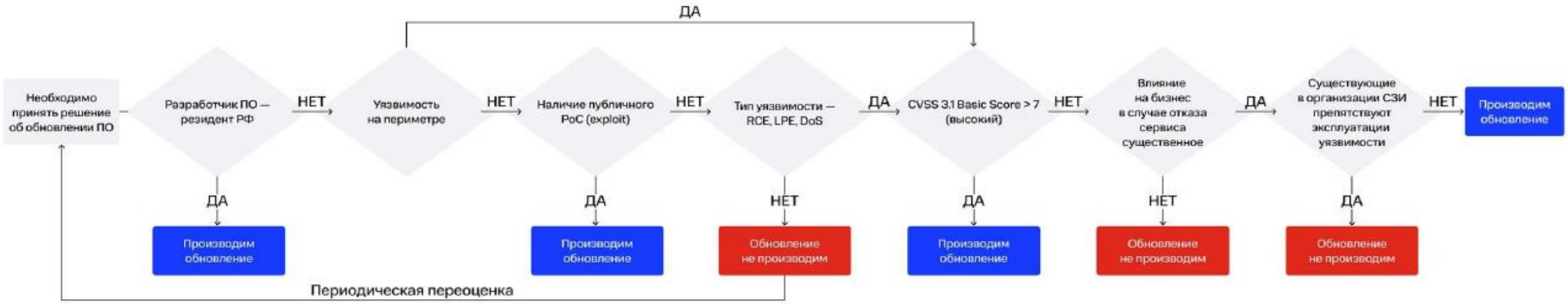
НКЦКИ рекомендует **отключить автоматическое обновление** иностранного ПО

3. 

В долгосрочной перспективе это приведет к тому, что **уязвимостей станет больше**, появится угроза **для бизнес-процессов**

4. 

НКЦКИ выпускает алгоритм по принятию решений об обновлении критически важного ПО



Скачать бюллетень: safe-surf.ru/upload/ALRT/ALRT-20220415.1.pdf

Как работать
с алгоритмом НКЦКИ

Когда не нужно устанавливать обновления

Ситуация № 1

- Разработчик ПО **не** резидент России
- Уязвимость **не** на периметре
- Публичный эксплойт **отсутствует**
- Тип уязвимости **не** RCE, LPE, DoS

Уязвимости

Группы активов

Фильтр активов

```
not (Host.IpAddress in 192.168.2.0/24)
```

Фильтр уязвимостей

```
Host.Softs.@Vulners and

(Host.Softs.Vendor not in ["Communigate Systems", "Crypto-Pro", "Doctor
Web", "Famatech", "Igor Pavlov", "InfoTeCS", "Kaspersky Lab", "Positive
Technologies", "QIP", "Ruby Team", "Veeam Software", "Yandex",
"CherryPy", "Dnsmasq", "EZB Systems", "Eclipse Foundation", "Go",
"Gpg4win", "ISC", "KeePass", "Lighttpd", "MariaDB Foundation", "Media
Player Classic", "Notepad++", "Nullsoft", "OpenSSH", "OpenSSL Project",
"OpenSSL Software Foundation", "OpenVPN", "PHP Group", "Pidgin",
"PostgreSQL", "PowerDns", "ProFTPD Project", "PuTTy", "Python Software
Foundation", "Realtek", "Redis", "Samba", "Sendmail", "Squid",
"SumatraPDF", "Telegram", "Tor Project", "TortoiseSVN", "Total
Commander", "TrueCrypt Foundation", "University Of Cambridge",
"VideoLAN", "WhatsApp", "WinPcap", "Wireshark", "XnView", "mod_ssl",
"vsFTPd"])

and (Host.Softs.@Vulners.Metrics.Exploitable = false)

and not (Host.Softs.@Vulners.Name like "%Remote Code Execution%" or
Host.Softs.@Vulners.Name like "%Удаленное%выполнение%" or
Host.Softs.@Vulners.Name like "%Повышение%привилеги%" or
Host.Softs.@Vulners.Name like "dos%" or Host.Softs.@Vulners.Name like
"%Отказ%в%обслуживании%")
```

Ctrl + Enter для проверки запроса

✔ 9398 уязвимостей соответствуют запросу

Уязвимость **не** на периметре

Разработчик ПО **не** резидент России

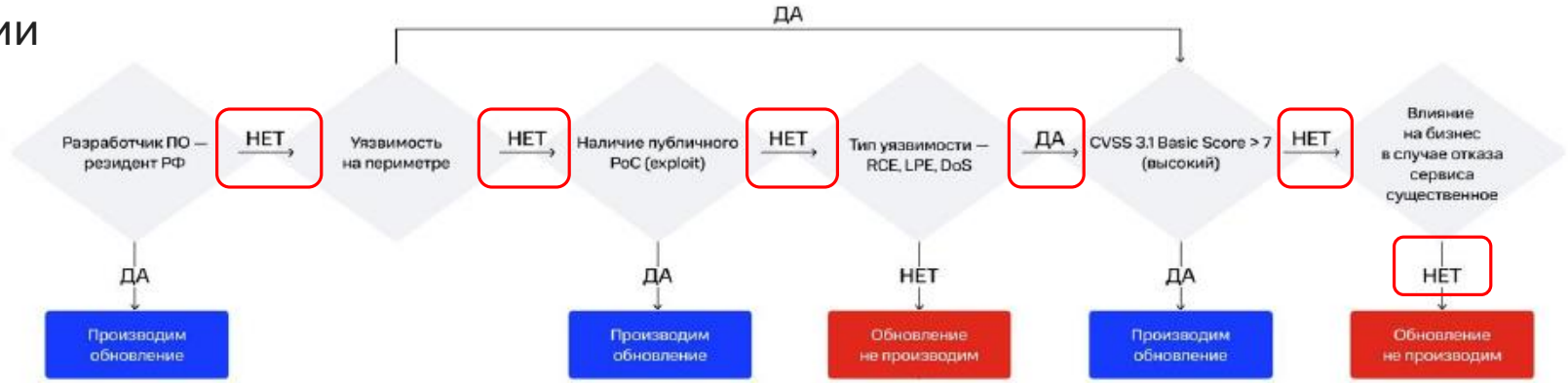
Публичный эксплойт **отсутствует**

Тип уязвимости **не** RCE, LPE, DoS

Когда не нужно устанавливать обновления

Ситуация № 2

- Разработчик ПО **не** резидент России
- Уязвимость **не** на периметре
- Публичный эксплойт **отсутствует**
- Тип уязвимости — RCE, LPE, DoS
- CVSS 3.1 ≤ 7
- **Не влияет** на важные бизнес-процессы компании



Уязвимости

Группы активов

Фильтр активов

```
not (Host.IpAddress in 192.168.2.0/24)
and (Host.@Importance != 'H')
```

Фильтр уязвимостей

```
Host.Softs.@Vulners and

(Host.Softs.Vendor not in ["Communigate Systems", "Crypto-Pro", "Doctor
Web", "Famatech", "Igor Pavlov", "InfoTeCS", "Kaspersky Lab", "Positive
Technologies", "QIP", "Ruby Team", "Veeam Software", "Yandex",
"CherryPy", "Dnsmasq", "EZB Systems", "Eclipse Foundation", "Go",
"Gpg4win", "ISC", "KeePass", "Lighttpd", "MariaDB Foundation", "Media
Player Classic", "Notepad++", "Nullsoft", "OpenSSH", "OpenSSL Project",
"OpenSSL Software Foundation", "OpenVPN", "PHP Group", "Pidgin",
"PostgreSQL", "PowerDns", "ProFTPD Project", "PuTTy", "Python Software
Foundation", "Realtek", "Redis", "Samba", "Sendmail", "Squid",
"SumatraPDF", "Telegram", "Tor Project", "TortoiseSVN", "Total
Commander", "TrueCrypt Foundation", "University Of Cambridge",
"VideoLAN", "WhatsApp", "WinPcap", "Wireshark", "XnView", "mod_ssl",
"vsFTPd"])

and (Host.Softs.@Vulners.Metrics.Exploitable = false)

and (Host.Softs.@Vulners.Name like "%Remote Code Execution%" or
Host.Softs.@Vulners.Name like "%Удаленное%выполнение%" or
Host.Softs.@Vulners.Name like "%Повышение%привилеги%" or
Host.Softs.@Vulners.Name like "dos%" or Host.Softs.@Vulners.Name like
"%Отказ%в%обслуживании%")

and (Host.Softs.@Vulners.CVSS3BaseScore <= 7)
```

Ctrl + Enter для проверки запроса

99 уязвимостей соответствуют запросу

Уязвимость **не** на периметре

Не на активах высокой значимости

Разработчик ПО **не** резидент России

Публичный эксплойт **отсутствует**

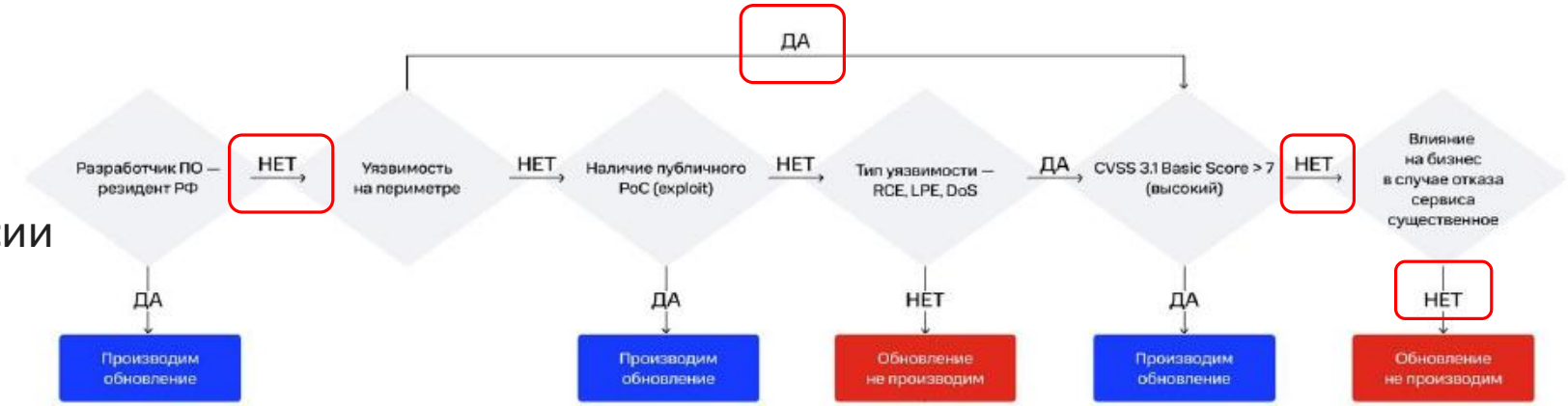
Тип уязвимости RCE, LPE, DoS

CVSS 3.1 ≤ 7

Когда не нужно устанавливать обновления

Ситуация № 3

- Разработчик ПО **не** резидент России
- Уязвимость **на** периметре
- CVSS 3.1 ≤ 7
- **Не влияет** на важные бизнес-процессы компании



Уязвимости

Группы активов

Фильтр активов

```
(Host.IpAddress in 192.168.2.0/24)
and (Host.@Importance != 'H')
```

Фильтр уязвимостей

```
Host.Softs.@Vulners and

(Host.Softs.Vendor not in ["Communigate Systems", "Crypto-Pro", "Doctor
Web", "Famatech", "Igor Pavlov", "InfoTeCS", "Kaspersky Lab", "Positive
Technologies", "QIP", "Ruby Team", "Veeam Software", "Yandex",
"CherryPy", "Dnsmasq", "EZB Systems", "Eclipse Foundation", "Go",
"Gpg4win", "ISC", "KeePass", "Lighttpd", "MariaDB Foundation", "Media
Player Classic", "Notepad++", "Nullsoft", "OpenSSH", "OpenSSL Project",
"OpenSSL Software Foundation", "OpenVPN", "PHP Group", "Pidgin",
"PostgreSQL", "PowerDns", "ProFTPD Project", "PuTTy", "Python Software
Foundation", "Realtek", "Redis", "Samba", "Sendmail", "Squid",
"SumatraPDF", "Telegram", "Tor Project", "TortoiseSVN", "Total
Commander", "TrueCrypt Foundation", "University Of Cambridge",
"VideoLAN", "WhatsApp", "WinPcap", "Wireshark", "XnView", "mod_ssl",
"vsFTPd"])

and (Host.Softs.@Vulners.CVSS3BaseScore <= 7)
```

Ctrl + Enter для проверки запроса

Ни одна уязвимость не соответствует запросу

Уязвимость **на** периметре

Не на активах высокой значимости

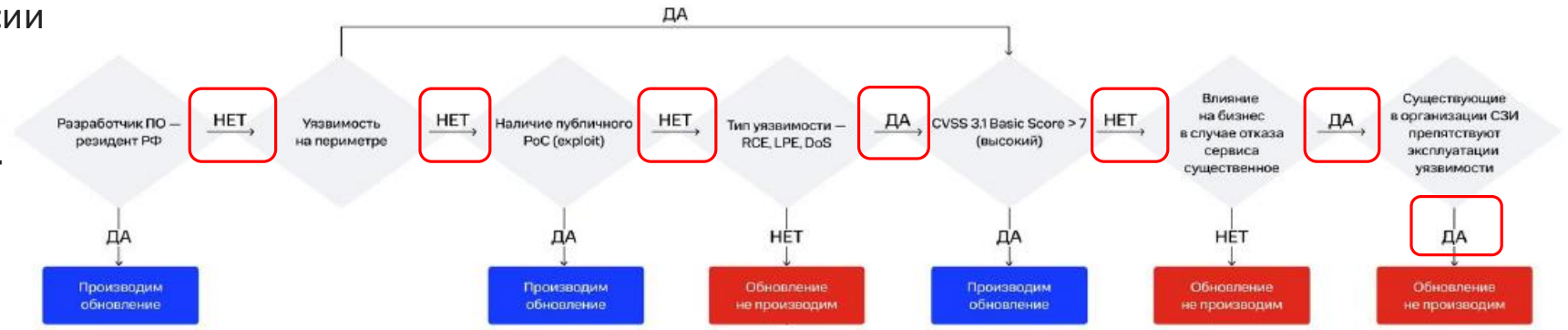
Разработчик ПО **не** резидент России

CVSS 3.1 ≤ 7

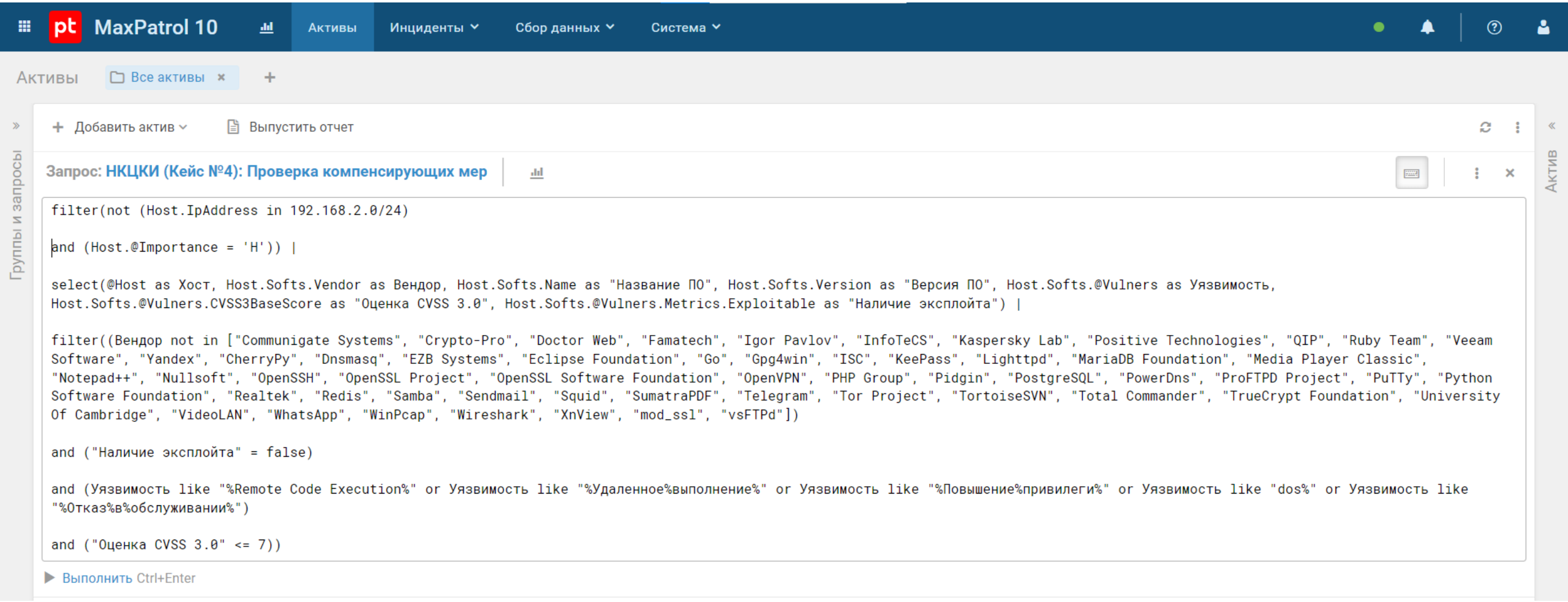
Когда не нужно устанавливать обновления

Ситуация № 4

- Разработчик ПО **не** резидент России
- Уязвимость **не** на периметре
- Публичный эксплойт **отсутствует**
- Тип уязвимости — RCE, LPE, DoS
- CVSS 3.1 ≤ 7
- **Влияет** на важные бизнес-процессы компании
- Эксплуатация невозможна благодаря сторонним средствам защиты информации (СЗИ) в компании



Как работать с алгоритмом НКЦКИ



↑ Собираем **фильтр** по первым шести критериям

Как работать с алгоритмом НКЦКИ

MaxPatrol 10 | Активы | Инциденты | Сбор данных | Система

Активы > Все активы

Добавить актив | Выпустить отчет

Запрос: НКЦКИ (Кейс №4): Проверка компенсирующих мер

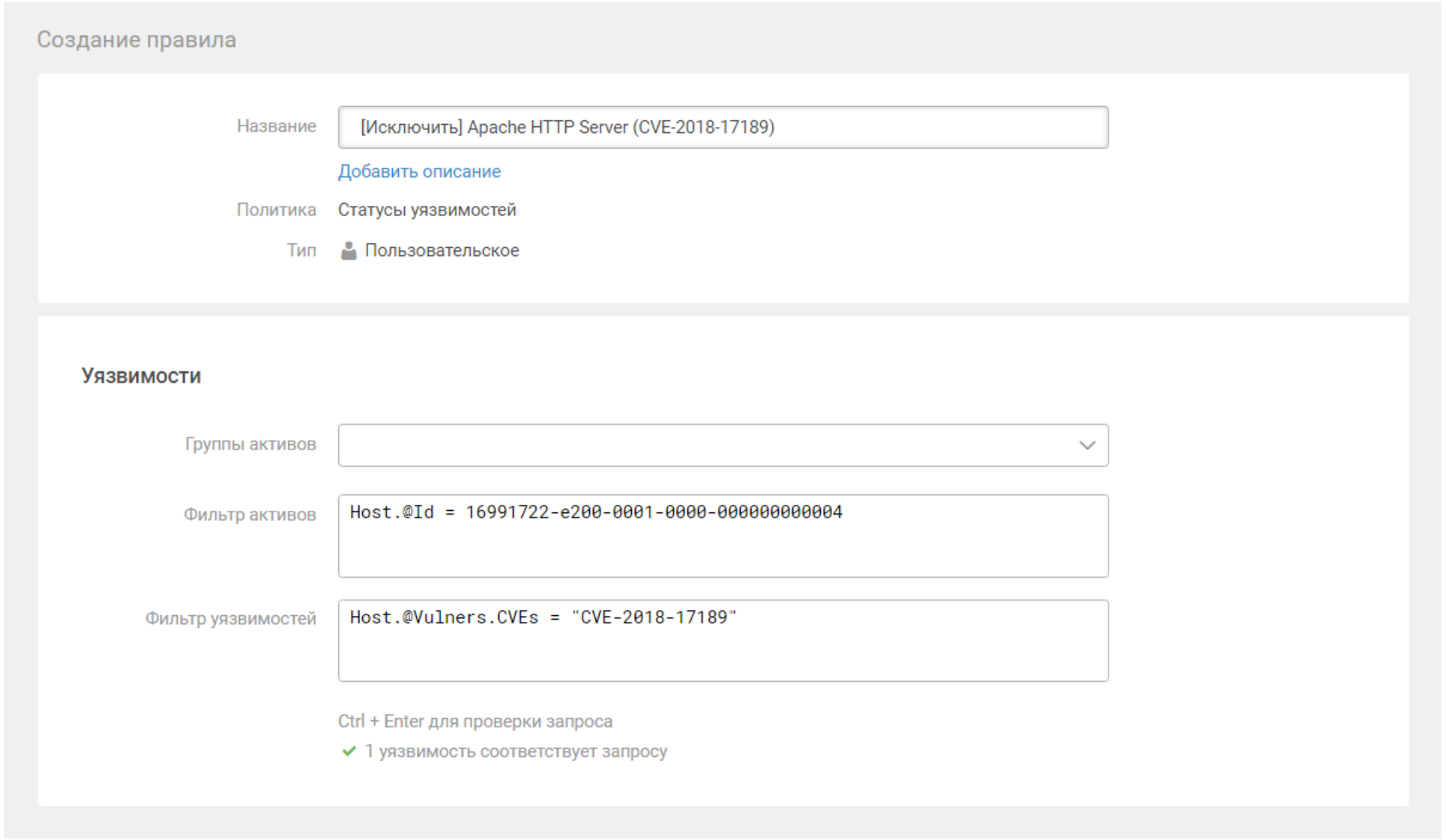
not (Host.IpAddress in 192.168.2.0/24… | @Host as Хост, Host.Softs.Vendor as B… | (Вендор not in ["Communigate Systems"… | Выполнить

Узел Хост	Производитель Вендор	Название Название ПО	Версия Версия ПО	Уязвимость Уязвимость	Базовая оценка уязвимости CVSS v3 Оценка CVSS 3.0	Эксплойт Наличие эксплойта
192.168.0.5	Apache Software Foundation	Apache HTTP Server	2.4.18	Отказ в обслуживании	5,3	False
192.168.0.5	Apache Software Foundation	Apache HTTP Server	2.4.18	Отказ в обслуживании	5,9	False
192.168.0.5	Apache Software Foundation	Apache HTTP Server	2.4.18	Отказ в обслуживании	5,9	False
srv2.company.com (192.168.0.6)	Microsoft	Microsoft .NET Framework	4.5.2	Повышение привилегий	5,5	False
srv2.company.com (192.168.0.6)	Microsoft	Microsoft .NET Framework	4.5.2	Отказ в обслуживании	5,5	False
srv2.company.com (192.168.0.6)	Microsoft	Microsoft .NET Framework	4.5.2	Повышение привилегий	5,5	False
srv2.company.com (192.168.0.6)	Microsoft	Microsoft .NET Framework	4.5.2	Отказ в обслуживании	5,5	False
srv2.company.com (192.168.0.6)	Microsoft	Microsoft .NET Framework	3.5.1	Отказ в обслуживании	5,5	False
srv2.company.com (192.168.0.6)	Microsoft	Microsoft .NET Framework	3.5.1	Отказ в обслуживании	5,5	False
srv2.company.com (192.168.0.6)	Microsoft	Microsoft Internet Explorer	11.0	Удаленное выполнение кода	6,4	False

↑ Выбираем, на каких узлах мы можем **применить компенсирующие меры** с помощью внедренных СЗИ

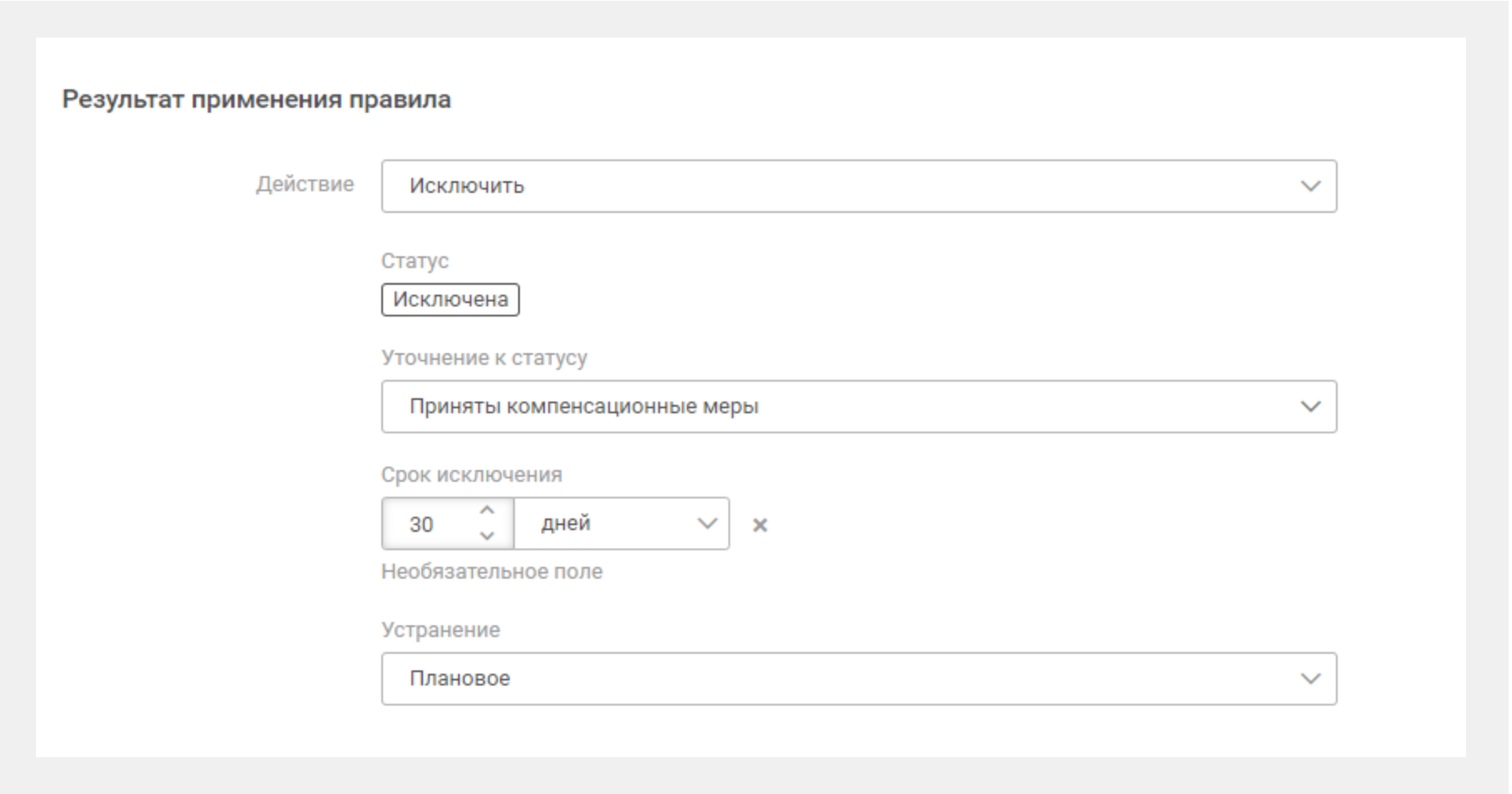
→

Создаем **правило исключения уязвимости** из процесса планового патч-менеджмента



→

Создаем **правило исключения уязвимости** из процесса планового патч-менеджмента



Как использовать алгоритм в MaxPatrol VM

Задаем фильтр в MaxPatrol VM

Разработчик ПО
не резидент России

Host.Softs.Vendor not in ["Communigate Systems", "Crypto-Pro", "Doctor Web", "Famatech", "Igor Pavlov", "InfoTeCS", "Kaspersky Lab", "Positive Technologies", "QIP", "Ruby Team", "Veeam Software", "Yandex", "CherryPy", "Dnsmasq", "EZB Systems", "Eclipse Foundation", "Go", "Gpg4win", "ISC", "KeePass", "Lighttpd", "MariaDB Foundation", "Media Player Classic", "Notepad++", "Nullsoft", "OpenSSH", "OpenSSL Project", "OpenSSL Software Foundation", "OpenVPN", "PHP Group", "Pidgin", "PostgreSQL", "PowerDns", "ProFTPD Project", "PuTTy", "Python Software Foundation", "Realtek", "Redis", "Samba", "Sendmail", "Squid", "SumatraPDF", "Telegram", "Tor Project", "TortoiseSVN", "Total Commander", "TrueCrypt Foundation", "University Of Cambridge", "VideoLAN", "WhatsApp", "WinPcap", "Wireshark", "XnView", "mod_ssl", "vsFTPd"]

Задаем фильтр в MaxPatrol VM

Host.IpAddress not in X.X.X.X/X

Уязвимость
не на периметре

Задаем фильтр в MaxPatrol VM

Host.Softs.@Vulners.Metrics.Exploitable = false

Публичный эксплойт
отсутствует

Задаем фильтр в MaxPatrol VM

Тип уязвимости
не RCE, LPE, DoS

```
not (Host.Softs.@Vulners.Name like "%Remote Code Execution%" or
Host.Softs.@Vulners.Name like "%Удаленное%выполнение%")
```

```
not (Host.Softs.@Vulners.Name like "%Повышение%привилеги%")
```

```
not (Host.Softs.@Vulners.Name like "dos%" or
Host.Softs.@Vulners.Name like "%Отказ%в%обслуживании%")
```

Задаем фильтр в MaxPatrol VM

Тип уязвимости — RCE, LPE, DoS

```
(Host.Softs.@Vulners.Name like "%Remote Code Execution%" or
Host.Softs.@Vulners.Name like "%Удаленное%выполнение%")
```

```
(Host.Softs.@Vulners.Name like "%Повышение%привилеги%")
```

```
(Host.Softs.@Vulners.Name like "dos%" or Host.Softs.@Vulners.Name
like "%Отказ%в%обслуживании%")
```

Задаем фильтр в MaxPatrol VM

Host.Softs.@Vulners.CVSS3BaseScore <= 7

CVSS 3.1 ≤ 7

Задаем фильтр в MaxPatrol VM

```
Host.@Importance != 'H'
```

Не влияет на важные бизнес-процессы компании
(**НЕ** на активах высокой значимости)

Задаем фильтр в MaxPatrol VM

Host.@Importance = 'H'

Влияет на важные бизнес-процессы компании (**на** активах высокой значимости)

Создание виджетов для отслеживания исключенных уязвимостей

Строим виджеты в MaxPatrol VM

Контроль **исключенных** уязвимостей

```
filter(not (Host.IpAddress in 192.168.2.0/24)) |

select(@Host as Хост, Host.Softs.Vendor as Вендор, Host.Softs.Name as "Название ПО", Host.Softs.Version as "Версия ПО",
Host.Softs.@Vulners as Уязвимость, Host.Softs.@Vulners.CVSS3BaseScore as "Оценка CVSS 3.0", Host.Softs.@Vulners.Metrics.Exploitable as
"Наличие эксплойта") |

filter((Вендор not in ["Communigate Systems", "Crypto-Pro", "Doctor Web", "Famatech", "Igor Pavlov", "InfoTeCS", "Kaspersky Lab", "Positive
Technologies", "QIP", "Ruby Team", "Veeam Software", "Yandex", "CherryPy", "Dnsmasq", "EZB Systems", "Eclipse Foundation", "Go",
"Gpg4win", "ISC", "KeePass", "Lighttpd", "MariaDB Foundation", "Media Player Classic", "Notepad++", "Nullsoft", "OpenSSH", "OpenSSL
Project", "OpenSSL Software Foundation", "OpenVPN", "PHP Group", "Pidgin", "PostgreSQL", "PowerDns", "ProFTPD Project", "PuTTy", "Python
Software Foundation", "Realtek", "Redis", "Samba", "Sendmail", "Squid", "SumatraPDF", "Telegram", "Tor Project", "TortoiseSVN", "Total
Commander", "TrueCrypt Foundation", "University Of Cambridge", "VideoLAN", "WhatsApp", "WinPcap", "Wireshark", "XnView", "mod_ssl",
"vsFTPd"])

and ("Наличие эксплойта" = false)

and not (Уязвимость like "%Remote Code Execution%" or Уязвимость like "%Удаленное%выполнение%" or Уязвимость like
"%Повышение%привилеги%" or Уязвимость like "dos%" or Уязвимость like "%Отказ%в%обслуживании%")) |

group("Название ПО", "Версия ПО", COUNT(*)) |

sort("COUNT(*)" DESC)
```

Группы и запросы

Актив

+ Добавить актив | Выпустить отчет

Запрос: НКЦКИ (Кейс №2)

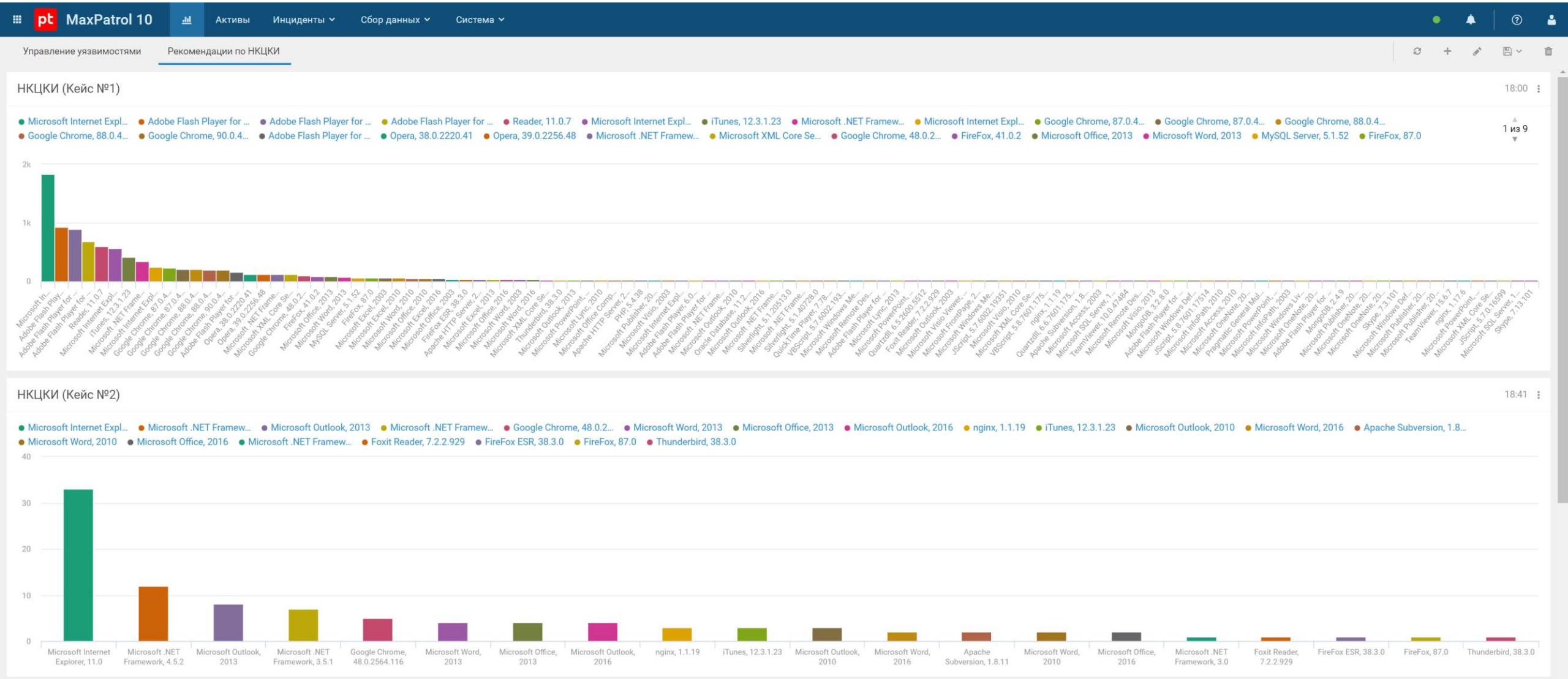
```
filter(not (Host.IpAddress in 192.168.2.0/24)

and (Host.@Importance != 'H')) |

select(@Host as Хост, Host.Softs.Vendor as Вендор, Host.Softs.Name as "Название ПО", Host.Softs.Version as "Версия ПО", Host.Softs.@Vulners as Уязвимость,
Host.Softs.@Vulners.CVSS3BaseScore as "Оценка CVSS 3.0", Host.Softs.@Vulners.Metrics.Exploitable as "Наличие эксплойта") |

filter((Вендор not in ["Communigate Systems", "Crypto-Pro", "Doctor Web", "Famatech", "Igor Pavlov", "InfoTeCS", "Kaspersky Lab", "Positive Technologies", "QIP", "Ruby Team", "Veeam
Software", "Yandex", "CherryPy", "Dnsmasq", "EZB Systems", "Eclipse Foundation", "Go", "Gpg4win", "ISC", "KeePass", "Lighttpd", "MariaDB Foundation", "Media Player Classic",
"Notepad++", "Nullsoft", "OpenSSH", "OpenSSL Project", "OpenSSL Software Foundation", "OpenVPN", "PHP Group", "Pidgin", "PostgreSQL", "PowerDns", "ProFTPD Project", "PuTTy", "Python
Software Foundation", "Realtek", "Redis", "Samba", "Sendmail", "Squid", "SumatraPDF", "Telegram", "Tor Project", "TortoiseSVN", "Total Commander", "TrueCrypt Foundation", "University
Of Cambridge", "VideoLAN", "WhatsApp", "WinPcap", "Wireshark", "XnView", "mod_ssl", "vsFTPd"])

and ("Наличие эксплойта" = false)

and (Уязвимость like "%Remote Code Execution%" or Уязвимость like "%Удаленное%выполнение%" or Уязвимость like "%Повышение%привилеги%" or Уязвимость like "dos%" or Уязвимость like
"%Отказ%в%обслуживании%")

and ("Оценка CVSS 3.0" <= 7)) |

group("Название ПО", "Версия ПО", COUNT(*)) |

sort("COUNT(*)" DESC)
```

▶ Выполнить Ctrl+Enter

Название Название ПО	Версия Версия ПО	COUN...	Узел Хост	Производитель Вендор	Название Название ПО	Версия Версия ПО	Уязвимость Уязвимость	Базовая оценка уяз... Оценка CVSS 3.0	Эксплойт Наличие эксплойта
Microsoft Internet Explorer	11.0	33	pc7.company.com (192.168.0.93)	Microsoft	Microsoft Internet ...	11.0	Удаленное вы...	6,4	False
Microsoft .NET Framework	4.5.2	12	pc7.company.com (192.168.0.93)	Microsoft	Microsoft Internet ...	11.0	Повышение пр...	4,3	False
Microsoft Outlook	2013	8	pc7.company.com (192.168.0.93)	Microsoft	Microsoft Internet ...	11.0	Повышение пр...	2,6	False

Всего 20 группировок, выбрана 1

Всего 33 записи, выбрана 1 запись (1 актив, 1 уязвимость)


MaxPatrol 10
Активы
Инциденты
Сбор данных
Система
Управление уязвимостями
Рекомендации по НКЦКИ
НКЦКИ (Кейс №1)
18:00
1 из 9
НКЦКИ (Кейс №2)
18:41
Microsoft Internet Explorer, 11.0
Microsoft .NET Framework, 4.5.2
Microsoft Outlook, 2013
Microsoft .NET Framework, 3.5.1
Google Chrome, 48.0.2564.116
Microsoft Word, 2013
Microsoft Office, 2013
Microsoft Outlook, 2016
nginx, 1.1.19
iTunes, 12.3.1.23
Microsoft Outlook, 2010
Microsoft Word, 2016
Apache Subversion, 1.8.11
Microsoft Word, 2010
Microsoft Office, 2016
Microsoft .NET Framework, 3.0
Foxit Reader, 7.2.2.929
FireFox ESR, 38.3.0
FireFox, 87.0
Thunderbird, 38.3.0

MaxPatrol VM

Выстроит процесс управления уязвимостями, результаты которого видны

- Телеграм-канал с новостями о продуктах Positive Technologies: t.me/ptproductupdate
- Задать вопрос о функционале MaxPatrol 10: t.me/MPSIEMChat