



Кондитерская фабрика

**ПОБЕДА**

«Импортозамещение»,

как мы его видим

Гордиенко Ростислав

Директор по информационным  
технологиям.

тел. моб: +7 966 06 06 620

e-mail: [r.gordienko@pobedavkusa.ru](mailto:r.gordienko@pobedavkusa.ru)

[store.pobedavkusa.ru](http://store.pobedavkusa.ru)





# 24 года



# 2023

-Общая производственная площадь трех фабрик (Россия + Латвия) компании составляет 43 тыс. кв. м.

-Численность персонала группы компаний «Победа» составляет **более 1500 сотрудников.**

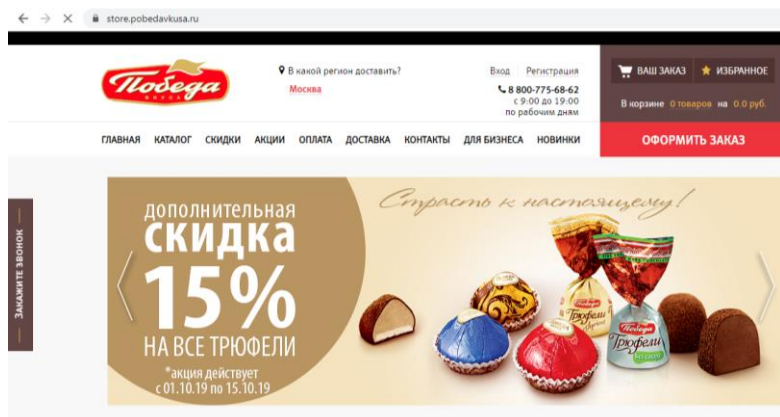
-**Производственная мощность всех фабрик – 250 тонн шоколада в сутки**

-общий объём накопленных инвестиций с 1999 года — более \$80 млн.

-Знание марки «Победа вкуса» - 30% среди всех потребителей шоколада в России (данные Mediascope 2019)



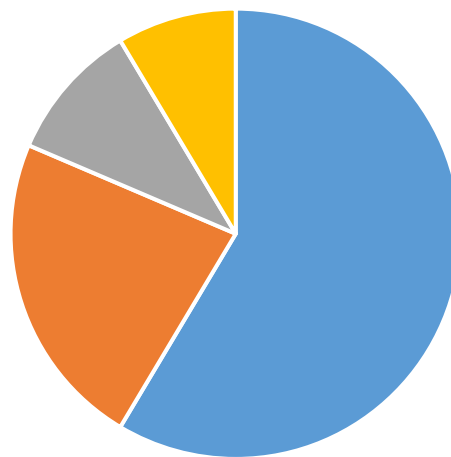
## Интернет магазин



## Филиалы

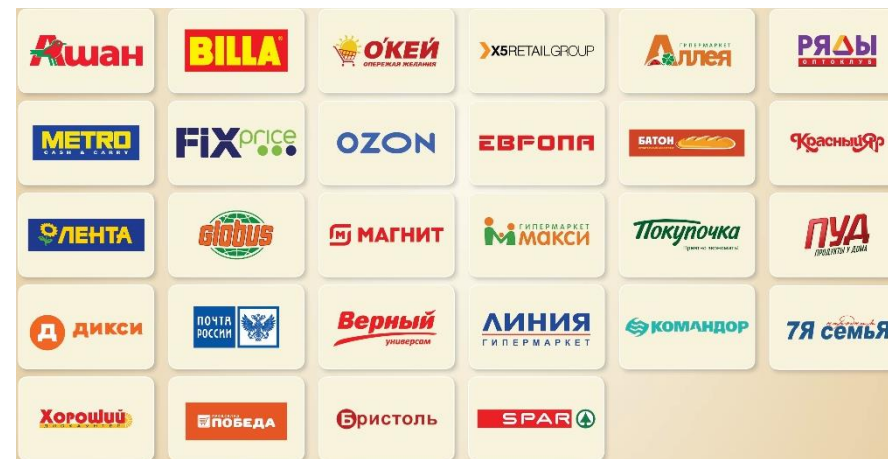


## Продажи



■ Кв. 1 ■ Кв. 2 ■ Кв. 3 ■ Кв. 4

## Сети



## Маркетплейс



# ПРОБЛЕМЫ



- Отсутствие специалистов (администраторы Linux, администраторы WMS систем, разработчики)
- Отсутствие нишевых отечественных решений
- Сопротивление пользователей изменениям (переход на другое ПО)
- Повышение цен на российское ПО после определенных событий
- Отсутствие сопоставимых Российских аналогов оборудования и ПО



# Риски использования западного ПО



- неожиданный уход вендоров;
- безопасность использования;
- отключение доступа к информационным ресурсам и потеря данных;
- отсутствие поддержки и обновлений.



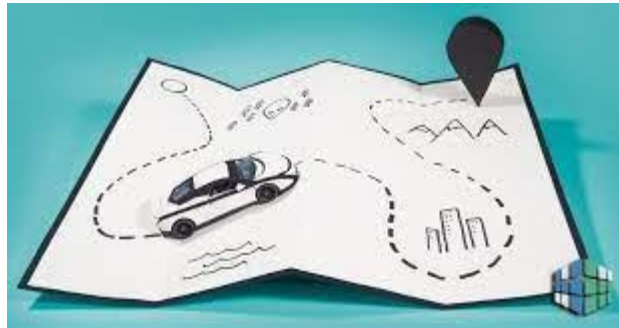
покупка сервиса на зарубежное юрлицо;  
переход на российское решение.

# Импортозамещение



- Обеспечение технологического суверенитета
- Экономический рывок для отечественных разработчиков
- Лучшая адаптированность к российской специфике (законы, интерфейс)
- Изменение мнения, что все западное – лучше!

# План действий



- Инвентаризация ИТ активов
- Классификация, выборы аналогов
- Определение рисков и критичности
- Каждое замещение как отдельный проект



# Новая реальность



- С февраля 2022 года Россия –цель № 1 для хакеров и киберпреступников
- >170 комплексных компьютерных атак ежедневно
- Число кибератак на российскую инфраструктуру выросло на 80%
- Не менее, чем в 20 раз выросло число кибератак на финансовые организации
- С 24 февраля были украдены данные 65 млн россиян.



# Автоматическое обнаружение уязвимостей



XSpider (Positive Technologies)

MaxPatrol 8 (Positive Technologies)

RedCheck («АЛТЭКС-СОФТ»)

ScanOVAL (ФСТЭК России)

ScanOVAL ГЛАВНОЕ СПРАВКА

Отображать: Только обнаруженные

Идентификатор уязвимости	Результат	Уровень о...	Ссылки на источники	Название уязвимости
cpe:/a:microsoft:access:2016 (2)				
cpe:/a:microsoft:visual_c++:2010:redistribution_pkg (1)				
cpe:/a:microsoft:powerpoint:2016 (5)				
BDU:2021-01364	Обнаружена	Высокий	VULN-20210322.9; CVE-2021-270	Уязвимость удаленного выполнения кода Microsoft PowerPoint (BDU:2021-01364)
BDU:2019-04764	Обнаружена	Высокий	VULN-20191217.2; CVE-2019-146	Уязвимость удаленного выполнения кода Microsoft PowerPoint (BDU:2019-04764)
BDU:2020-01734	Обнаружена	Высокий	VULN-20200415.2; CVE-2020-076	Уязвимость удаленного выполнения кода Microsoft Office (BDU:2020-01734)
BDU:2018-01638	Обнаружена	Средний	CVE-2018-8628; CVE-2018-8628	Уязвимость удаленного выполнения кода Microsoft PowerPoint (BDU:2018-01638)
BDU:2020-05871	Обнаружена	Средний	VULN-20201223.5; CVE-2020-171	Уязвимость удаленного выполнения кода Microsoft PowerPoint (BDU:2020-05871)
cpe:/o:microsoft:windows_10::x64 (1)				
cpe:/a:7-zip:7-zip (2)				

Группировать по рискам   Группировать по продуктам   20 107 62 4

**Подробности**

**Идентификатор уязвимости** [BDU:2021-01364](#)

**Результат** Обнаружена

**Уровень опасности уязвимости** Высокий

**OVAL** [oval:ru.altx-soft.win:def:75336](#) (версия 5)

**Название уязвимости** Уязвимость удаленного выполнения кода Microsoft PowerPoint (BDU:2021-01364)

**Описание уязвимости** Уязвимость удаленного выполнения кода Microsoft PowerPoint.

**Возможные меры по устранению уязвимости** Использование рекомендаций:  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27056>

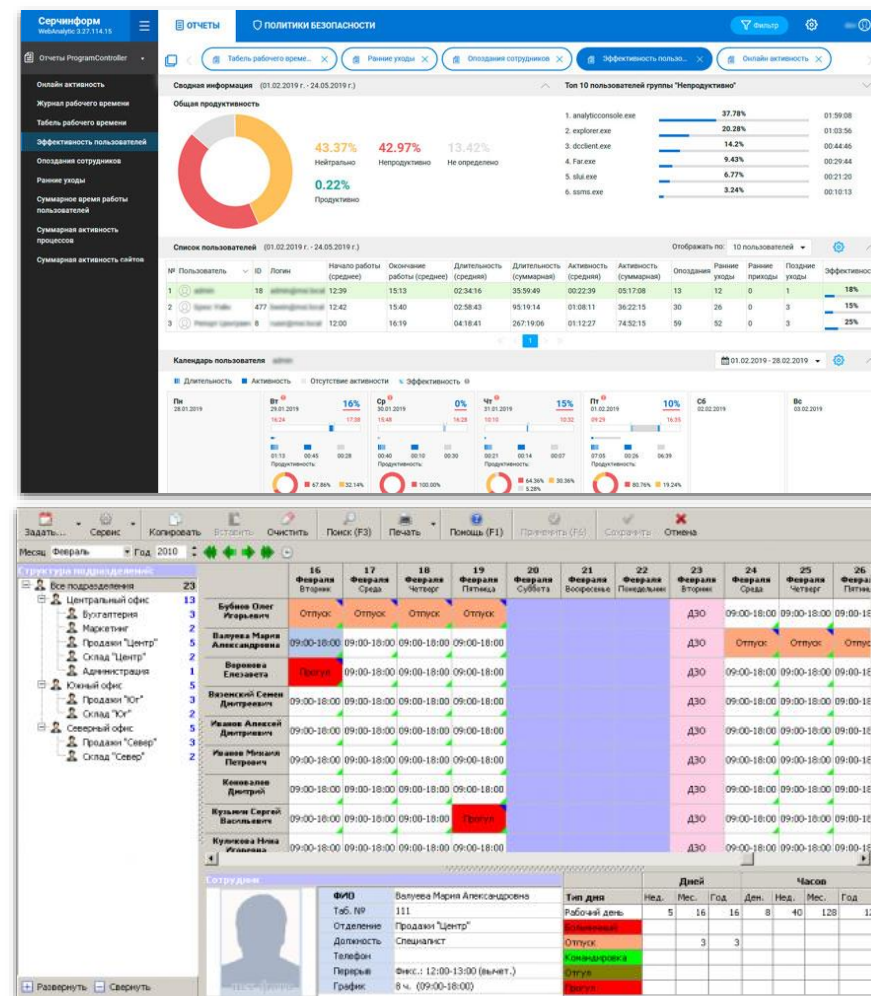
**Ссылки на источники** NKCKI | [VULN-20210322.9](#)  
Microsoft | [CVE-2021-27056](#)  
CVE | [CVE-2021-27056](#)

**Базовый вектор уязвимости** CVSS: AV:N/AC:L/Au:S/C:C/I:C/A:C

<https://bdu.fstec.ru/vul>

# DLP ВОЗМОЖНОСТИ ПЕРЕХВАТА

1. Контроль отправки персональных данных, зарплатных файлов и т.п. по почте «наружу» (предварительно требуется обучение программы, что есть подобные данные);
2. Контроль облачных сервисов;
3. Контроль за движением документов.
4. Контроль мессенджеров
5. Контроль печати
6. Контроль нерационального использования рабочего времени;
7. И многое другое...



# Контроль продуктивности



## Показатель продуктивности пользователей (период: 13.04.2020-16.04.2020)

День	Показатель	Активность
<b>Результатов: 4</b>		
<b>13.04.2020</b>		<b>7:27</b>
Нейтрально	0,09%	23с
Продуктивно	99,04%	7:23
Не определено	0,82%	0:03
Непродуктивно	0,05%	13с
<b>14.04.2020</b>		<b>8:17</b>
Нейтрально	0,04%	13с
Продуктивно	99,95%	8:17
Непродуктивно	0,01%	2с
<b>15.04.2020</b>		<b>7:33</b>
Нейтрально	0,44%	0:01
Продуктивно	99,54%	7:31
Непродуктивно	0,02%	6с
<b>16.04.2020</b>		<b>4:39</b>
Нейтрально	0,02%	3с
Продуктивно	99,98%	4:39

## Нарушения рабочего режима (период: 20.04.2020 - 20.04.2020)

Дата	Опоздания			Низкая активность	
	Пользователь	Пришел	Опоздание	Пользователь	Активность
20.04.2020 Пн	[Redacted]	12:47	3:47	[Redacted]	1:48
		11:49	2:49		2:37
		10:39	1:39		4:33
		9:19	0:19		

## Показатель продуктивности пользователей (период: 13.04.2020-16.04.2020)

День	Показатель	Активность
<b>Результатов: 4</b>		
<b>13.04.2020</b>		<b>7:27</b>
Нейтрально	0,09%	23с
iexplore.exe		15с
chrome.exe		8с
Продуктивно	99,04%	7:23
1cv8.exe		5:25
OUTLOOK.EXE		0:30
mstsc.exe		0:21
WINWORD.EXE		0:19
explorer.exe		0:18
1cv8c.exe		0:14
EXCEL.EXE		0:03
acrord32.exe		0:02
vr402001.res		0:02
rocket.chat.exe		0:01
pobeda.ispringonline.ru		38с
cmd.exe		13с
1cv8s.exe		4с
Не определено	0,82%	0:03
Непродуктивно	0,05%	13с

# FileAuditor



**Выявляет** в общем документообороте информацию, подлежащую защите.



**Управляет** доступом к данным: отслеживает группы сотрудников, которые создают, хранят или обрабатывают данные ограниченного доступа.



**Следит** за операциями с конфиденциальными данными.



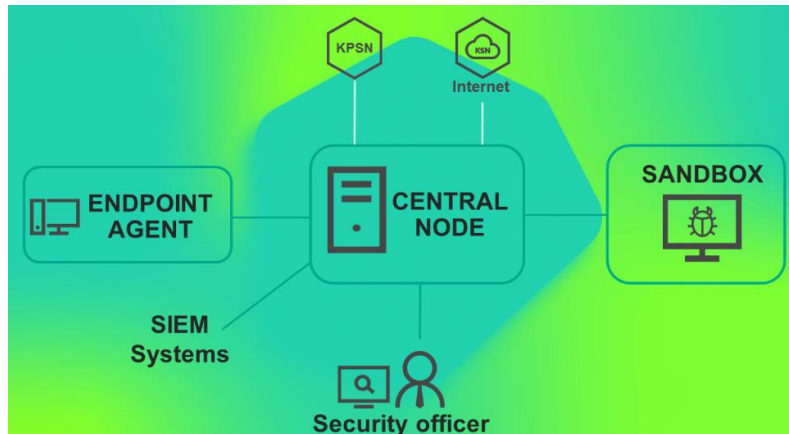
**Блокирует** опасную активность с конфиденциальными файлами в любом произвольном приложении.

# Текущие пилоты

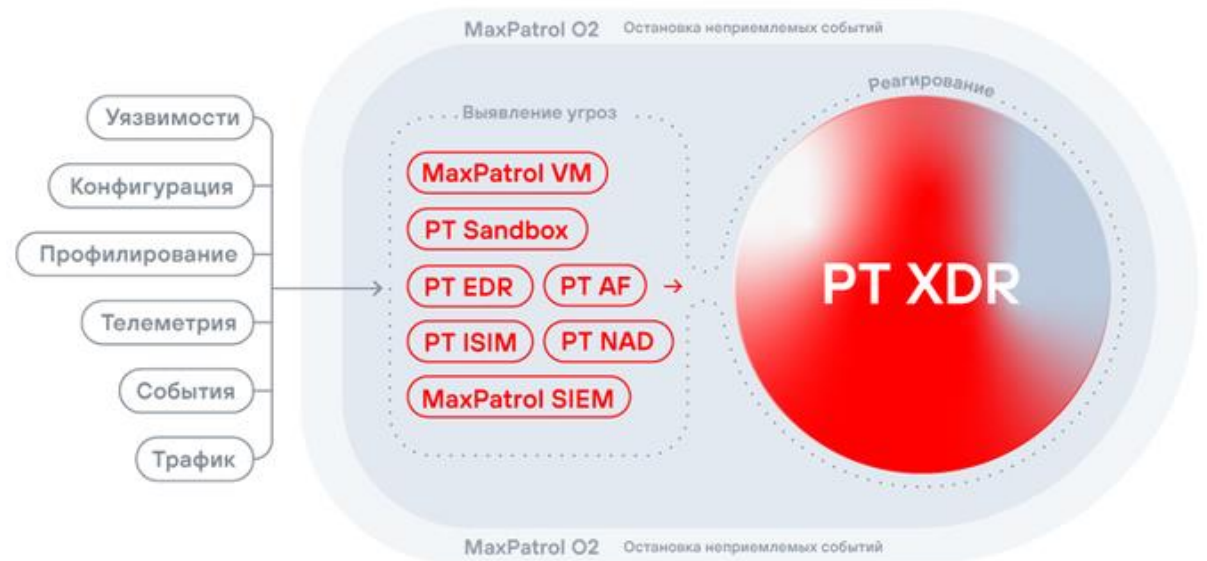


- EDR, XDR решения

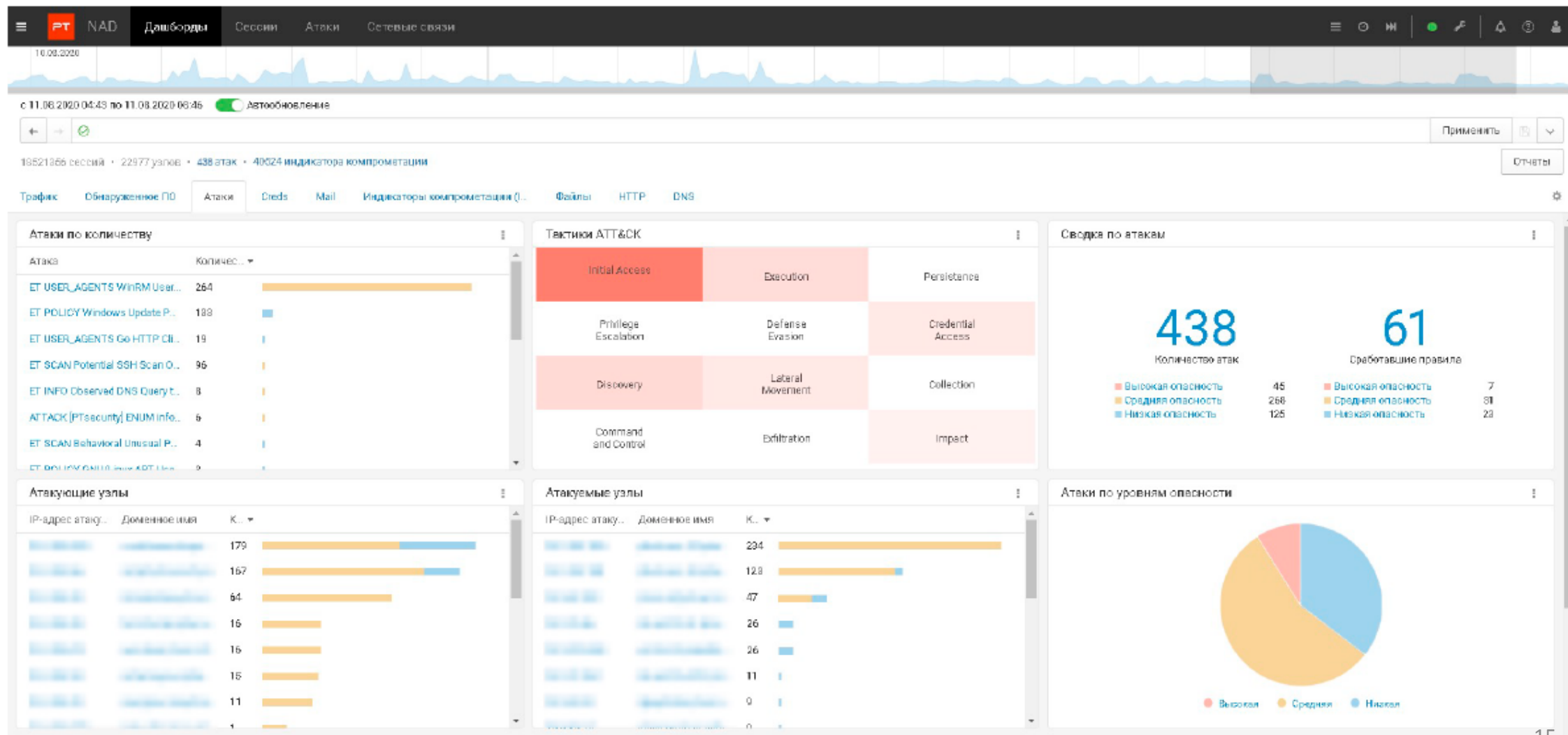
kaspersky



pt positive technologies



# PT Network Attack Discovery





# Positive Technologies Sandbox



**pt Sandbox** | Сводка | Задания | Объекты | Исключения | Образы VM | Система ▾ | + Проверить объекты ▾ | 🔔 | ⓘ | 👤

**Сводка** | 1 час | 24 часа | 7 дней | 30 дней | Произвольный период: 30 мар, 16:58 — 4 апр, 16:58 | Обновить

### Выполненные задания

● **4609** ● **14** ● **10**

Всего | С опасными файлами | С потенциально опасными файлами

Заданий в час

2k  
1k

31 мар 15:00 1 апр 15:00 2 апр 15:00 3 апр 15:00 4 апр 15:00

### Задания по источникам

С опасными файлами | Все

За период **4609**

retro	512	web	2	ptnad	25
f5-icap-test	3941	interactive_analysis	1		
PTDemo-XDR-One	55	icap-test	70		
cybsi-demo	1	mail-agent	2		

### Рейтинг файлов по опасности

[Перейти к заданиям](#)

<a href="#">INVOICE.pdf.exe</a>	4 апр, 10:27	API PTDemo-XDR-One	Бэкдор	🔥🔥🔥
<a href="#">INVOICE.pdf.exe</a>	4 апр, 10:27	API PTDemo-XDR-One	Бэкдор	🔥🔥🔥
<a href="#">INVOICE.pdf.exe</a>	3 апр, 15:56	API cybsi-demo	Бэкдор	🔥🔥🔥
<a href="#">INVOICE.pdf.exe</a>	31 мар, 12:54	Хранилище (повторная проверка)	Бэкдор	🔥🔥🔥
<a href="#">INVOICE.pdf.exe</a>			Бэкдор	🔥🔥🔥

### Проверено файлов методом поведенческого анализа

<b>win10-1803-x64</b>	<b>win7-sp1-x64</b>
● <b>5</b> Всего	● <b>2</b> Всего
● <b>1</b> Опасных	● <b>0</b> Опасных



**Kaspersky Anti Targeted Attack Platform**

- Мониторинг
- Обнаружения 999+
- Поиск угроз
- Задчи
- Политики
- ИОС-проверка
- Хранилище
- Endpoint Sensors
- Отчеты

## Мониторинг > Создать схему

Название схемы  Сохранить Отмена Графики

### Работоспособность системы

Статус компонентов:

- С ошибкой: 0
- Без ошибок: 10
- Отключено: 0

Обработка данных:

- ✓ Sensors
- ✓ Очереди

### Обработка данных (SPAN) titanic.avp.ru Текущая загрузка

Трафик	262
Файлы	1.121
URL-адреса	2.501

Ошибки обработки:

- Сессии: 72.282
- Пакеты: 3.032
- Файлы: 0
- URL-адреса: 0
- KSN-обнаружения: 0
- IDS-обнаружения: 0

### Обнаружения по состоянию

- Новых: 796
- В обработке: 0
- Обработано: 0

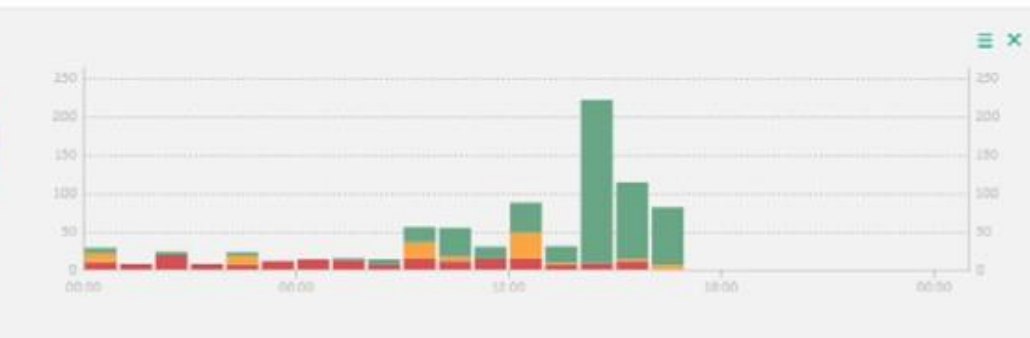
Всего: 796

### Обнаружения по степени важности

- Высокая: 161
- Средняя: 94
- Низкая: 541

Всего: 796

Учитывать обработанные



### Топ 10 IP-адресов

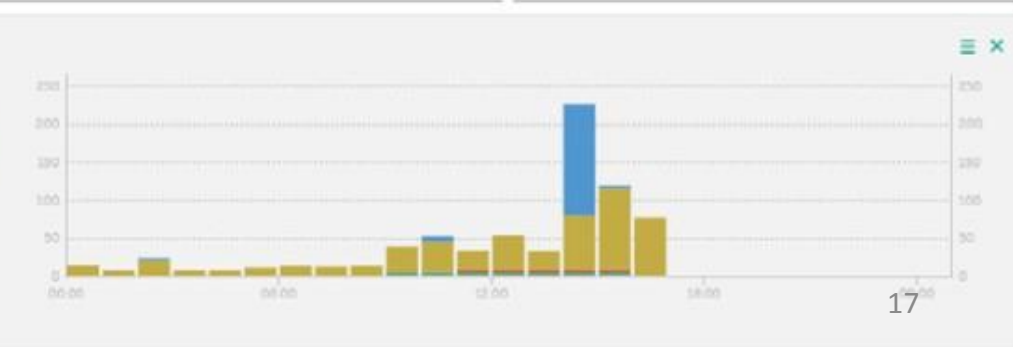
1.	10.16.34.129	135
2.	10.64.48.11	81
3.	10.64.48.10	67
4.	10.16.35.29	52
5.	10.69.119.111	45
6.	10.16.112.38	27
7.	192.168.240.239	24
8.	10.16.40.15	20
9.	82.118.17.122	15
10.	10.16.35.64	12

### Топ 10 доменов

1.	api.ceb23e42.sovce	29
2.	coinhive.com	25
3.	frankshelley.com	24
4.	ws024.coinhive.com	20
5.	www.lubreg.ru	20
6.	ws026.coinhive.com	18
7.	ws027.coinhive.com	18
8.	ws022.coinhive.com	17
9.	ws023.coinhive.com	17
10.	m91e6.simpotex.com	16

### Обнаружения по вектору атаки

- Комплексные: 12
- Файлы из почты: 0
- Файлы из трафика: 9
- URL из почты: 0
- URL из трафика: 523
- Endpoint Sensors: 156



# Замещено



kaspersky

zoom



# Планы



- NGFW



**МегаФон NGFW**  
Межсетевой экран нового поколения



- Аналоги active directory

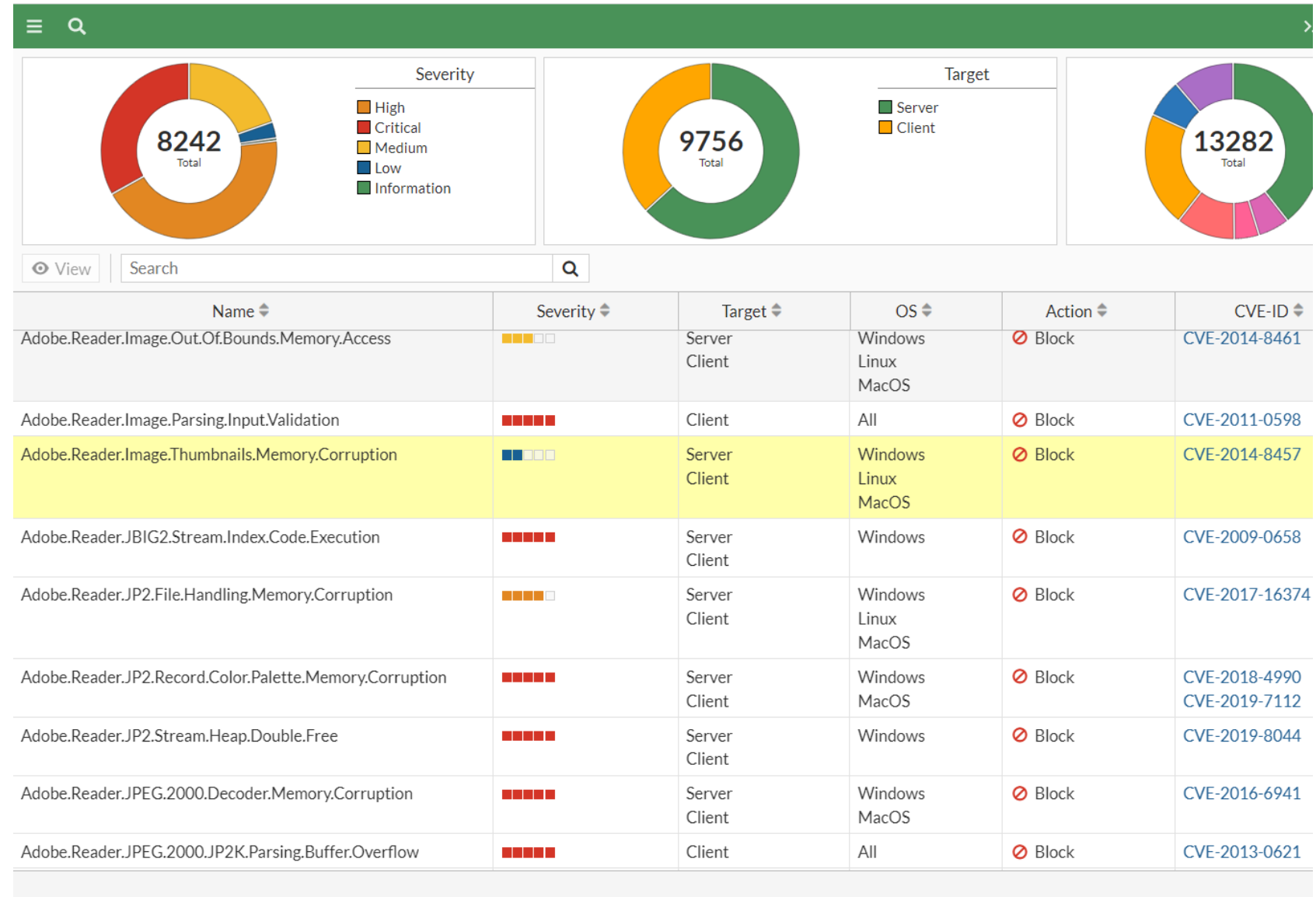


# NGFW (FortiGate)\*



Intrusion Prevention System, — система предотвращения вторжений

CVE (Common Vulnerabilities and Exposures) – это список известных уязвимостей и дефектов безопасности



**CVE ID**  
**CVE-2018-20580** Detail

Год опубликования: CNA номер

**Current Description**

Тип уязвимости: Продукт: Версия: Воздействие:

The WSDL import functionality in SmartBear ReadyAPI 2.5.0 and 2.6.0 allows remote attackers to execute arbitrary Java code via a crafted request parameter in a WSDL file.

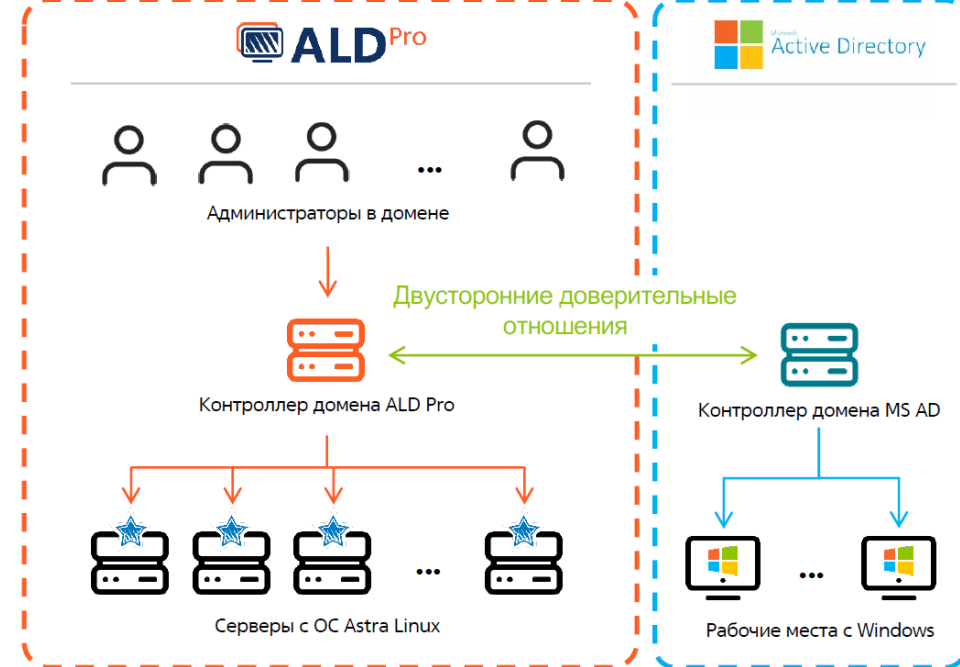
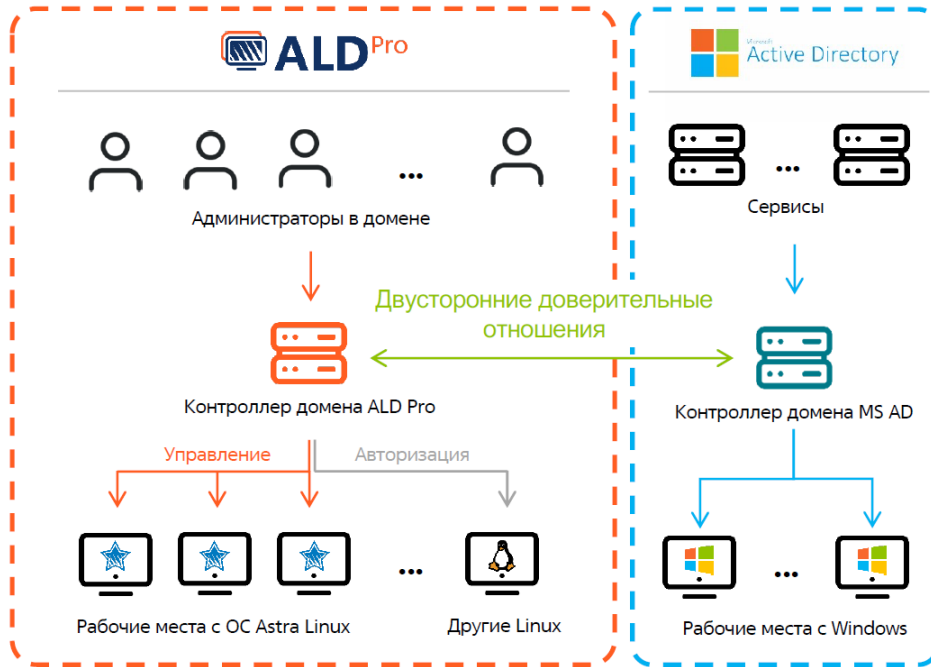
Атака

**Severity** CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: **8.4** CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/LH/A:H

# Astra Linux Directory (ALD) Pro



## Июль-август

- **Глобальный каталог**
- **Двусторонние доверительные отношения** (базовая реализация)
- **Синхронизация объектов и параметров между MS AD и ALD Pro** (базовая реализация)

## Сентябрь-октябрь

- **Расширение области применения групповых политик**
- **Расширение количества ролей администраторов**
- **Разработка документации** для снижения порога вхождения

## Ноябрь-декабрь

- **Расширение возможностей API**
- **Лес доменов** на базе ALD Pro (ALD Pro/FreeIPA)
- **Базовая поддержка ARM**
- **Базовая поддержка мобильной ОС Astra Linux**

# Методические рекомендации по цифровой трансформации

требование по увеличению в два раза совокупных расходов на информационные технологии в 2022-2024 гг. в сравнении с 2019-2021 гг.;

требование, чтобы совокупная доля расходов на закупку российского ПО и связанных с ним работ (услуг) по итогам 2022-2024 гг. в общем объеме расходов на закупку ПО составила 80%;

расходы на внутренние разработки не более 30% общих расходов на ИТ в 2022-2024 гг.;

доля инвестиций в готовое российское ПО не менее 35% в общем портфеле расходов;

полный запрет на использование иностранного ПО на значимых объектах КИИ с 1 января 2025 г.

# Предложения

1. Повысить значимость ИТ технологий в школе:

1. Увеличить количество часов
2. Улучшить материальную базу
3. Увеличить количество кружков по робототехнике, программированию



2. В ВУЗах проводить обучение на базе отечественного программного обеспечения.



# СПАСИБО ЗА ВНИМАНИЕ!!!

Гордиенко Ростислав

Директор по информационным  
технологиям.

тел. моб: +7 966 06 06 620

e-mail: [r.gordienko@pobedavkusa.ru](mailto:r.gordienko@pobedavkusa.ru)

[store.pobedavkusa.ru](http://store.pobedavkusa.ru)