

Возможность защиты промышленных предприятий – рецепты Dr.Web



**Необходимость защиты
критической инфраструктуры
не вызывает сомнений:
есть требования государства, прописана
ответственность за их нарушение...**



И есть довольно много предложений по защите предприятий, подразумевающих проверку промышленных протоколов и обеспечение целостности ПО, используемого в различном оборудовании.



Но как правило вредоносное ПО проникает через почту или сменные носители – либо же появляется вместе с новым оборудованием.



Это требует в первую очередь позаботиться о защите станций тех же операторов, компьютеров и устройств сотрудников, имеющих доступ к почте.



На что нужно обратить внимание,
выбирая решение для защиты?



Отсутствие влияния на процессы

До начала использования решения необходимо не просто установить продукт, но и проверить типовые процедуры, включающие его использование. В том числе отсутствие влияния обновлений на рабочие процессы (достаточность каналов связи), возможность тестирования обновлений до момента их распространения.



Удобные процедуры установки и обновления

Наличие различных вариантов установки (со сканированием сети, с использованием AD...) и обновления, включая возможность обновления без прямого доступа к Интернету.

Низкие системные требования и скорость проверки

Используемый продукт во время своей работы не должен существенно задействовать жесткий диск.

Скорость срабатывания антивируса не должна существенно зависеть от степени использования жесткого диска другими процессами.



Продукт должен быть совместим в том числе с устаревшими и неподдерживаемыми производителем системами (Низкие системные требования и поддержка оборудования компании Windows XP SP2).



Интеграция с SIEM/SOC/ГосСопка

спешность работы таких систем ГосСОПКА, SIEM, IRP или SOAR напрямую зависит от глубины и полноты передаваемой в них информации о происходящих в сети событиях ИБ. Dr.Web является бесспорным профессионалом в деле сбора такой информации. Интеграция любых внешних систем сбора данных об ИБ-событиях с Dr.Web позволяет еще быстрее реагировать на аномальное поведение в защищаемой Dr.Web сети.

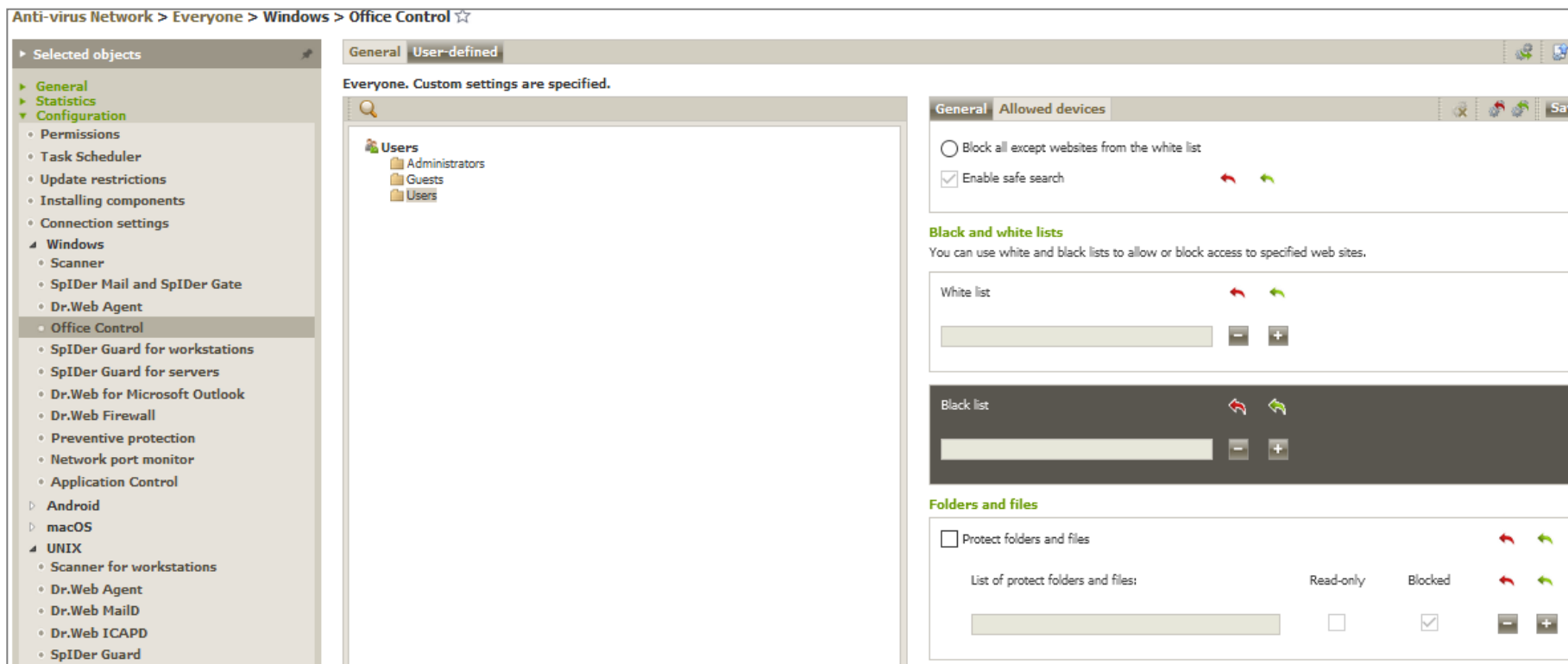


Минимум ложных срабатываний (в идеале – их полное отсутствие), настройки, которые исключают удаление любых обнаруженных файлов без разрешения администратора сети, удобная система информирования об инцидентах безопасности.

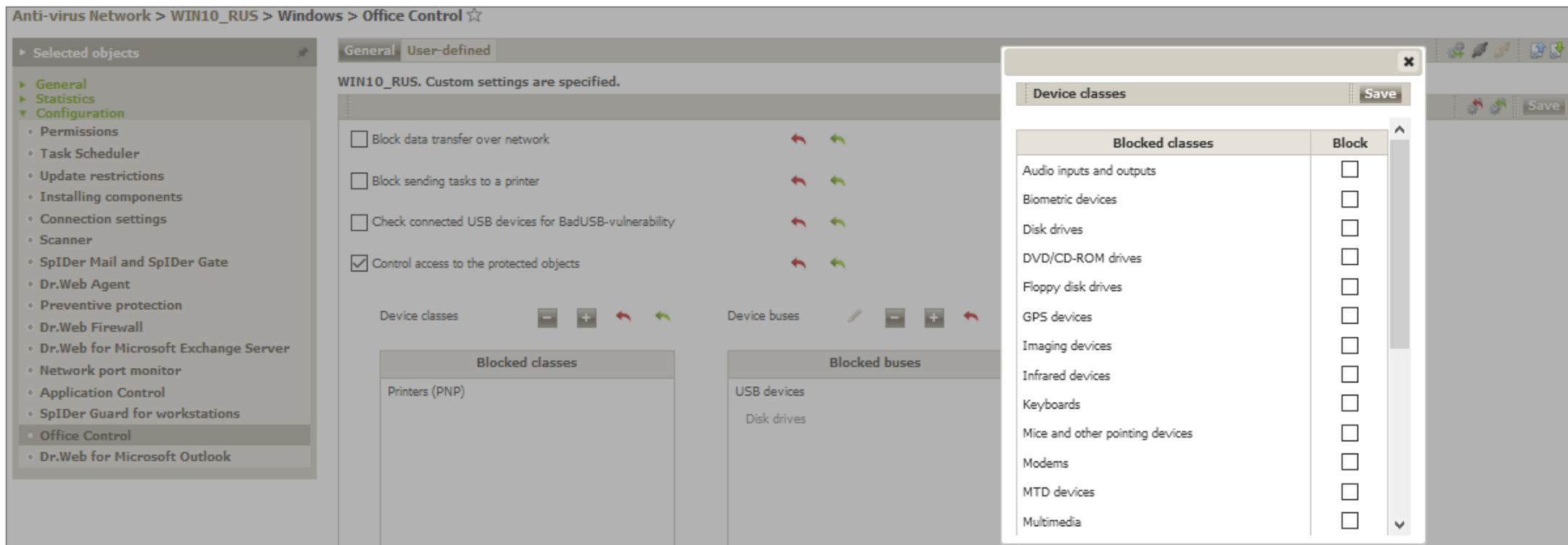
Белые списки

Доступ только к «ЧИСТЫМ» ресурсам

Доступ к ресурсам только в указанное время



Контроль использования внешних носителей и оборудования компании



Anti-virus Network > WIN10_RUS > Windows > Office Control ☆

Selected objects

- General
- Statistics
- Configuration
 - Permissions
 - Task Scheduler
 - Update restrictions
 - Installing components
 - Connection settings
 - Scanner
 - SpIDer Mail and SpIDer Gate
 - Dr.Web Agent
 - Preventive protection
 - Dr.Web Firewall
 - Dr.Web for Microsoft Exchange Server
 - Network port monitor
 - Application Control
 - SpIDer Guard for workstations
 - Office Control
 - Dr.Web for Microsoft Outlook

General User-defined

WIN10_RUS. Custom settings are specified.

- Block data transfer over network
- Block sending tasks to a printer
- Check connected USB devices for BadUSB-vulnerability
- Control access to the protected objects

Device classes

Blocked classes

Printers (PNP)

Device buses

Blocked buses

USB devices

Disk drives

Device classes

Blocked classes	Block
Audio inputs and outputs	<input type="checkbox"/>
Biometric devices	<input type="checkbox"/>
Disk drives	<input type="checkbox"/>
DVD/CD-ROM drives	<input type="checkbox"/>
Floppy disk drives	<input type="checkbox"/>
GPS devices	<input type="checkbox"/>
Imaging devices	<input type="checkbox"/>
Infrared devices	<input type="checkbox"/>
Keyboards	<input type="checkbox"/>
Mice and other pointing devices	<input type="checkbox"/>
Modems	<input type="checkbox"/>
MTD devices	<input type="checkbox"/>
Multimedia	<input type="checkbox"/>

Контроль запуска программ пользователем (и под его именем)

Anti-virus Network > Everyone > Windows > Application Control ☆

Selected objects

- General
- Statistics
- Configuration
 - Permissions
 - Task Scheduler
 - Update restrictions
 - Installing components
 - Connection settings
 - Windows
 - Scanner
 - SpIDer Mail and SpIDer Gate
 - Dr.Web Agent
 - Office Control
 - SpIDer Guard for workstations
 - SpIDer Guard for servers
 - Dr.Web for Microsoft Outlook
 - Dr.Web Firewall
 - Preventive protection
 - Network port monitor
 - Application Control

Everyone. Custom settings are specified.

Profile name	Operation mode	Functional analysis criteria	Deny rules	Allow rules	Trusted applications
new	Active, Test	12 conditions	0 rules	0 rules	0 groups

1 Page: 1 Showing 1 – 1 of 1 10

DR.WEB ENTERPRISE SECURITY SUITE

Защищает по закону

 ИСПДн	 ГИС/МИС		 Объекты КИИ
до 1 уровня защищенности включительно	до 1 класса защищенности включительно	Системы обработки сведений, содержащих гостайну	вплоть до высшей категории

- ✓ Государственные гарантии отсутствия в сертифицированных продуктах Dr.Web недеklarированного функционала.
- ✓ Лицензии и сертификаты ФСТЭК России, Минобороны России, ФСБ России.

Все лицензии и сертификаты: https://company.drweb.ru/licenses_and_certificates/

**С радостью ответим
на ваши вопросы!**

И благодарим за внимание.

ООО "Доктор Веб"

Телефон +7 (495) 789-45-87

Факс +7 (495) 789-45-97

e-mail secretary@drweb.com

