КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАК НЕЗАЩИТИТЬ ДАННЫЕ. РЕАЛЬНЫЙ СЛУЧАЙ АНАЛИЗА ИНЦИДЕНТА

ВЯЧЕСЛАВ МЕДВЕДЕВ
Ведущий аналитик отдела развития
Доктор Веб

МЕСТО ВСТРЕЧИ ИБ-ПРОФЕССИОНАЛОВ

13 ФЕВРАЛЯ’20

РОСТОВ-НА-ДОНУ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как изменится ваша ИБ в 2020 году

Dr.WEB®
с 1992 года

Вячеслав Медведев
ООО «Доктор Веб»

ТЕЛЕФОН: +7 495 789-45-87

EMAIL: v.medvedev@drweb.com

13 февраля 2020
Ростов-на-Дону

Dr.WEB®
с 1992 года

Мы постоянно рассказываем о росте количества угроз, новом функционале, возможностях, которые могут использовать наши клиенты

Давайте в этот раз сделаем по иному. Посмотрим, что получается, когда советы не используются

Dr.WEB®
с 1992 года

Компания Dr.Web занимается анализом компьютерных инцидентов (тем что в просторечии называется расследованием преступлений), выступает в роли эксперта по таким делам.

И что удивительно – ситуации бывают самые разные. А вот причины, которые послужили основой возникших проблем – почти всегда одинаковы

Dr.WEB®
с 1992 года

Пример реального инцидента

Dr.WEB®
с 1992 года

Вводная:

Весной 2019 года в службу технической поддержки «Доктор Веб» обратился корпоративный клиент с жалобой на проблемы в работе сервера. Нагрузка на вычислительные мощности была очень высокой и возникала словно из ниоткуда.

Dr.WEB®
с 1992 года

Перед экспертами было поставлено несколько задач.

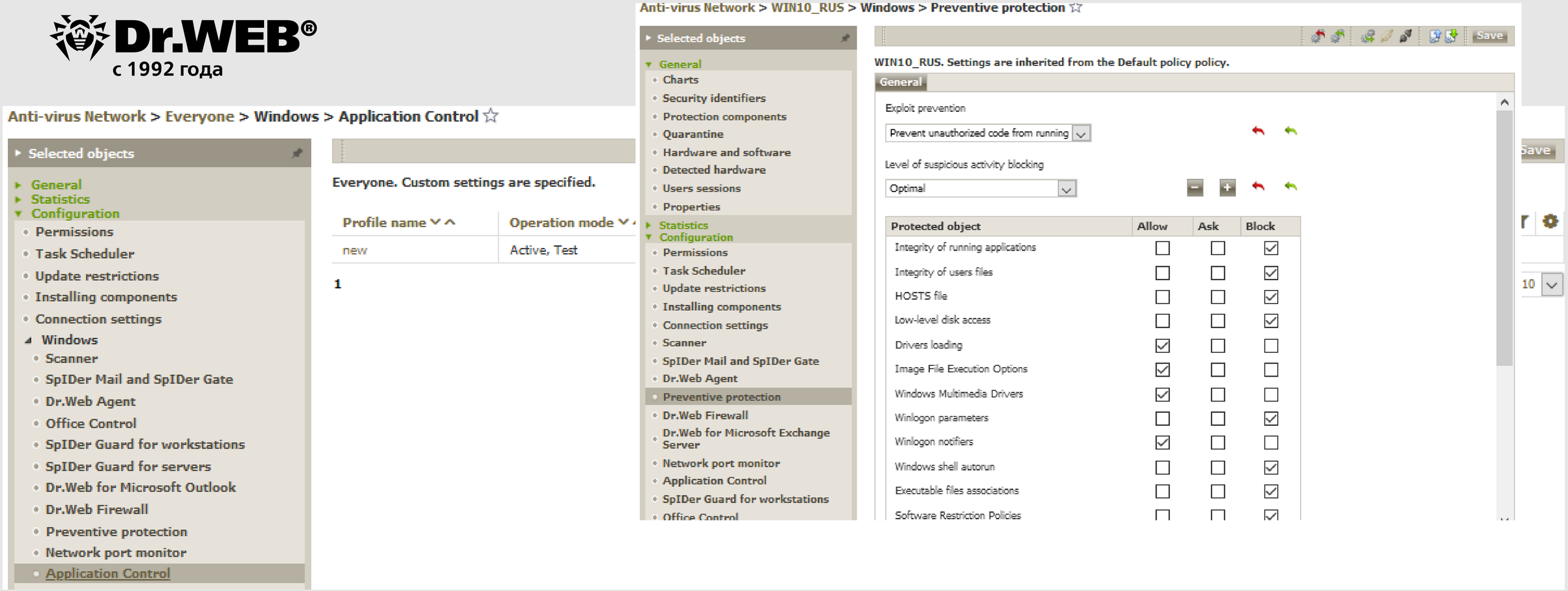
- Обнаружить причину необычно высокого потребления ресурсов.
- Отследить источник и способ атаки, чтобы пресечь дальнейшее распространение вредоносной программы. Сделать подробное описание атаки.
- На основании проведенного исследования разработать рекомендации по усилению мер безопасности в сети клиента.
- Помочь правоохранительным органам найти виновного в атаке.

Dr.WEB®
с 1992 года

Заражение начиналось с RCE-уязвимости в легальном продукте.

- Уязвимости есть всегда. Только не все они еще известны
- Мер защиты много. В частности антивирус – это защита от использования уязвимостей:
  - Превентивная защита
  - Контроль целостности
  - Защита от эксплойтов
  - …

Dr.WEB®
с 1992 года



Отключение защиты целостности процессов в используемом антивирусе – путь к заражению!

#CODEIB

Dr.WEB®
с 1992 года

Через эксплойт на стороне пострадавшего клиента создавалась административная учетная запись для доступа по RDP.

Возможные проблемы:

- Работа программ с административными правами
- Отсутствие запрета на запуск нового ПО
- Слабые пароли
- Отсутствие контроля целостности

Dr.WEB®
с 1992 года

…до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. 273 УК РФ

Злоумышленник вручную заходил на сервер по RDP и, используя легитимное ПО ProcessHacker, «убивал» установленный антивирус или просто отключал его напрямую через GUI

Dr.WEB®
с 1992 года

Возможные проблемы

- Наличие удаленного доступа
- Запущенные ненужные сервисы
- Установка неразрешенного ПО
- Разрешение на загрузку драйверов
- Наличие прав пользователя на отключение антивируса
- Отсутствие централизованной защиты
- Отсутствие контроля за изменением состава ПО
- Отсутствие белого списка ПО
- Отсутствие пароля на доступ к настройкам антивируса
- Отсутствие пароля на удаление ПО или пароль, совпадающий с паролем доступа в систему

Dr.WEB®
с 1992 года

Контроль приложений Dr.Web

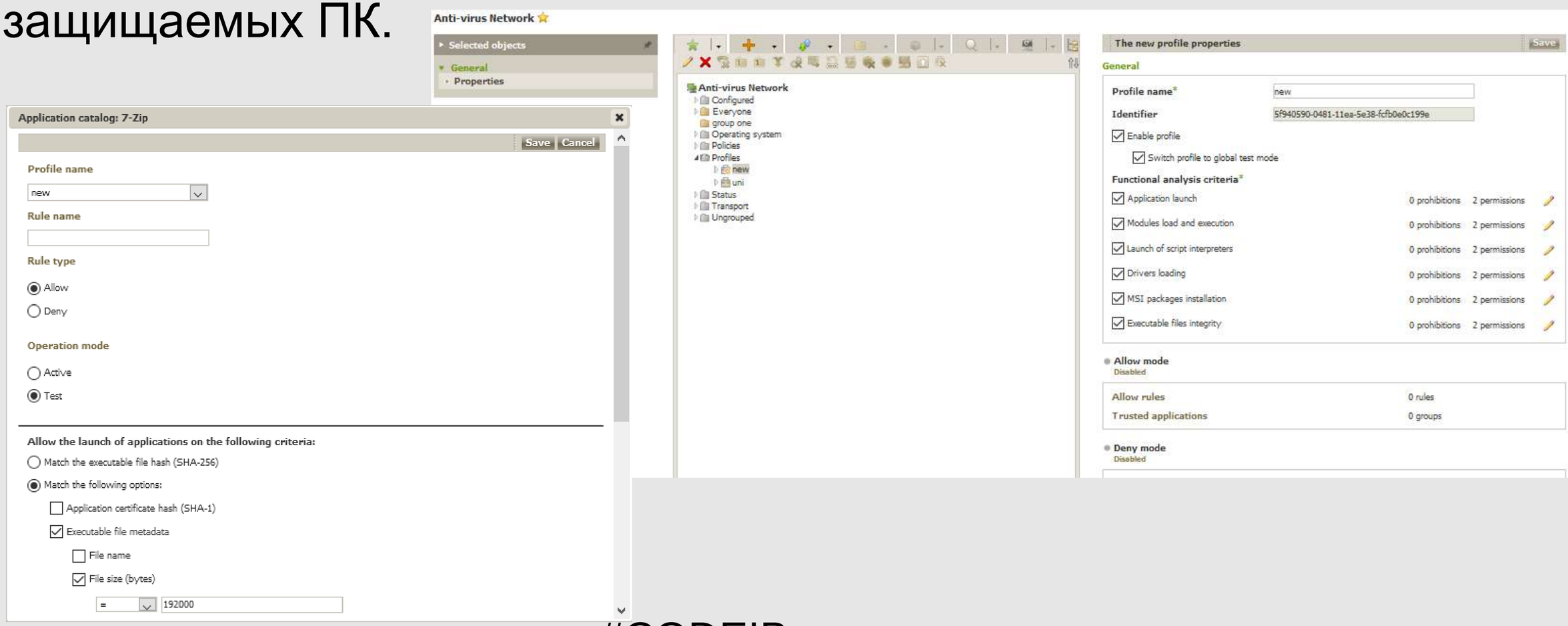
Управление работой модуля **Контроль приложений** производится на основе:

- ✓ запрещающих правил,
- ✓ разрешающих правил,
- ✓ специальных правил, созданных для противодействия наиболее часто используемым злоумышленниками методик обхода антивирусной защиты.

Dr.WEB®
с 1992 года

Контроль приложений Dr.Web

Администратор может определять, что контролировать на защищаемых ПК.

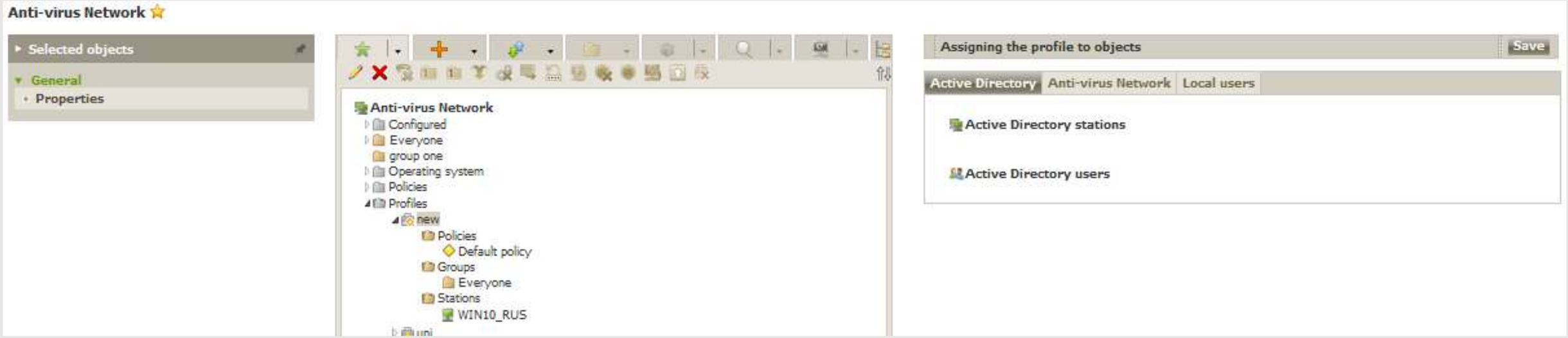


#CODEIB

Dr.WEB®
с 1992 года

Контроль приложений Dr.Web

Ограничения по запуску программ могут быть назначены на отдельных пользователей, станции или группы.



Dr.WEB®
с 1992 года

Получив доступ в систему, злоумышленник загружал на сервер троянца-майнера и запускал его.
В дальнейшем расследование показало, что в планах злоумышленника был запуск шифровальщика

Заметили проблему – займитесь анализом или обращайтесь к нам!

Dr.WEB®
с 1992 года

Возможности технологий Dr.Web

Эвристический анализатор

Технология Origins Tracing

Модуль эмуляции исполнения

Технология Fly-Code

Комплексный анализатор упакованных угроз

Технология Script Heuristic

Технология анализа структурной энтропии
и много других технологий

Типичная проблема – отключение компонента вместо настройки антивируса

#CODEIB

Dr.WEB®
с 1992 года

В результате исследования этого носителя и используемых «Доктор Веб» ханипотов было обнаружено еще несколько эксплойтов. Было выявлено несколько видов ранее неизвестных антивирусу Dr.Web вредоносных программ и список жертв, атакованных аналогичным образом.
Среди пострадавших оказались пользователи самых разных антивирусных продуктов.
После анализа полученных исходных кодов нового вредоносного ПО вирусная база Dr.Web пополнилась новыми записями.

Dr.WEB®
с 1992 года

Выяснив какое ПО связано с активностью троянца, мы обратились к его разработчику, который передал нам для анализа НЖМД **руководителя** (!) своей разработки.

Именно там мы нашли исходники эксплойтов

Вывод. Доверяй, но проверяй. Увы, но если вы разработчик ПО, то всегда есть вероятность, что в вашем коллективе есть крыса. Анализируйте свое ПО на наличие недокументированного функционала. Репутация – ваше все

Dr.WEB®
с 1992 года

…до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

274.1 УК РФ

Виновный наказан?

Совместно с правоохранительными органами и разработчиком данного ПО, удалось установить злоумышленника и возбудить уголовное дело.

Dr.WEB®
с 1992 года

Самое главное:

Благодаря экспертизе, разработчику удалось закрыть уязвимость, переосмыслить подходы к разработке ПО с учетом текущих требований к информационной безопасности, установить соответствующий контроль за выпускаемой продукцией/услугой и предпринять соответствующие меры для недопущения подобных инцидентов в будущем.

Но стоит особо отметить, что в данном случае жертва еще «легко отделалась». Злоумышленник, получив доступ в систему, устанавливал туда троянца-майнера, который «всего лишь» сильно загружал ресурсы системы, не нанося прямого урона. Поскольку речь идёт о весьма специфическом ПО, которое обычно находится на том же сервере, что и, например, приложения типа 1С, ситуация могла развиваться иначе.

Dr.WEB®
с 1992 года

Если произошла нештатная ситуация (пропали деньги или данные, утекли пароли к корпоративным ресурсам, компьютеры работают с перебоями и т. д.) и вы предполагаете, что причина в действиях вредоносного ПО, закажите экспертизу ВКИ в компании «Доктор Веб».

Dr.WEB®
с 1992 года

Итого

…до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

274.1 УК РФ

Dr.WEB®
с 1992 года

…до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

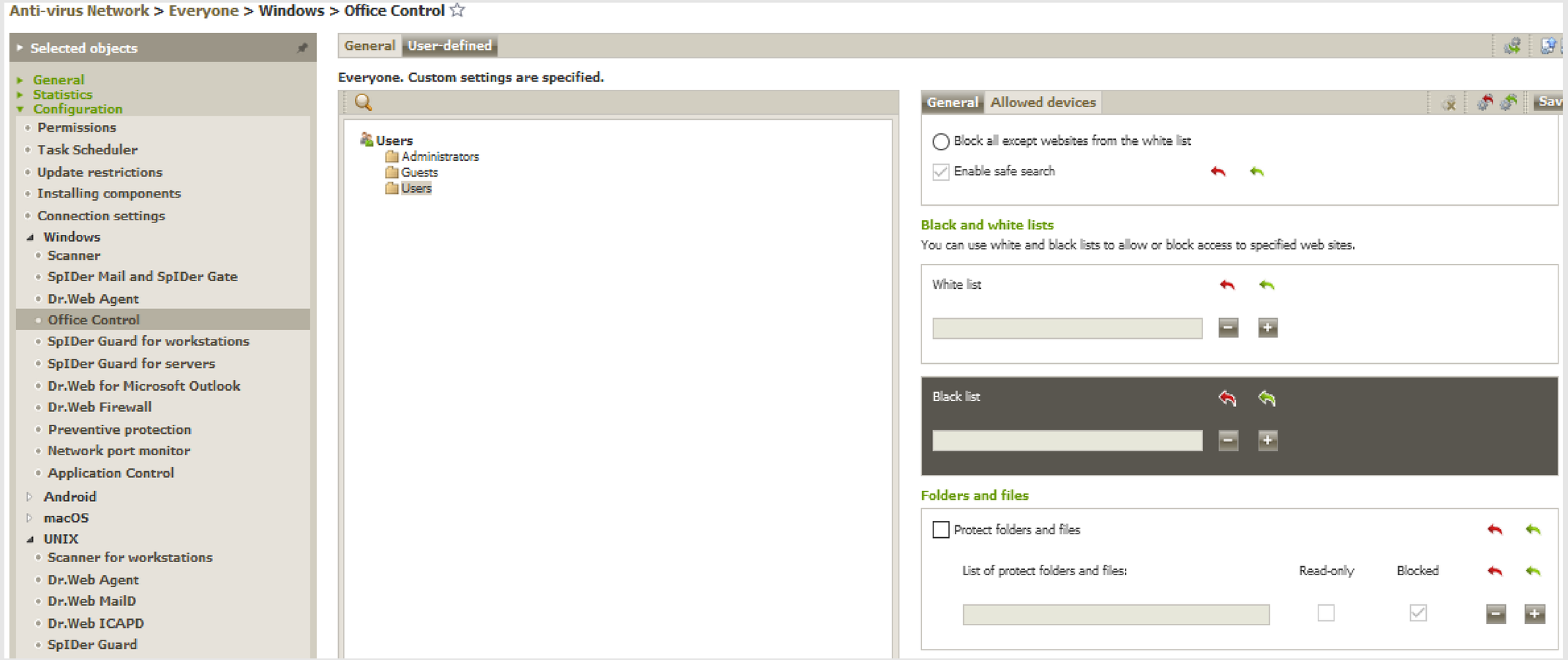
274.1 УК РФ

Для предотвращения инцидентов:

- ✓ Устанавливайте обновления
- ✓ Используйте белый список ПО
- ✓ Контролируйте изменений состава ПО
- ✓ Никаких админских прав у пользователей
- ✓ Надежные пароли, отличающиеся для пользователей и программ
- ✓ Централизованное управление защитой и/или пароль на доступ к антивирусу
- ✓ Минимум прав у пользователей
- ✓ Отключайте ненужные сервисы

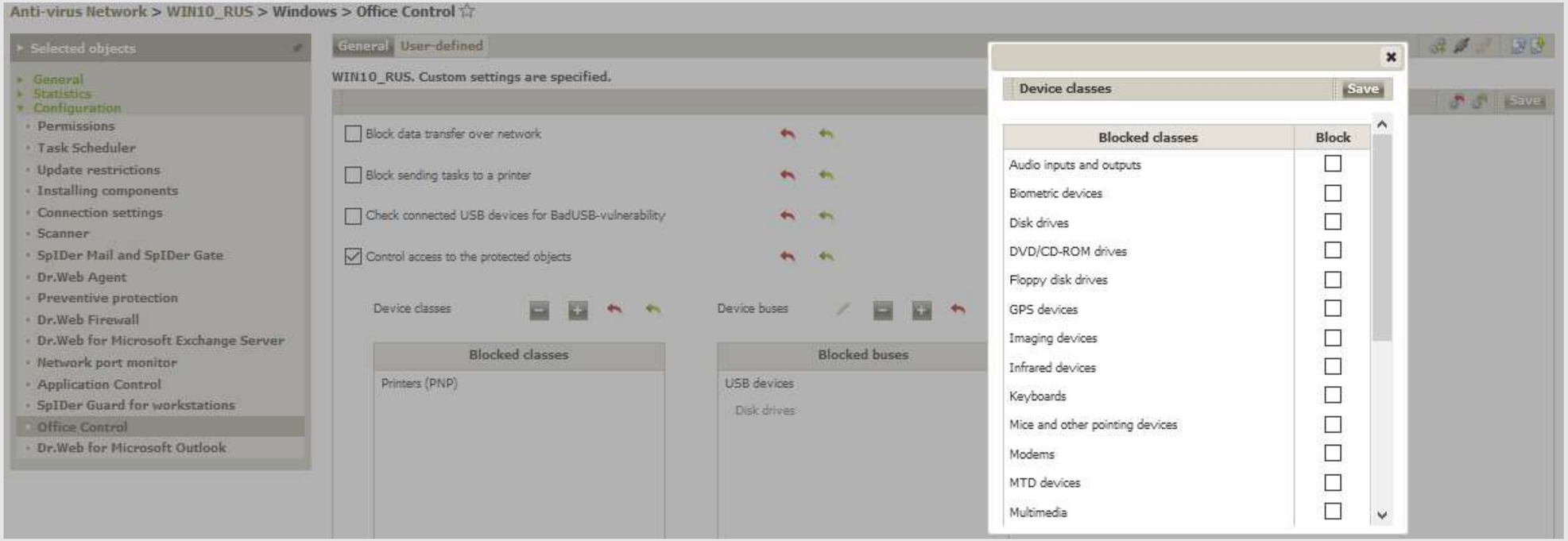
Dr.WEB®
с 1992 года

Офисный контроль



Dr.WEB®
с 1992 года

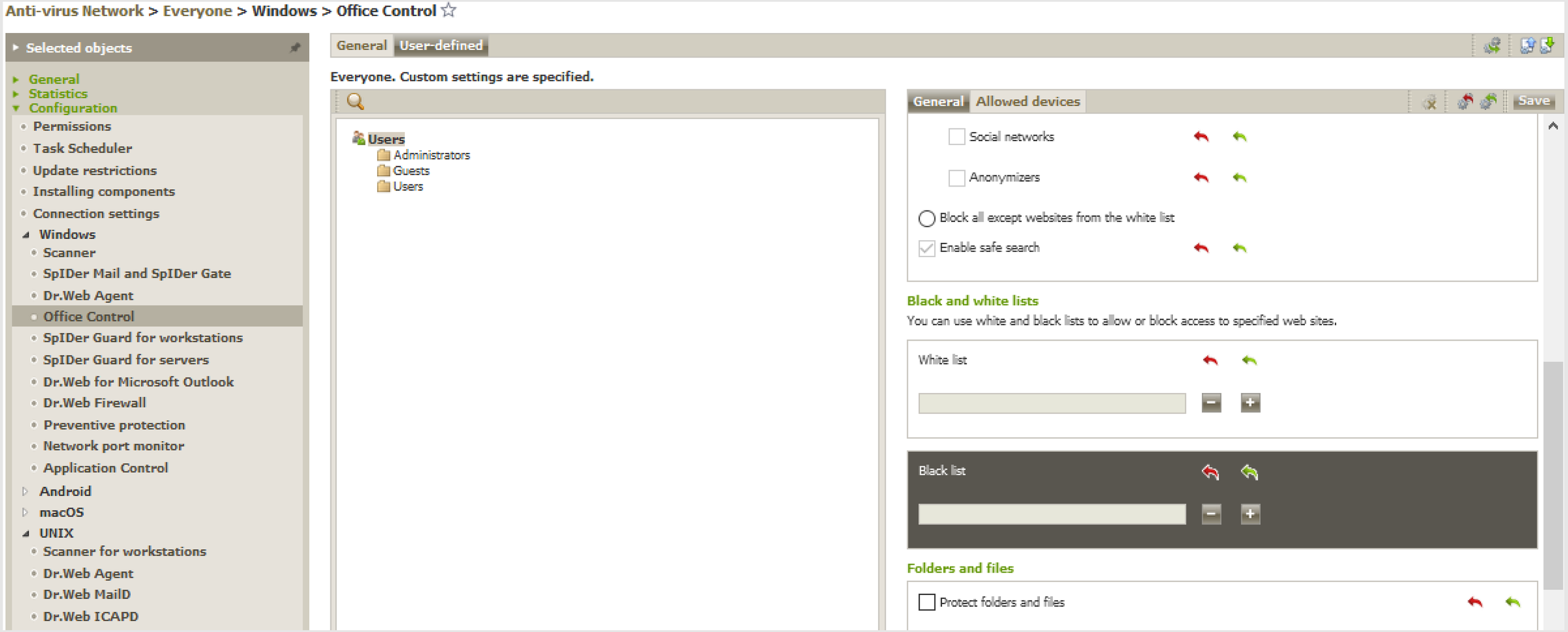
Предотвращение заражений через сменные носители



#CODEIB

Dr.WEB®
с 1992 года

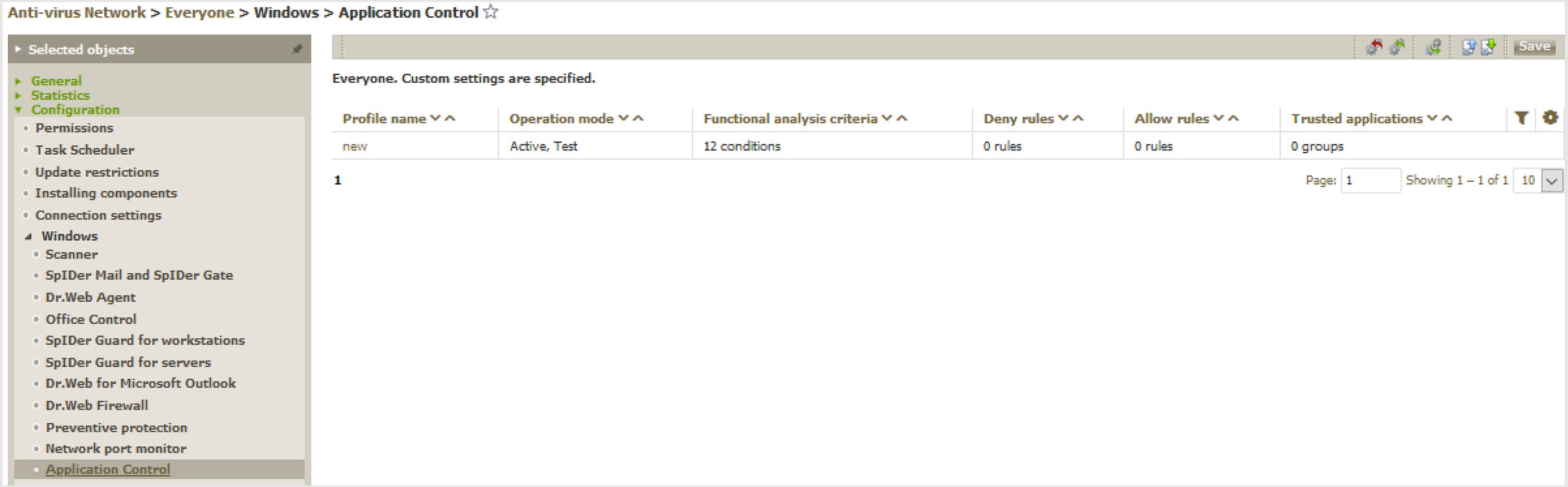
Ограничение доступа сотрудников к сайтам



#CODEIB

Dr.WEB®
с 1992 года

Контроль запуска программ пользователем



#CODEIB

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Благодарим за внимание!

Номер службы технической поддержки

8-800-333-7932

Запомнить просто! –
возникла проблема – набери DRWEB!

8-800-33-DRWEB

Убедитесь, что на ваших компьютерах нет вирусов

Dr.WEB®
с 1992 года

#CODEIB