КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАК защитить компанию от вредоносных программ? Современные технологии Dr.Web

Виталий БУГАЕВ
Доктор Веб

АНТИВИРУС НЕ НУЖЕН ?

«Да, антивирус делает что-то полезное, но в реальности он похож на канарейку в угольной шахте . . .»

Darren Bilby, Google
специалист по безопасности

«Антивирусы отравляют всю софтверную экосистему в целом, так как их инвазивный и плохо написанный код осложняет работу разработчиков браузеров и другого ПО, мешая им самим заниматься улучшением безопасности . . .»

Robert O'Callahan, Mozilla
экс-разработчик

«. . . если кто-то попытается их атаковать, то он, вероятно, будет использовать новую технику, которую пропустит большинство антивирусных продуктов . . .»

Jeremiah Grossman,
CTO White Hat Security

Современные вирусные угрозы

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОМПРОМЕТАЦИЯ
компьютерных систем

ХИЩЕНИЯ ДАННЫХ
БАНКОВСКИХ КАРТ

ВЫМОГАТЕЛЬСТВО
и/или порча информации

МОШЕННИЧЕСТВО

ХИЩЕНИЯ СРЕДСТВ
АУТЕНТИФИКАЦИИ
к системам ДБО
и платежным онлайн-системам

ХИЩЕНИЯ
ПРОПРИЕТАРНОГО
КОНТЕНТА

УЩЕРБ

БАНК РОССИИ ФИНЦЕРТ

ОБЪЁМ НЕСАНКЦИОНИРОВАННЫХ ОПЕРАЦИЙ в 2018 году:
платежные карты – 1,385 млрд. руб.
системы ДБО – 1,469 млрд. руб.

СБЕРБАНК

УБЫТКИ КОМПАНИЙ от кибератак:
2018 - $1,5 трлн.
2019 - $2,5 трлн. (прогноз)

WORLD ECONOMIC FORUM

СУММА ПЛАНЕТАРНОГО УЩЕРБА от кибератак вырастет **к 2022 году до $8 трлн**.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пути проникновения вирусных угроз в корпоративные сети

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 **ЭЛЕКТРОННАЯ ПОЧТА**

2 **ВЕБ-САЙТЫ**
Бесконтрольное посещение сотрудниками сайтов

3 **СЪЁМНЫЕ УСТРОЙСТВА**

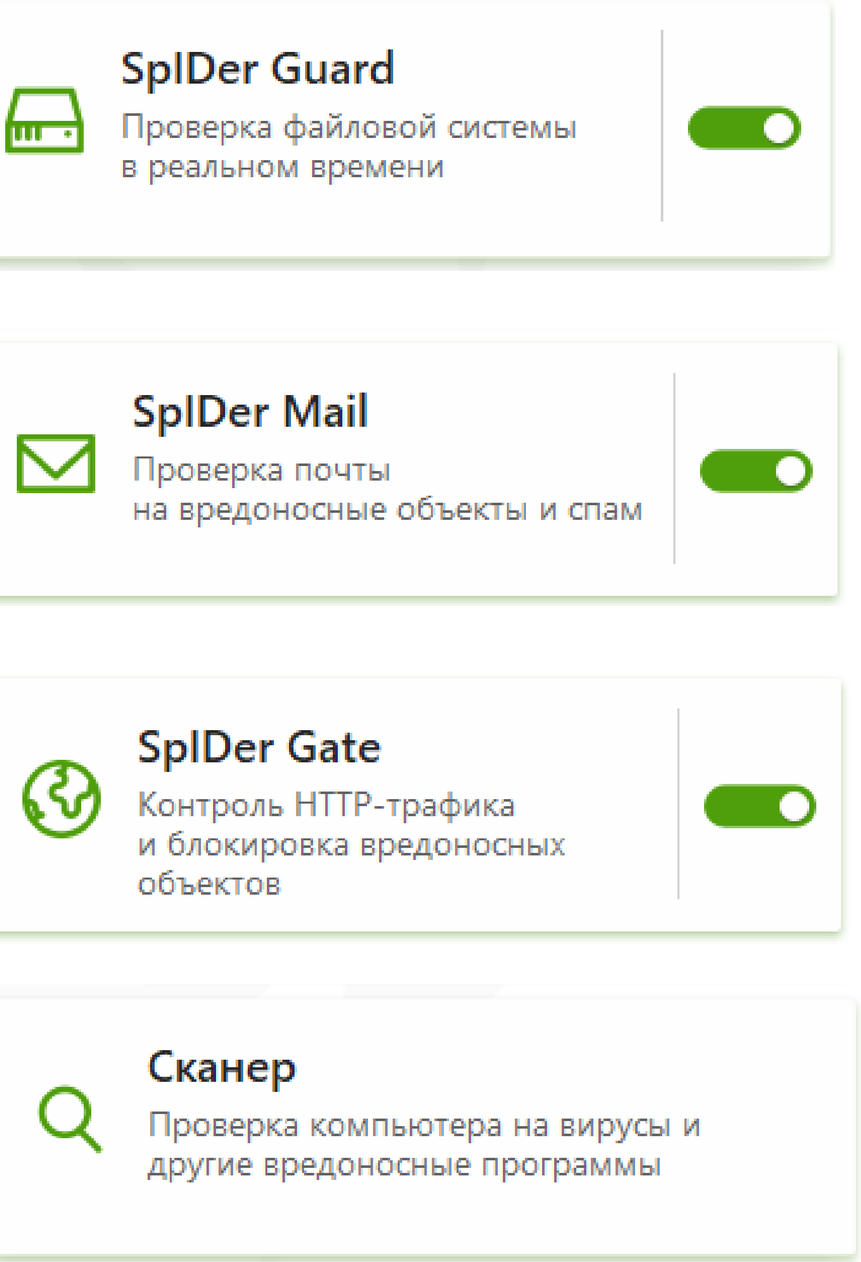
4 **УЯЗВИМОСТИ**
в программном обеспечении

5 **СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ**

6 **ЛИЧНЫЕ УСТРОЙСТВА СОТРУДНИКОВ**
в том числе мобильные

7 **ОШИБКИ**
в настройках антивирусной защиты

ОБЯЗАТЕЛЬНЫЕ КОМПОНЕНТЫ

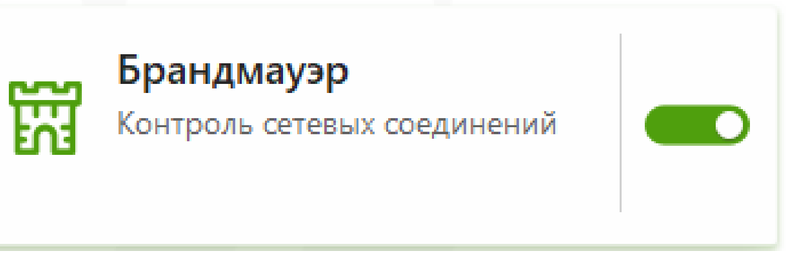


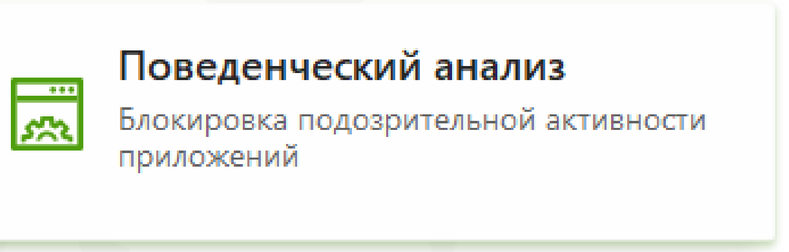
1

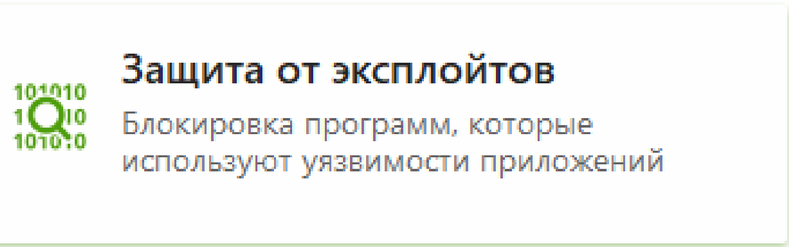
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

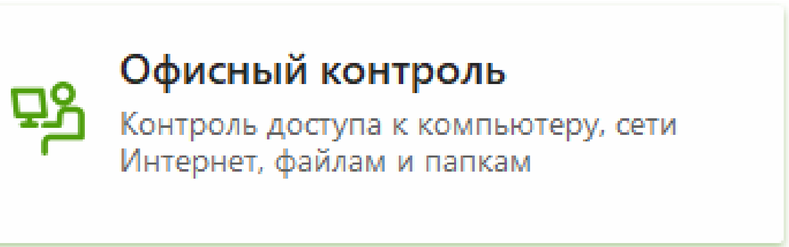
ОБЯЗАТЕЛЬНЫЕ КОМПОНЕНТЫ

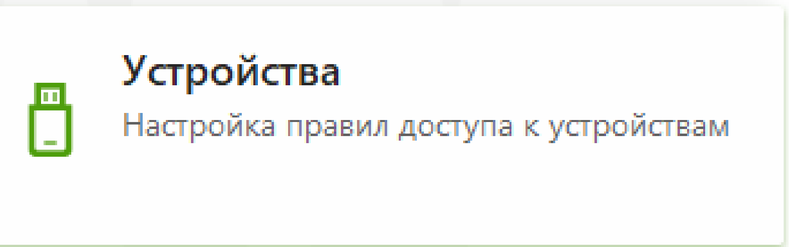
2











КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕХНОЛОГИИ НЕСИГНАТУРНОГО ОБНАРУЖЕНИЯ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 ЭВРИСТИЧЕСКИЙ АНАЛИЗАТОР

2 МОДУЛЬ ЭМУЛЯЦИИ ИСПОЛНЕНИЯ

3 КОМПЛЕКСНЫЙ АНАЛИЗАТОР УПАКОВАННЫХ УГРОЗ

4 АНАЛИЗ СТРУКТУРНОЙ ЭНТРОПИИ

5 ORIGINS TRACING

6 FLY-CODE

7 SCRIPT HEURISTIC

8 ТЕХНОЛОГИИ МАШИННОГО ОБУЧЕНИЯ

ТЕХНОЛОГИИ ПРЕВЕНТИВНОЙ ЗАЩИТЫ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Dr.WEB PROCESS HEURISTIC
анализ поведения каждой запущенной программы «на лету»

Dr.WEB SHELL GUARD
защита от эксплойтов, в том числе уязвимостей «нулевого дня»

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНОВЛЕНИЯ Dr.Web SHELL GUARD

ЦЕНТР УПРАВЛЕНИЯ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Dr.WEB | Администрирование | Антивирусная сеть | Избранное | admin | Выход

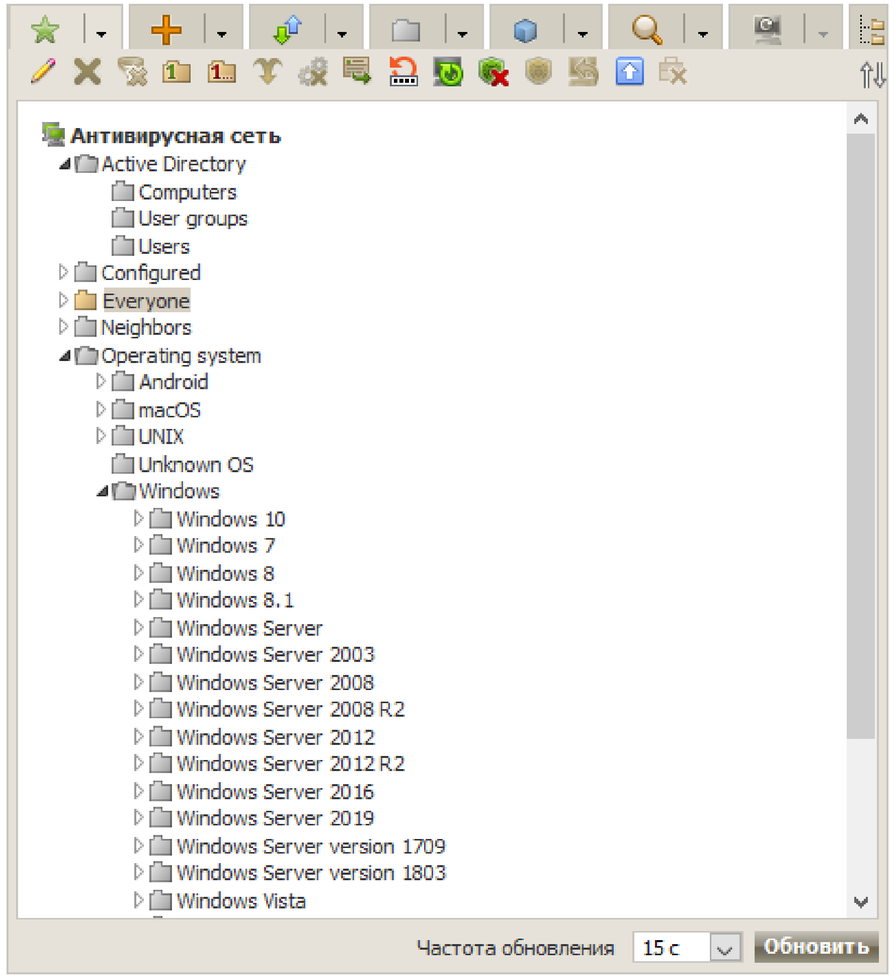
Антивирусная сеть

Выбранные объекты

Everyone

Общие
- Графики
- Идентификаторы безопасности
- Компоненты защиты
- Карантин
- Оборудование и программы
- Обнаруженные устройства
- Сессии пользователей
- Неактивные станции
- Свойства

Статистика
- Угрозы
- Ошибки
- Сводные данные
- Статистика сканирования
- Запуск/Завершение
- Статистика угроз
- Состояние
- Задания
- Заблокированные устройства
- Продукты
- События Превентивной защиты
- События Контроля приложений
- Инсталляции Агентов
- Деинсталляции Агентов



Свойства группы Everyone

Общие

Идентификатор*	20e27d73-d21d-b211-a788-85419c46f0e6
Название*	Everyone
Родительская группа	Нет родительской группы
Описание	All stations

Сведения о станциях

Всего станций	1
Первичная группа для	1
Станций в сети	1
Расположение	Нет объектов для отображения на карте

Конфигурация

Права. Заданы персональные настройки.

Планировщик заданий. Заданы персональные настройки.

Лицензионные ключи. Заданы персональные настройки.

Ограничения обновлений. Заданы персональные настройки.

16:29 11-10-2019 (UTC +6:00) | 00.843, 00.203 CPU

КАК защитить компанию от вредоносных программ?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 **ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ**
защитой всех узлов корпоративной сети, из любой точки сети Интернет

2 **КОМПЛЕКСНАЯ АНТИВИРУСНАЯ ЗАЩИТА**
по всем направлениям возможного проникновения вирусных угроз

3 **ДОПОЛНИТЕЛЬНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ**
кроме сигнатурных и эвристических

4 **СИСТЕМА ОГРАНИЧЕНИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ**
к ресурсам сети Интернет, подключенным устройствам, файлам и папкам

5 **ОГРАНИЧЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЕЙ**
на отключение антивируса, обновление баз и модулей, вплоть до полного запрета

6 **ЗАЩИТА ЛИЧНЫХ УСТРОЙСТВ ПОЛЬЗОВАТЕЛЕЙ**

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!

v.bugaev@drweb.kz
+7 727 323-6-232
www.drweb.ru