



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

**ESET – НОВЫЕ РЕАЛИИ.
НОВЫЕ РЕШЕНИЯ.
НОВЫЕ ВОЗМОЖНОСТИ.**

Сергей Фёдоров
ESET Russia



ТРИ СТОЛПА РЕШЕНИЙ ESET NOD32

7-ОЕ ПОКОЛЕНИЕ КОРПОРАТИВНЫХ ПРОДУКТОВ ESET



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

КОМПЛЕКСНЫЕ РЕШЕНИЯ ESET NOD32 ДЛЯ ЗАЩИТЫ ОРГАНИЗАЦИЙ ЛЮБЫХ МАСШТАБОВ



НАДЕЖНОСТЬ

БЫСТРОДЕЙСТВИЕ

УДОБСТВО В РАБОТЕ

НАДЕЖНОСТЬ! 7-ОЕ ПОКОЛЕНИЕ

МНОГОУРОВНЕВАЯ ЗАЩИТА ТЕХНОЛОГИЯМИ ESET.

АКТИВНЫ ПОСТОЯННО



ОБНАРУЖЕНИЕ
И БЛОКИРОВАНИЕ
ПО ПОВЕДЕНИЮ (HIPS)



ESET LIVE GRID



МАШИННОЕ ОБУЧЕНИЕ

NEW



ЗАЩИТА ОТ
ШИФРАТОРОВ



РАСШИРЕННОЕ
СКАНИРОВАНИЕ
ПАМЯТИ



ОБЛАЧНАЯ СИСТЕМА
ЗАЩИТЫ



ЗАЩИТА
ОТ БОТНЕТОВ

NEW



СКАНЕР UEFI



ЗАЩИТА
ОТ СЕТЕВЫХ АТАК



РЕПУТАЦИЯ
И КЭШ



ПЕСОЧНИЦА



ДНК СИГНАТУРЫ



ЗАЩИТА
ОТ ЭКСПЛОЙТОВ

ДО ВЫПОЛНЕНИЯ УГРОЗЫ

ПОСЛЕ ВЫПОЛНЕНИЯ УГРОЗЫ



**Расширенная защита
рабочих станций
(ESET Endpoint Security)**



**Защита рабочих станций
(ESET Endpoint Antivirus)**



Антивирус	●	●
Антишпион	●	●
Антифишинг	●	●
Файервол	●	●
Защита от сетевых атак	●	●
Антиспам	●	●
Контроль устройств	●	●
Веб-контроль	●	●
HIPS	●	●
Защита от ботнетов	●	● <i>new</i>
Защита от эксплойтов	●	●
Защита от шифраторов	● <i>new</i>	● <i>new</i>
Сканер UEFI	● <i>new</i>	● <i>new</i>



ESET ENDPOINT SECURITY ESET ENDPOINT ANTIVIRTUS

- ✓ Поддержка *ESET Dynamic Threat Defense* -
- ✓ *Планировщик* для контроля устройств и веб-контроля



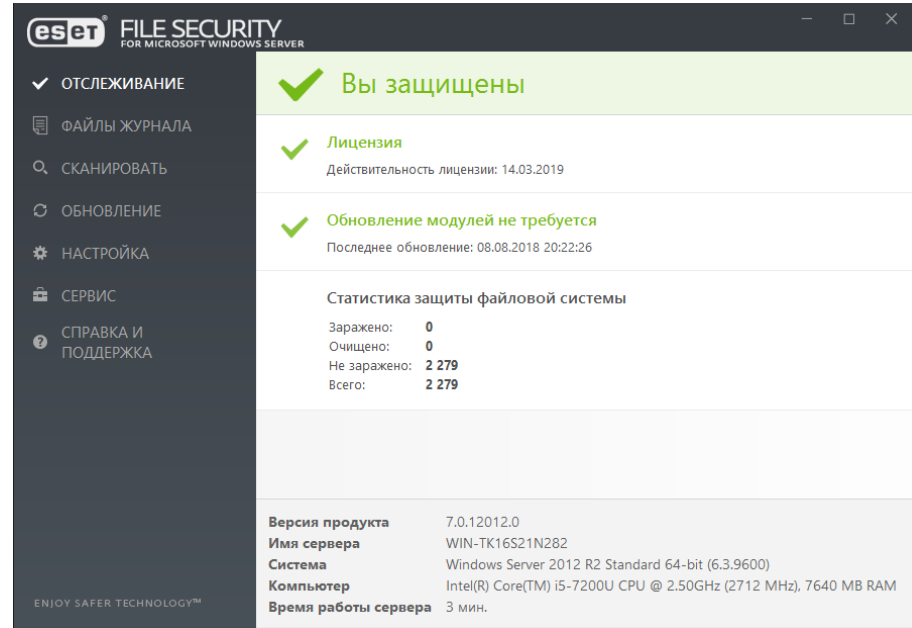
The image shows two overlapping windows from the ESET software suite. The top window is titled "eset ENDPOINT ANTIVIRUS" and displays the "Обновление" (Update) section. It shows a green checkmark for "ESET Endpoint Antivirus" with the current version "7.0.2066.0". Below this, it indicates that the last successful update was completed and that the next update check is scheduled.

The bottom window is titled "eset ENDPOINT SECURITY" and displays the "Состояние защиты" (Protection Status) section. It features a large green banner with the text "Вы защищены" (You are protected). Below the banner, it shows a green checkmark for "Лицензия" (License) with the note "Действительность лицензии: Продление каждый месяц (автоматическое продление)" (License validity: Renewal every month (automatic renewal)). Another green checkmark is shown for "Обновление модулей не требуется" (Module updates not required) with the note "Последнее обновление: 08.08.2018 18:31:51" (Last update: 08.08.2018 18:31:51).

Both windows have a dark sidebar on the left with navigation icons and labels: СОСТОЯНИЕ ЗАЩИТЫ, СКАНИРОВАНИЕ КОМПЬЮТЕРА, ОБНОВЛЕНИЕ, НАСТРОЙКА, СЕРВИС, СПРАВКА И ПОДДЕРЖКА. The ESET logo and "ENJOY SAFER TECHNOLOGY™" are visible at the bottom of the windows.

ESET FILE SECURITY ДЛЯ WINDOWS SERVER

- ✓ Поддержка Microsoft **Office 365**
- ✓ Защита от сетевых атак (IDS)
- ✓ Поддержка **ESET Dynamic Threat Defense**
- ✓ Добавление исключений по **хэшу файлов**
- ✓ **64-битное** ядро сканирования



ESET MAIL SECURITY ДЛЯ EXCHANGE SERVER

- ✓ *Уведомление администратора о карантине*
- ✓ *Защита Backscatter*
- ✓ *Поддержка Microsoft Office 365*
- ✓ *Защита от сетевых атак (IDS)*
- ✓ *Поддержка ESET Dynamic Threat Defense*

ESET MAIL SECURITY ДЛЯ IBM DOMINO

- ✓ *Защита от Backscatter*
- ✓ *Поддержка ESET Dynamic Threat Defense*
- ✓ *64-битное ядро сканирования*



The screenshot displays the ESET Mail Security interface for Microsoft Exchange Server. The top window shows the 'Статистика системы защиты' (System Protection Statistics) window, which lists various protection modules and their status. The bottom window shows the 'MONITORING' (Мониторинг) section, which displays the overall protection status as 'Maximum protection' (Максимальная защита) and provides details about the license, virus signature database, and system protection statistics.

Module	Status
Защита от вирусов и шпионских программ	Active
Защита файловой системы	Active
Защита почтового клиента	Active
Защита почтового сервера	Active
Защита доступа в Интернет и защита от фишинга	Active
Защита почтового сервера от спама	Active

Category	Value
Overall Status	Maximum protection
License	Valid until: 12/30/2016
Virus Signature Database	The virus signature database is up to date Last update: 2/18/2016 1:52:06 PM
File System Protection Statistics	Infected: 0 Cleaned: 0 Clean: 400,833 Total: 400,833
Product version	6.4.14007.0
Server name	W2008R2-LOTUS
System	Windows Server 2008 R2 Standard 64-bit (6.1.7600)
Computer	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz (2800 MHz), 2048 MB RAM
Server uptime	1 day, 4 minutes
Mailbox count	0

БЫСТРОДЕЙСТВИЕ

ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

- Высокая скорость работы на любых устройствах, включая устаревающее оборудование
- Минимальное влияние на производительность системы



УДОБСТВО В РАБОТЕ

- Простота внедрения и настройки
- Понятная и простая навигация благодаря единому стилю всех решений
- Централизованное управление безопасностью
- Отсутствие навязчивых окон и диалогов

NEW





REMOTE ADMINISTRATOR

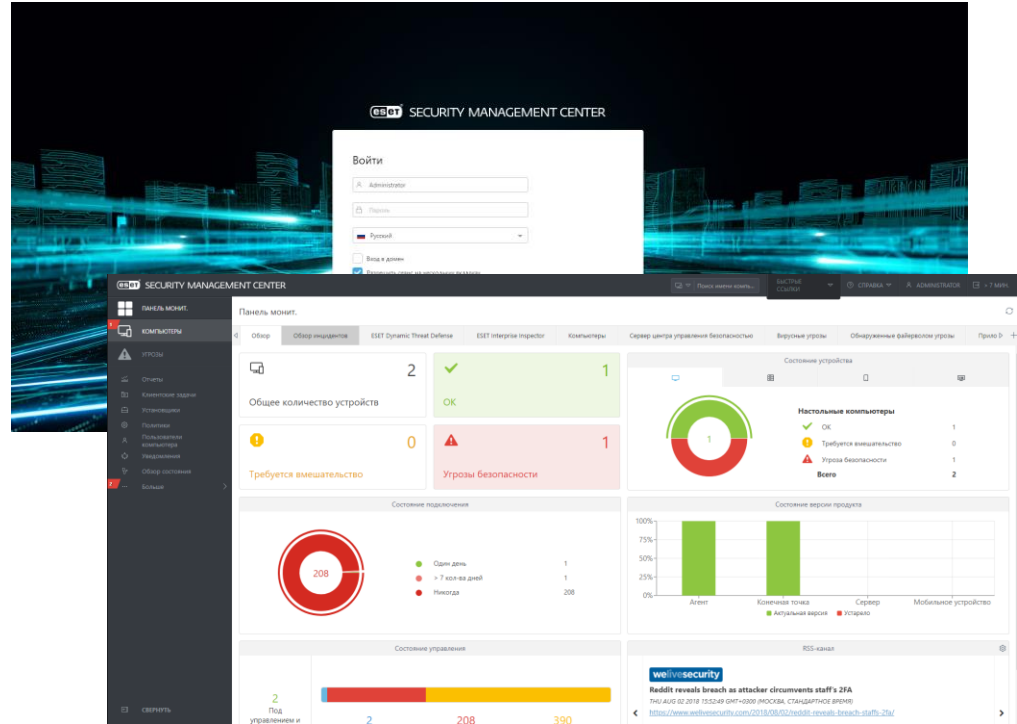


SECURITY MANAGEMENT CENTER

NEW

ESET SECURITY MANAGEMENT CENTER

- ✓ ESET Push Notification Service (EPNS)
- ✓ Автоматическое определение «клонов»
- ✓ Инвентаризация оборудования
- ✓ Поддержка ESET Enterprise Inspector
- ✓ Поддержка ESET Dynamic Threat Defense



ESET SECURITY MANAGEMENT CENTER

✓ Инвентаризация оборудования

The screenshot shows the ESET Security Management Center interface. The left sidebar contains navigation options: ПАНЕЛЬ МОНИТ., КОМПЬЮТЕРЫ, УРОЗЫ, Отчеты, Контекстные задачи, Установщики, Политики, Пользователи компьютера, Уведомления, Обзор состояния, and Больше. The main area is titled 'Панель мониторинга' and displays several data panels:

- Компьютеры с соответствующими сведениями:** A table listing computers with columns for Name, Manufacturer, Model, and Serial Number.
- Компьютеры со сведениями о ЦП:** A table listing computers with columns for Name, Manufacturer, Description, and Number of Cores.
- Компьютеры со сведениями об ОЗУ:** A table listing computers with columns for Name, Grouped by architecture, and Total memory in MB.
- Число компьютеров, сгруппированных по общей архитектуре:** A donut chart showing 4 computers grouped by architecture.

The screenshot shows the hardware details for a selected computer. The top navigation bar includes '< НАЗАД', 'Компьютеры', and navigation icons. The left sidebar contains: ОБЗОР, КОНФИГУРАЦИЯ, ЖУРНАЛЫ, ВЫПОЛНЕНИЯ ЗАДАЧИ, УСТАНОВЛЕННЫЕ ПРИЛОЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ, ВОПРОСЫ, УРОЗЫ И КАРАНТИН, and ПОДРОБНОСТИ. The main area is titled 'Оборудование' and displays hardware details for a Lenovo PBAK414 computer:

- Устройство:** Lenovo PBAK414 (Manufacturer: LENOVO, Model: 4180PUG, Serial number: PBAK414).
- CPU:** Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz (Description: Intel(R) Core(TM)... 2, Number of cores: 2, Logical processors: 4, Architecture: x64, Manufacturer: GenuineIntel).
- RAM:** 8 GiB (Capacity: 8 GiB, Frequency: 1333 MHz, Manufacturer: Kingston, Description: Physical Memory, Architecture: Unknown).
- Хранилище:** Physical disk drive (Type: Физический дисковый накопитель, Description: INTEL SSDSC2BW480A4 SCSI Disk Device, Capacity: 447 GiB, Serial number: PHDA410301PH4805GN, Manufacturer: (Стандартные дисковые накопители)).

Новые продукты

NEW



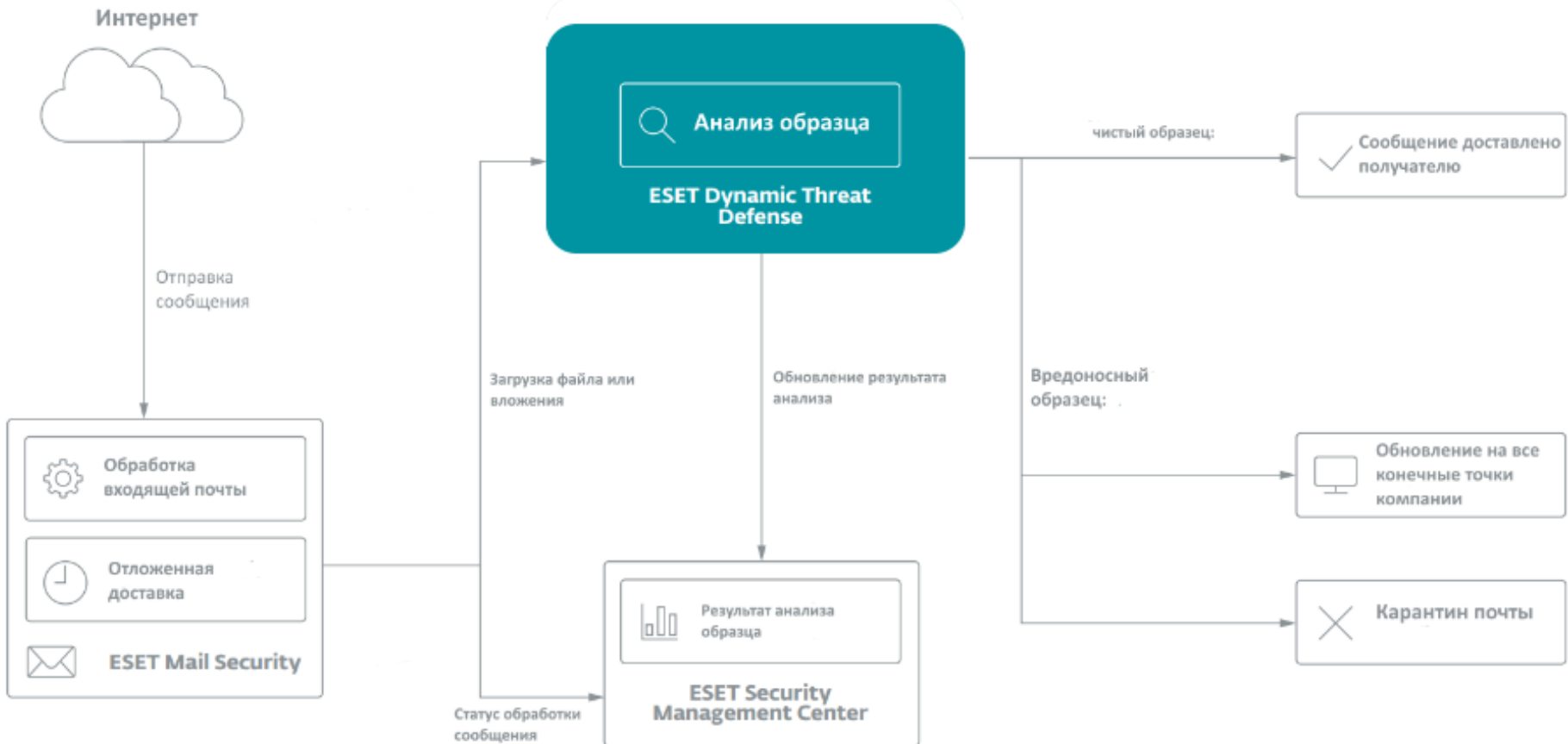
DYNAMIC THREAT DEFENSE

ESET DYNAMIC THREAT DEFENSE

- ✓ **Облачная** песочница, встроенная в антивирус
- ✓ **Автоматическая** защита
- ✓ **Многоуровневое** обнаружение угроз

Эффективен против шифраторов

- ✓ **E-mail** до сих пор основной способ доставки
- ✓ **Несколько уровней** более эффективны



ESET DYNAMIC THREAT DEFENSE

ПОДДЕРЖИВАЕМЫЕ ПРОДУКТЫ

ESET Endpoint Antivirus	версия 7 или новее
ESET Endpoint Security	версия 7 или новее
ESET Mail Security	версия 7 или новее
ESET File Security для Windows Server	версия 7 или новее



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



ENTERPRISE INSPECTOR

NEW

ESET ENTERPRISE INSPECTOR: КАК РАБОТАЕТ



- ✓ **Собирает информацию** в режиме реального времени
- ✓ Обеспечивает **фильтрацию и сортировку**
- ✓ Позволяет создавать **собственные правила**
- ✓ Использует систему репутаций **ESET LiveGrid**

ESET ENTERPRISE INSPECTOR



Обнаружение

Поиск вредоносных
аномалий



Отображение

Что затронуто?
Когда это произошло?
Как это произошло?



Реагирование

Блокировать
Удалить

ESET ENTERPRISE INSPECTOR: ПРЕИМУЩЕСТВА В КЛАССЕ EDR



- ✓ **Простое** внедрение, интеграция, использование
- ✓ **Проактивный** поиск и обнаружение угроз
- ✓ Сочетание **поведенческого анализа и репутационной эвристики**
- ✓ **Интуитивно понятные** уведомления и простое реагирование на инциденты
- ✓ **Многоуровневые** технологии защиты

ВНУТРЕННИЕ УГРОЗЫ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

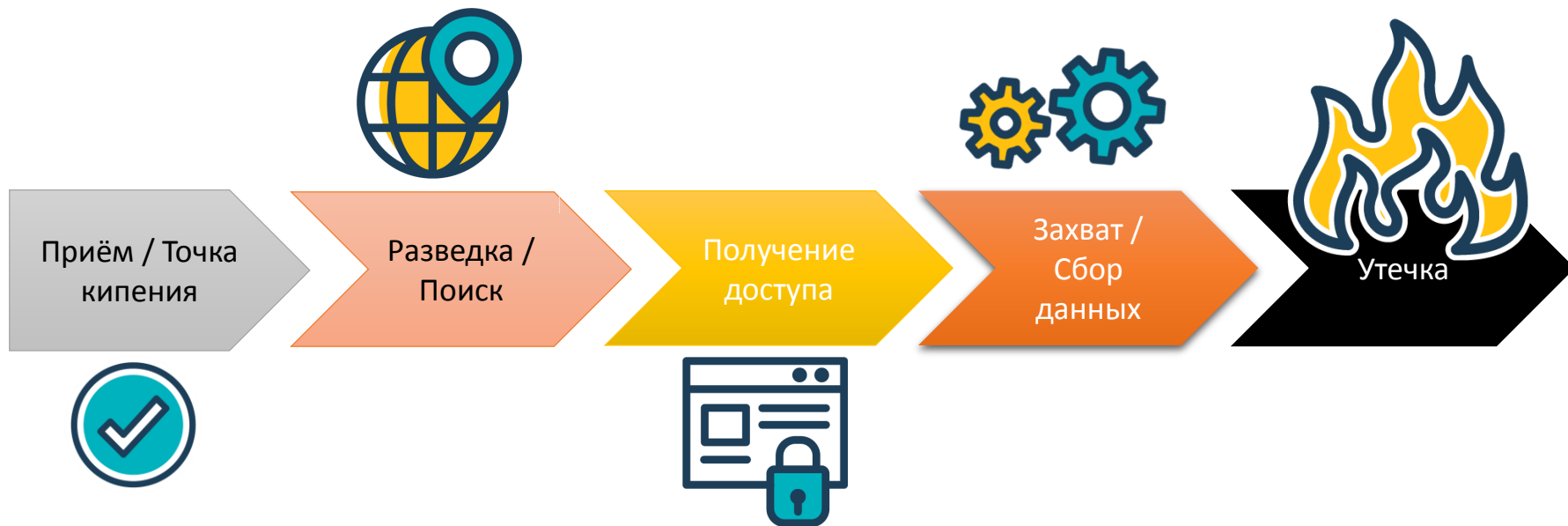
ЧЕЛОВЕЧЕСКИЙ ФАКТОР

С ЧЕГО НАЧИНАЕТСЯ ПРОЦЕСС НАНЕСЕНИЯ УЩЕРБА КОМПАНИИ?

- Приём на работу сотрудника. (некомпетентность, проблемы эффективности)
- Доведение сотрудника(инсайдера) до точки кипения (конфликт, не желание работать, отсутствие доп. мотивации, желание открыть свое дело, новое место работы и др.)

*63% инцидентов информационной безопасности в компаниях связано с бывшими и действующими сотрудниками**

ЧТО ДАЛЬШЕ КАКИЕ СЛЕДУЮТ ДЕЙСТВИЯ?



УТЕЧКА ДАННЫХ

КАК ЭТО ПРОИСХОДИТ?

- USB-флешки / телефоны / внешние жесткие диски
- DropBox / и другие облачные хранилища
- Электронная почта
- Различные приложения
- Мессенджеры
- Bluetooth
- ...



ЧЕЛОВЕЧЕСКИЙ ФАКТОР-KILL CHAIN КАК ЗАЩИТИТЬСЯ?

ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA

- ST-Чешская компания, основана в 2009 году
- Клиенты в более чем 50 странах
- Продукт входит в TOP 5 DLP - в рейтинге журнала SC Magazine
- DLP решение для любого типа бизнеса - по версии Gartner
- Входит в ESET Technology Alliance с 2016 года

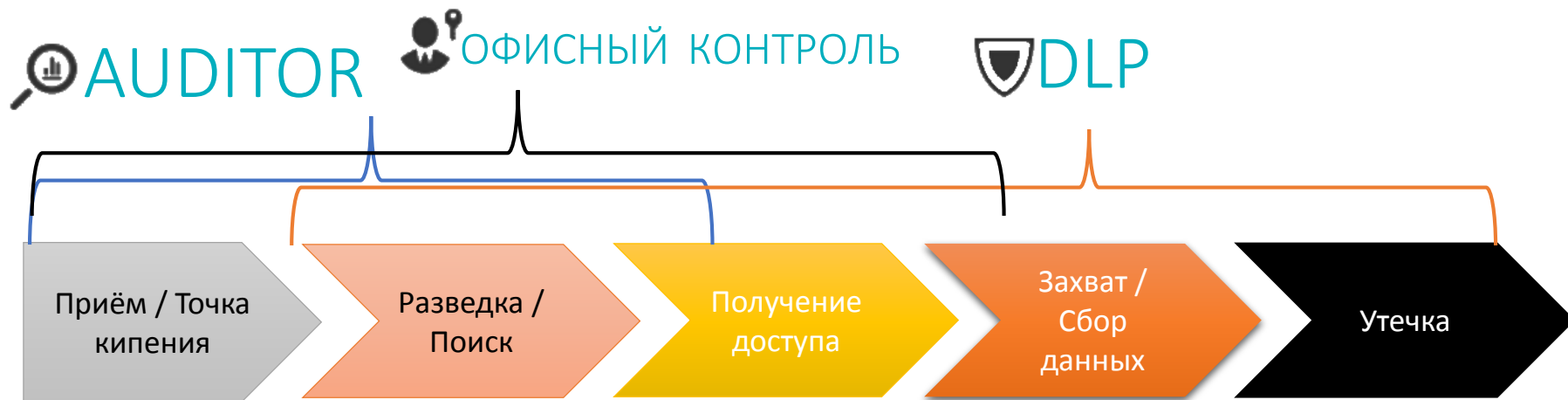


SAFETICA – КОМПЛЕКСНОЕ РЕШЕНИЕ!

61% сотрудников

*злоупотребляет доступом к конфиденциальным
данным компании**

** Ponemon Institute, 2016*



ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)



АУДИТ
ЧУВСТВИТЕЛЬНЫХ
ДАННЫХ КОМПАНИИ



ПРЕДСТАВЛЕНИЕ О
ТОМ, ЧТО ПРОИСХОДИТ
В КОМПАНИИ



УМЕНЬШЕНИЕ
РАСХОДОВ НА
ПЕРСОНАЛ



ПОВЫШЕНИЕ
ЭФФЕКТИВНОСТИ
СОТРУДНИКОВ



СОКРАЩЕНИЕ
РАСХОДОВ КОМПАНИИ
НА ОФИСНЫЕ НУЖДЫ!



СРАВНЕНИЕ РАБОТЫ
СОТРУДНИКОВ



СОБЛЮДЕНИЕ ПОЛИТИК
БЕЗОПАСНОСТИ



ОКУПАЕМОСТЬ
ВНЕДРЕНИЯ



ЭФФЕКТИВНОСТЬ
ИСПОЛЬЗОВАНИЯ ПО



ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ SUPERVISOR)



WEB-КОНТРОЛЬ

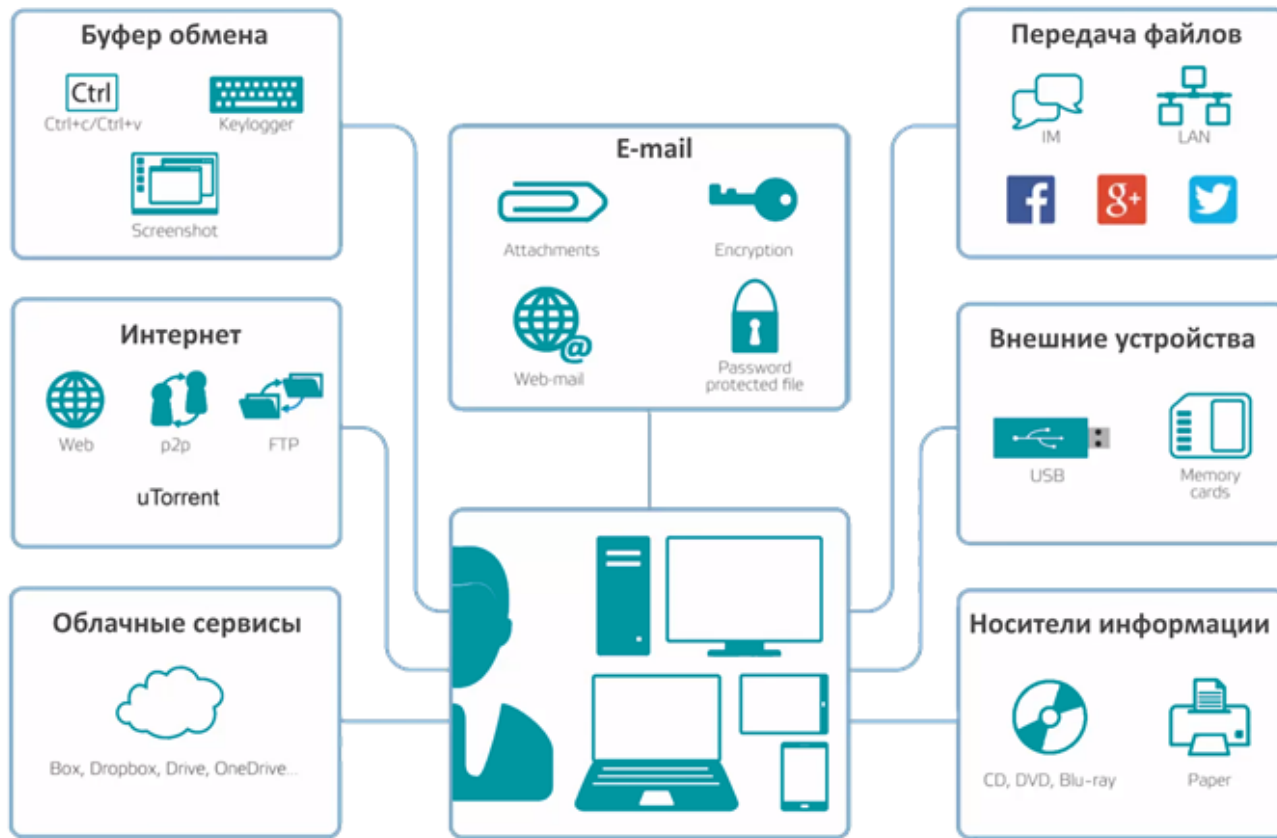


КОНТРОЛЬ ПРИЛОЖЕНИЙ



КОНТРОЛЬ ПЕЧАТИ

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА



safetica

КОНТЕКСТНЫЙ ФИЛЬТР

1. ЭФФЕКТИВНО И ПРОСТО
2. БЕЗ ЛОЖНЫХ СРАБАТЫВАНИЙ
3. ЗАЩИЩАЕТ ДОКУМЕНТ ПО РАСШИРЕНИЮ, А НЕ ПО СОДЕРЖИМОМУ

В 12В14

ABC

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)

› ПРАВИЛА ПРИЛОЖЕНИЙ

Определение приложений и категорий приложений, в которых выходные файлы должны быть помечены выбранной категорией данных

› ПРАВИЛА ПО ПУТИ

Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.

› ВЕБ ПРАВИЛА

Веб-правила могут использоваться для установки меток на файлы, загруженные с определенных доменов или доменов из определенной категории

› КОНТЕНТНЫЕ ПРАВИЛА

Все файлы, содержащие определенный контент, будут автоматически получать необходимую метку.

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

- ЭЛЕКТРОННАЯ ПОЧТА
- МЕССЕНДЖЕРЫ
- ВНЕШНИЕ УСТРОЙСТВА
- ЗАГРУЗКА ФАЙЛОВ В ИНТЕРНЕТ

^ КОНТРОЛЬ ЭЛЕКТРОННОЙ ПОЧТЫ

Вложения для почтовых клиентов

Отправка любых вложений из почтовых клиентов (кроме изображений): Уведомлять

Отправка веб-почты с вложениями

Загрузка файлов на веб-сайты, классифицированные как веб-почта: Запретить

Конфиденциальные данные

Отправка конфиденциальных данных из почтовых клиентов: Запретить

Безопасная Зона

Отправка вложений на домены Безопасной Зоны электронной почты : Всегда разрешено

^ КОНТРОЛЬ ВНЕШНИХ УСТРОЙСТВ

Передача файлов на внешние устройства

Передача файлов на внешние устройства: Уведомлять

Конфиденциальные данные

Передача файлов, содержащих конфиденциальные данные: Запретить



Передача чувствительных данных может быть определена только для операций копирования / перемещения

Разрешить файловые операции, кроме копирования / перемещения: Нет

Безопасная Зона

Передача файлов на устройства из Безопасной Зоны: Всегда разрешено



ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР В НОВОЙ ВЕРСИИ ПРОДУКТА)

› ПРЕДУСТАНОВЛЕННОЕ СОДЕРЖИМОЕ

Идентификационные номера и номера социального страхования различных стран, номера кредитных карт, номера банковских счетов.

› КЛЮЧЕВЫЕ СЛОВА И РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

Любые слова и словосочетания, использование регулярных выражений с применением синтаксиса ECMAScript

› МЕТАДААННЫЕ СТОРОННИХ КЛАССИФИКАТОРОВ

Протестирована поддержка метаданных Microsoft Azure Information Protection, Boldon James, Tukan GREENmod.



КЕЙСЫ

ПРОЕКТЫ!

ПРОИЗВОДСТВО

НЕФТЬ И ГАЗ

СТРАХОВАНИЕ

ЛОГИСТИКА

ФИНАНСОВЫЙ СЕКТОР

ГОСУДАРСТВЕННЫЙ СЕКТОР

ПРОЕКТИРОВАНИЕ

МЕДИЦИНА

ТОРГОВЛЯ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA

НАШИ ПРЕИМУЩЕСТВА:

1. **Внедрение решения** от несколько дней до 8 недель
2. **Выявление инсайдеров благодаря модульной структуре** продукта на всех этапах работы с информацией (Auditor, Supervisor, DLP)
3. **Полноценное DLP решение с агентной архитектурой**
4. **Не требуются серверов с высокими вычислительными мощностями**
5. **Проводит оценку** эффективности сотрудников
6. **Успешно прогнозирует** инциденты безопасности
7. **Точный мониторинг времени**
8. **Оптимальная стоимость**



ПАРОЛИ ПИШЕМ ИЛИ ЗАПОМИНАЕМ?



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

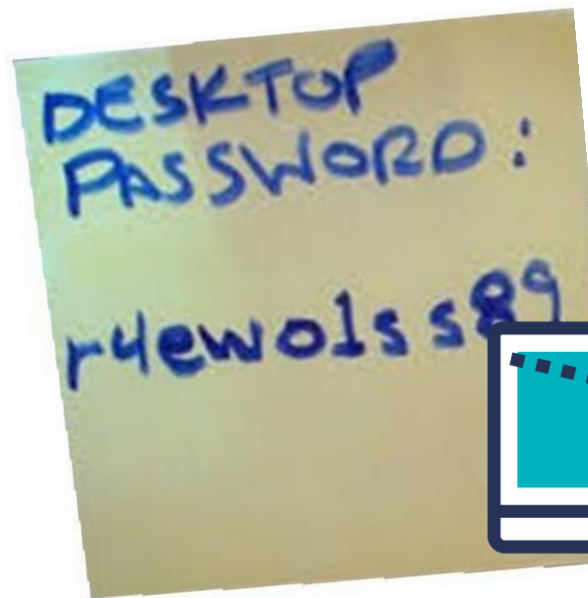
w#hN02v)b56

1234567890

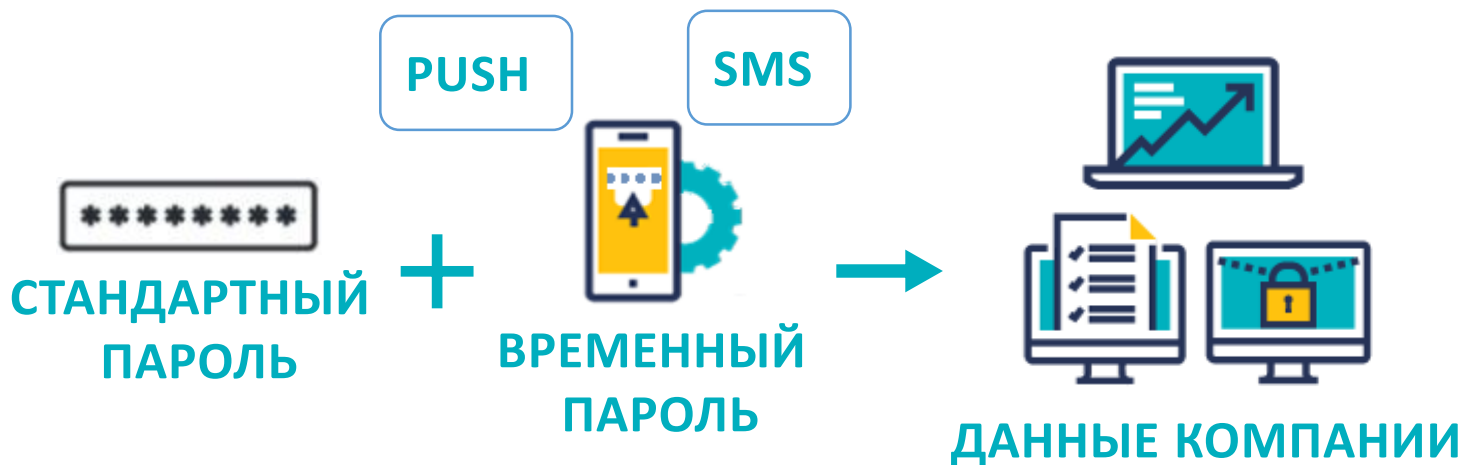
0987654321

Password123

Marina1990

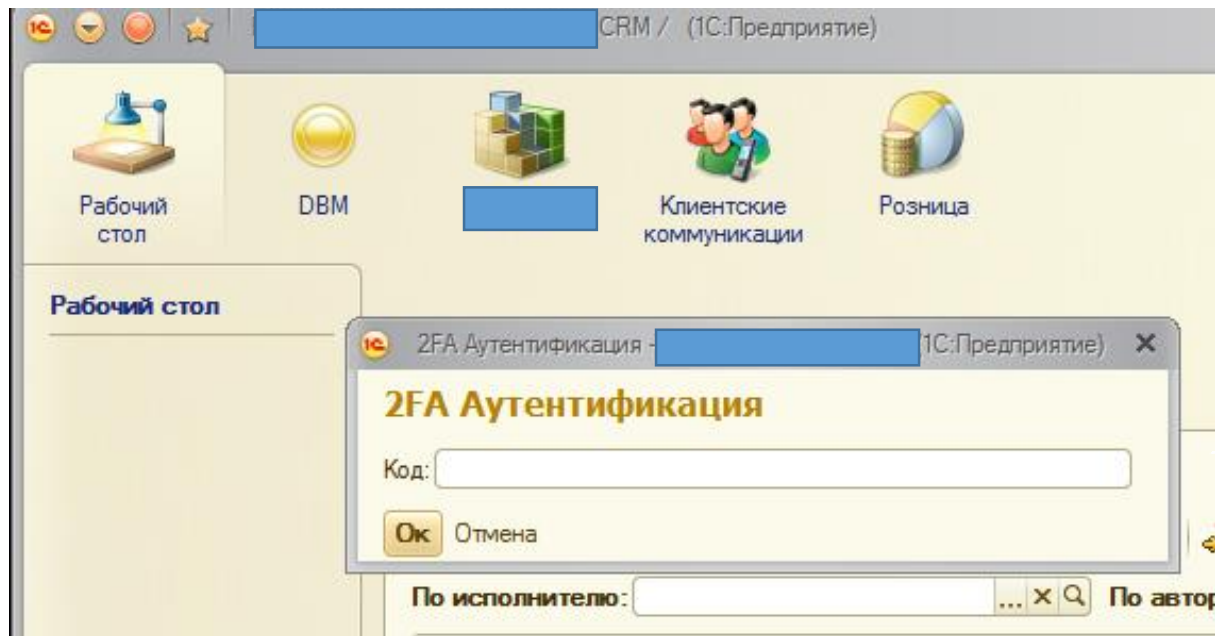


ESET Secure Authentication



- **Уникальные пароли при каждом подключении** для предотвращения утечки конфиденциальных данных
- **Двухфакторный разовый пароль аутентификации (2FA OTP)** — решение на базе мобильных устройств
- **Только программное обеспечение** — нет необходимости в дополнительном управлении аппаратными устройствами
- **Никаких дополнительных затрат на аппаратное обеспечение** — интегрируется в существующую инфраструктуру

ИНТЕГРАЦИЯ С 1С



ДОСТУПЕН:

- NFR
- ДЕМО СТЕНД





ESET - НОВЫЕ ВОЗМОЖНОСТИ



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Гарантия антивирусной защиты. Как это работает?



CyberEdge

– это комплексное решение, которое не только компенсирует возможные потери от утечки данных и позволяет успешно преодолеть кризис, возникший по причине утечки данных и последствий кибер – инцидента*.

Стандартный пакет

A: Ответственность за убытки в связи с потерей данных

B: Административное расследование в отношении данных

C: Сервисные расходы

Дополнительные опции

D: Ответственность за содержание информации

E: Виртуальное вымогательство

F: Убытки от сбоев в работе сети



*Правила безопасности: В выплате страхового возмещения может быть отказано, если в застрахованной компании совершались умышленные действия по загрузке небезопасных файлов, недобросовестно исполнялись обязанности по обновлению сигнатурных баз антивирусного ПО, несанкционированно подключались или отключались отдельные модули антивируса, а также были отмечены любые иные действия или бездействия, повлекшие неполноценную работу решения ESET.

АКАДЕМИЯ ESET

Курсы для технических специалистов

<https://academy.esetnod32.ru/business/specialist/>

Курсы для пользователей

<https://academy.esetnod32.ru/home/user/>



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

**СПАСИБО
ЗА ВНИМАНИЕ!**

Фёдоров Сергей
тел: +7 929 212-64-00
e-mail: sfedorov@esetnod32.ru



www.vkontakte.ru/nod32



www.facebook.com/ESETNOD32Russia



www.club.esetnod32.ru



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

