

The logo for Softline, featuring the word "softline" in a sans-serif font. The "soft" part is red and the "line" part is white. A white swoosh underline is positioned above the "line" part. A registered trademark symbol (®) is located at the top right of the word.

softline®

Microsoft M365

Сценарии продуктивности и безопасности

Microsoft 365

Office 365

Windows 10

Enterprise Mobility
+ Security

*Комплексное интеллектуальное решение для творческой
и совместной работы в безопасной среде*

Факты о кибератаках в России

203

Млрд руб.

Общая сумма
ущерба

123

Млрд руб.

Сумма ущерба
бизнесу

>1000

DDoS

Атак ежедневно

75%

Взломов -
Кража учётных
данных

30%

Рост
количества
зараженных ПК

Реальность

95% компаний

Сталкиваются с киберугрозами ежегодно

50% из них

Теряют данные безвозвратно

До 20 млн. руб.

Средний ущерб от кибератаки

По данным ежегодного исследования и частных расследований «Лаборатории Касперского»

Прогноз

НЕТ оснований

Для снижения уровня киберпреступности

173%

Рост количества атак

193%

Рост ущерба от кибератак

По данным опроса в рамках исследования ФРИИ, Microsoft и Group-IB

Последствия успешных кибератак



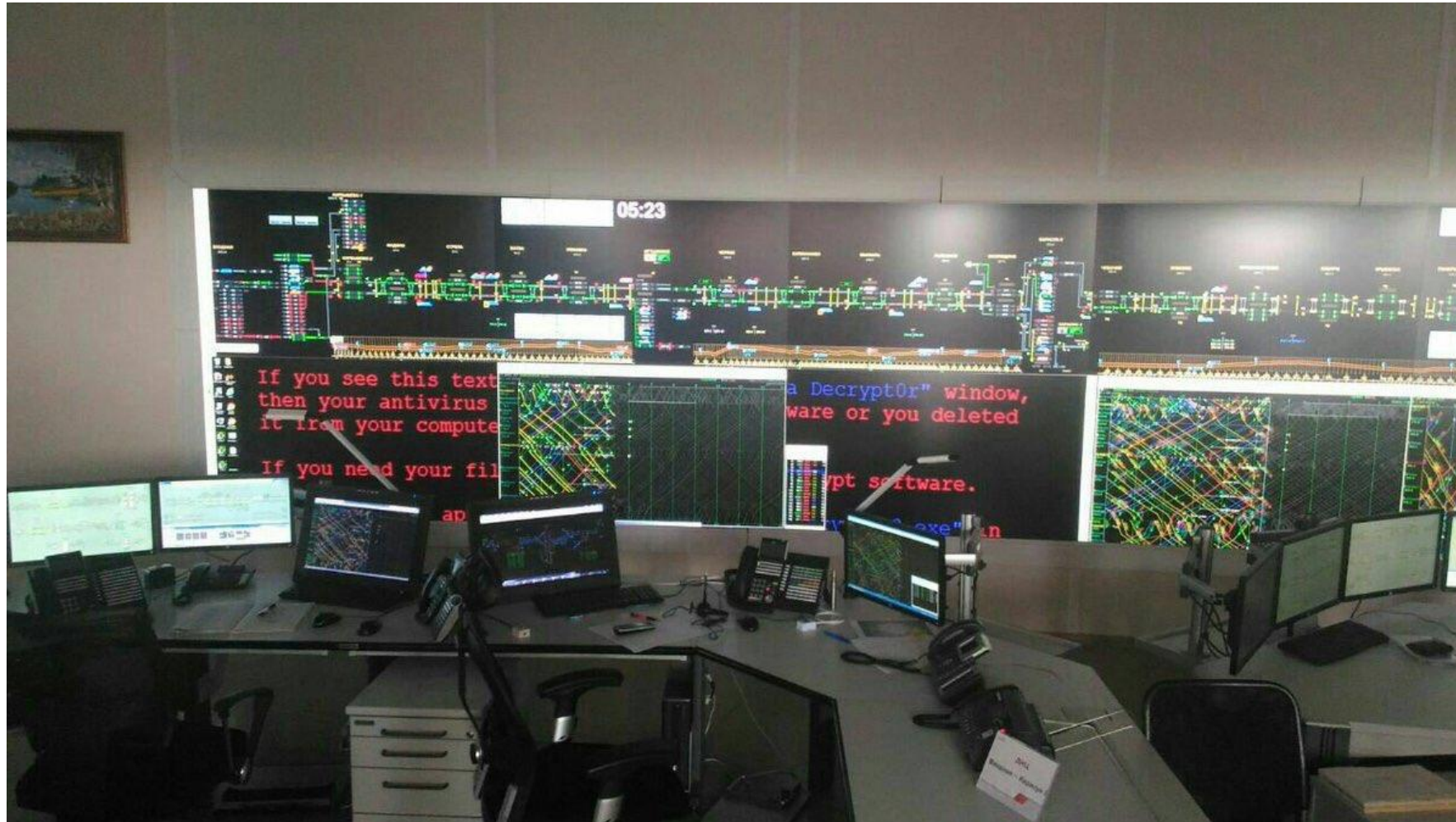
Последствия успешных кибератак



Последствия успешных кибератак



Последствия успешных кибератак



Последствия успешных кибератак



Последствия успешных кибератак



Результат попадания в киберловушку

**Потеря
данных**

**Остановка
бизнеса**

Убытки

**Урон
репутации**

**Расходы
на восстановление**

Страх
перед новыми
технологиями

Microsoft 365

Сценарии безопасности

Управление доступом



Единый портал доступа к корпоративным ресурсам

Сценарии многофакторной аутентификации

Сценарии сквозной аутентификации

Самостоятельный сброс пароля.

Защита от киберугроз



Защита почты от спама

Защита почты от вирусов и фишинга

Защита ПК от вирусов

Мониторинг и аналитика поведения пользователей

Выявления подозрительных действий и таргетированных атак

Управление устройствами



Управление ПК и мобильными устройствами

Управление приложениями

Выявление подозрительной активности

Защита учётных данных пользователя

Защита информации



Классификация и маркировка документов на основе контента

Шифрование

Управление Правами и политиками доступа

Отслеживание документов и отзыв прав

Контроль облачных сервисов



Аналитика использования облачных сервисов

Выявление потенциальных угроз

Обнаружение фактов публикации корпоративных документов

Борьба с «теневым IT»

Почему Microsoft?

>1 млрд \$

Ежегодные
инвестиции в
безопасность

>20 ЦОД

По
безопасности

>1 млрд

ПК
на Windows

>1300

Математиков работают над
алгоритмами машинного обучения

>8 ТВ логов

в день, связанных
с безопасностью



GO GLOBAL



GO CLOUD



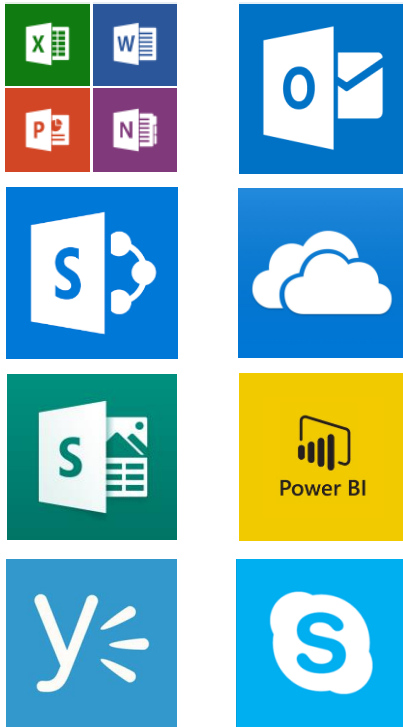
GO INNOVATIVE

Microsoft 365

Продуктивность

Microsoft Office

Привычные инструменты
для работы с документами



Teams

Командное взаимодействие
и корпоративный чат



Planner

Совместная работа над проектами
для небольших команд



Delve

Управление собственными
и общими документами



My Analytics

Трекер персональной
продуктивности



StaffHub

Управление сменными
работниками



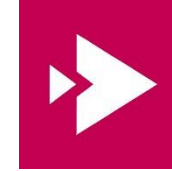
Bookings

Управление
бронированием



Forms

Проведение опросов
и голосований



Stream

Корпоративный
видео-портал

Возможности Office 365 E3/E5



Приложения

Office 365 Pro Plus:
Office на 5 ПК или Mac

Office для мобильных устройств:
Приложения для планшетов и смартфонов

Клиентский доступ и сервисы

Exchange Std + Ent CAL + Exchange online + EOP:
Электронная почта и календарь бизнес-класса

One Drive for Business:
Облачное хранилище и обмен файлами

SharePoint Std + Ent CAL:
Внутренние порталы и сайты

SfB Std + Ent CAL + SfB online:
Встречи, IM, Видеоконференции

Yammer:
Частная социальная сеть

Teams:
Взаимодействие команд в чате

StaffHub:
Управление сменными

Безопасность

Advanced Threat Protection:
Расширенная защита почты: от неизвестных угроз (угроз «нулевого дня») и фишинговых атак

Advanced Security Management:
Панель для сбора аналитики и контроля за действиями пользователей

Customer Lockbox:
Тотальный контроль и защита данных в облаке

Advanced eDiscovery:
Сервис для поиска данных, проведения электронного аудита и расследования действия пользователей

Аналитика

Power BI Pro:
Корпоративная аналитика по всем источникам данных в реальном времени

MyAnalytics:
Трекер персональной продуктивности работы сотрудников (количество и качество встреч, аналитика общения с коллегами и руководителем и т.д.)

Коммуникации в облаке

Cloud PBX + SfB Plus CAL:
Подключение облака O365 к корпоративной телефонии, выделение номеров пользователям

PSTN Conferencing:
Присоединение к онлайн-собраниям по звонку из любой точки мира, выделение номера для конференции

Office 365 E3^{1МИ}

Office 365 E5

Возможности Windows 10 Enterprise



Доверенная платформа

Повышение продуктивности

Персонализация

Широкий спектр устройств

Enterprise Data Protection

Защита от утечек данных за счет отделения корпоративной информации от личной.

Windows Hello for Business

Доступ к системе на основе биометрии

Credential Guard

Защита учетных записей с помощью аппаратных средств изоляции

AppLocker

Запуск нежелательных и подозрительных приложений в изолированной среде.

Device Guard

Запрет на запуск недоверенных приложений на устройстве.

Advanced Threat Protection

Анализ угроз за счет обнаружения подозрительного поведения, сопоставления с базой данных известных атак.

Azure Active Directory Join

Включение устройства в облачную или гибридную инфраструктуру организации.

MDM enablement

Управление устройством средствами MDM-решений

Windows Store for Business, Private Catalog

Каталог приложений, предоставляемых сотрудникам организацией.

Application Virtualization (App-V)

Упрощение развертывания и управления приложениями

User Experience Virtualization (UX-V)

Синхронизация пользовательских настроек между устройствами и виртуальными средами Windows

Granular UX Control

Управление интерфейсом через централизованные политики

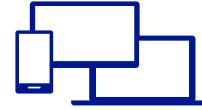
Windows 10 for Industry Devices

Использование недорогих, массовых устройств в качестве терминалов, киосков и др.

Windows 10 Enterprise E5

Windows 10 Enterprise E3

Возможности Enterprise Mobility + Security E3/E5



Управление учетными записями и доступом

Безопасность учетных записей

Управление устройствами, в т.ч. мобильными

Защита информации

WS RMS CAL + WS CAL + Azure Active Directory Premium P1

Единая учетная запись для локальных и облачных приложений
Многофакторная аутентификация, контроль доступа с разных устройств, отчетность и аналитика

Microsoft Advanced Threat Analytics

Анализ трафика и событий безопасности в локальном AD заказчика, предупреждения и проактивные действия. Локальный сервис (не облако).

SC Config Manager + Microsoft Intune

Управление мобильными устройствами и приложениями (политики пароля, пин-кода, шифрования для устройства, разделение приложений и учетных записей в них на личные и рабочие)

SC Endpoint Protection + Azure Information Protection Premium P1

Защита файлов через шифрование с помощью RMS (Azure и локального)
Отслеживание доступа к файлам (только через Azure RMS)
Ручная классификация документов

Azure Active Directory Premium P2

Расширенная аналитика и действия по событиям, связанным с учетными записями (на базе машинного обучения)
Дополнительная защита (временное предоставление доступа) для привилегированных учетных записей

Microsoft Cloud App Security

Обнаружение фактов использования облачных сервисов (через анализ сетевых журналов)
Управление облачными сервисами (Microsoft и др.)

Azure Information Protection Premium P2

Автоматическая классификация и наложение политик защиты на файлы
Одновременное использование локального RMS и Azure RMS

EMS E3

EMS E5