

Windows 10

для IT-специалистов

Introducing Windows 10 for IT Professionals

Technical Overview

ED BOTT

Microsoft[®]

Windows 10

для IT-специалистов

Эд БОТТ

Москва

ЭКОМ

2016

ББК 32.97

УДК 681.3

Б87

Ботт Э.

- Б87 Windows 10 для IT-специалистов.** / Э. Ботт; пер. с англ. – М.: Эком
Паблишерз, 2016. – 173 с.: ил.

ISBN: 978-0-7356-9697-6

Authorized translation from the English language edition, entitled INTRODUCING WINDOWS 10 FOR IT PROFESSIONALS, ISBN 9780735696976, by Bott, Ed, published by Microsoft Press a division of Microsoft Corporation.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

ISBN: 978-5-9790-0191-3

RUSSIAN language edition published by ECOM MEDIA GROUP LTD., Copyright © 2016.

ОГЛАВЛЕНИЕ

Глава 1

Обзор Windows 10	9
Что представляет собой Windows 10?	10
Новый подход к обновлениям	10
Эволюция взаимодействия Windows с пользователем	12
Учетные записи пользователей и синхронизация	14
Windows-приложения	16
Новый браузер по умолчанию	17
Что нового для IT-профессионалов?	19
Лучший контроль над обновлениями	19
Улучшения безопасности	20
Развертывание и управляемость	23
Виртуализация	24

Глава 2

Взаимодействие с пользователем в Windows 10	26
Обзор нового взаимодействия	27
с пользователем в Windows	27
Приложение Параметры	29
Уведомления и кнопки действий	31
Кортана	32
Универсальные приложения	34
в окнах изменяемого размера	34
Навигация	36
Режим планшета	38
Проводник	39
Подключения к облаку	40

Глава 3

Установка и активация	42
Совместимость и подготовка	42
Системные требования	43
Поддерживаемые пути обновления	43
Создание и использование установочного носителя	43
Новые правила активации	45
Варианты установки Windows 10	47

Создание и управление учетными записями пользователей	50 50
Какой тип учетной записи следует использовать?	51
Глава 4	
Развертывание Windows 10 в организации	56
Сценарии развертывания	57
Обзор средств развертывания в организациях	59
Microsoft Deployment Toolkit 2013	59
Windows Assessment and Deployment Kit.....	60
Глава 5	
Защита и конфиденциальность в Windows 10	64
Эволюция многообразия угроз.....	64
Защита аппаратного обеспечения	65
Защита процесса загрузки.....	66
Блокировка корпоративных ПК с помощью Device Guard.....	69
Защита данных на локальных запоминающих устройствах	70
Шифрование устройства	71
Шифрование диска BitLocker	71
Удаленное удаление бизнес-данных	72
Защита учетных данных	72
Блокировка вредоносного ПО	76
Защитник Windows (Windows Defender)	76
SmartScreen и защита от фишинга.....	77
Управление конфиденциальностью	78
Глава 6	
Microsoft Edge и Internet Explorer 11	83
Краткая история Internet Explorer	83
Браузеры в Windows 10	84
Microsoft Edge	87
Настройка режима предприятия в Windows 10	92
Глава 7	
Сеть в Windows 10	95
Усовершенствования беспроводной сети	95
Защищенное подключение к корпоративным сетям.....	99
Управление сетевыми подключениями	101
Поддержка IPv6	104

Глава 8	
Hyper-V и варианты виртуализации рабочих столов	105
Клиентский Hyper-V	105
Варианты виртуализации рабочих столов	109
Виртуализация приложений	112
Виртуализация User Experience	114
Глава 9	
Инструменты восстановления и устранения неполадок	115
Использование среды восстановления Windows	115
Windows 10 и варианты сброса по нажатию кнопки	118
Опция Сохранить мои файлы (Keep My Files)	121
Опция Удалить все (Remove Everything)	122
Инструменты диагностики	123
Инструменты Sysinternals	124
Пакет Microsoft Diagnostics and Recovery Toolset	124
Глава 10	
Интеграция с Azure Active Directory	126
Знакомство с Azure AD	126
Подключение ПК с Windows 10 к Azure AD	131
Добавление рабочих учетных записей в Windows 10	135
Глава 11	
Универсальные приложения и новый Windows Store	136
Универсальная платформа Windows	136
Знакомство с новым Windows Store	137
Как работают UWP-приложения	140
Использование Windows Store для бизнеса	143
Глава 12	
Хранилище	146
Инструменты управления хранилищем	146
Управление дисками	147
DiskPart	147
Storage Sense	148
История файлов	150
Дополнительные варианты хранилища	152

Глава 13	
Управление мобильными устройствами и корпоративными данными	156
Стратегии управления	
мобильными устройствами	156
System Center Configuration Manager	157
Microsoft Intune	159
Рабочие папки.....	161
Глава 14	
Windows 10 на телефонах и маленьких планшетах.....	163
Эволюция Windows на мобильных устройствах	163
Глава 15	
Что нового в групповой политике в Windows 10.....	165
Windows Update для бизнеса.....	165
Device Guard	166
Microsoft Passport для работы	168
Microsoft Edge и Internet Explorer	169
Управление доступом к предварительным сборкам и данным телеметрии.....	170
Управление оптимизацией доставки обновлений Windows	171
Политики безопасности	172

ГЛАВА 1

Обзор Windows 10

В Microsoft Windows 10 появился длинный список важных изменений, среди самых важных – существенно улучшено взаимодействие с пользователем, значительно усовершенствованы меры безопасности, создан новый веб-браузер.

Но самое значительное изменение связано с обновлением программного обеспечения в корпоративной среде. Теперь организации могут использовать новую технологию сразу, как только она становится доступной, а не годы спустя. Исторически переход бизнеса на новую версию Windows – это медленный и осмотрительный процесс с тщательным планированием и поэтапным развертыванием, который может занять несколько лет. В результате такого консерватизма многие организации предлагают своим работникам ПК с программным обеспечением, значительно отличающимся от установленного у сотрудников дома.

Windows 10 поставляет новые возможности в виде бесплатного обновления, а не откладывает их для главного выпуска, который может выйти годы спустя. В Windows 10 сама концепция главного выпуска ушла в небытие – или, по крайней мере, отошла на задний план.

Терри Майерсон (Terry Myerson), исполнительный директор подразделения операционных систем в компании Microsoft, называет новую модель предоставления обновлений «Windows как сервис» (Windows as a Service). Он утверждает, что «в течение двух лет Windows будет рассматриваться как один из самых больших интернет-сервисов на планете. И, как и в случае с любым интернет-сервисом, сам вопрос о номере версии не будет иметь смысла».

Этот процесс уже начался. В конце 2014 года Microsoft запустила программу Windows Insider с предварительным техническим выпуском Windows 10 Technical Preview, нацеленную на IT-профессионалов и потребителей. Спустя 10 месяцев, после множества обновлений и беспрецедентного числа отзывов от членов программы Insider, Microsoft официально выпустила Windows 10 для широкой общественности.

29 июля, спустя всего три месяца после выпуска Windows 10, компания Microsoft заявила, что уже более 110 миллионов устройств работают под управлением Windows 10. Эти пионеры Windows 10 получили первый пакет новых возможностей, официально обозначенный как версия 1511, через проверенный канал Windows Update в ноябре 2015 года. К январю 2016 Windows 10 работала уже более чем у 200 миллионов пользователей.

Windows 10 – это новый мир для всех, кто задействован в развертывании и поддержке Windows в организациях любого размера.

В этой главе предлагается обзор Windows 10 с рассказом о возможностях и функциях, представляющих интерес для IT-профессионалов.

Что представляет собой Windows 10?

Windows традиционно связывают с настольными ПК и ноутбуками. Выпуск Windows 10 предназначен для гораздо более широкого набора устройств, что показывает рис. 1-1, взятый из презентации Microsoft.



Рис. 1-1. Семейство Windows 10 охватывает широкий диапазон устройств: от телефонов и новой гарнитуры HoloLens (Очки добавленной реальности) до игровых консолей и персональных компьютеров

На всех этих устройствах используется большой объем общего кода, но это не значит, что один и тот же код будет выполняться на каждом устройстве. Версия Windows 10 Enterprise для 64-разрядного настольного ПК, например, очень отличается от Windows 10 Mobile или системы на базе Windows 10, работающей на игровой консоли Xbox One.

Но общий код имеет огромные преимущества при разработке программного обеспечения. Программы, построенные на универсальной платформе разработки приложений Windows 10, могут выполняться на всех устройствах из семейства Windows 10, которые доставляются через универсальный магазин Windows Store. Ими легче управлять, и они более защищены, чем традиционные настольные программы, которые могут работать только на ПК.

Новый подход к обновлениям

Как уже упоминалось, наиболее революционное изменение в Windows 10 – это концепция непрерывного совершенствования. Новые возможности доставляются через Windows Update, а не откладываются до следующего главного выпуска. Вопреки сложившимся практикам, Microsoft теперь рекомендует корпоративным клиентам включать службу Windows Update для большинства пользователей, хотя вариант с использованием служб обновлений Windows Server Update Services (WSUS) в некоторых конфигурациях все еще может применяться.

В новой модели «Windows как сервис» Microsoft планирует доставлять значительные обновления с новыми возможностями два-три раза в год. Это гораздо быстрее традиционной схемы выпуска Windows, в которой новые функции резервировались для новых версий, выходивших с фанфарами в среднем один раз в три года.

Чтобы помочь IT-профессионалам адаптироваться к новому ритму изменений, Microsoft разработала новую модель обслуживания для Windows 10. Обновления безопасности по-прежнему будут поступать во второй вторник каждого месяца через Windows Update вместе с дополнительными обновлениями для повышения надежности, обновлениями драйверов устройств и внеочередными обновлениями безопасности.

Новые возможности доставляются в пакетах обновлений большего размера, которые эквивалентны полному обновлению на месте (in-place upgrade). На пути к публике и бизнес-пользователям каждая новая сборка Windows 10 проходит через разные «ветви». На рис. 1-2 представлена концептуальная схема рабочего процесса разработки с указанием ориентировочных периодов тестирования, стабилизации и исправления ошибок перед переходом сборки к следующей ветви.

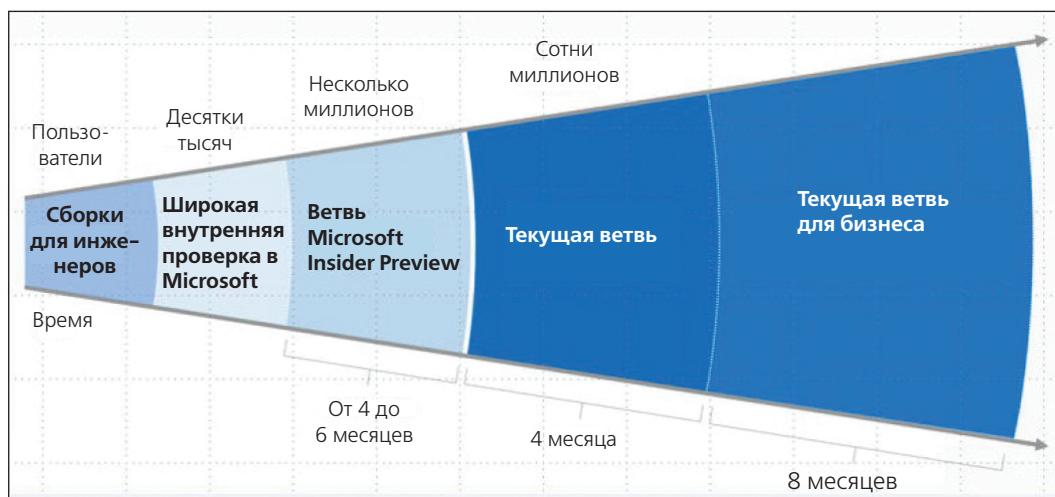


Рис. 1-2. Перед тем как попасть к пользователям в Текущей ветви, каждое новое обновление версии Windows 10 проходит через интенсивное внутреннее и внешнее тестирование. IT-профессионалы, которые предпочитают более консервативный подход, могут откладывать обновления на более долгий срок

Тестирующие внутри Microsoft получают предварительные сборки первыми, затем – члены программы подписки Windows Insider. Они используют предварительные сборки для предоставления обратного отклика, который используется компанией Microsoft для выявления ошибок и подстройки возможностей.

После этапа полировки и устранения ошибок на публику выпускается стабильная версия. Это Текущая ветвь, представленная на рис. 1-2.

Версия 1511 была выпущена в Текущую ветвь в ноябре 2015. (Схема нумерации версии соответствует дате выпуска, в формате ггмм.)

IT-профессионалы, которые не спешат развертывать новый код, могут подождать, пока выпуск перейдет к более поздней ветви, она называется Текущая ветвь для бизнеса. С момента выпуска обновления в Текущую ветвь до выпуска этой ветви проходит обычно от четырех до шести месяцев.

Версия 1511, например, была выпущена в Текущую ветвь в ноябре 2015, но в Текущую ветвь для бизнеса она попадет не раньше первой половины 2016 года. Когда она попадет в Текущую ветвь для бизнеса, то будет содержать обновления безопасности на основе опыта десятков или сотен миллионов ПК в Текущей ветви.

Ветвь долгосрочного обслуживания

Наиболее консервативная опция в новой модели предоставления обновлений Windows 10 – это Ветвь долгосрочного обслуживания (Long-Term Servicing Branch, LTSB), которая не представлена на рис. 1-2. Эта ветвь, доступная только в редакции Windows 10 Enterprise, предназначена для использования в критически важных устройствах, в которой новые возможности не играют большой роли, а стабильность имеет наивысший приоритет. При развертывании Windows 10 Enterprise LTSB на ПК или планшете устройство получает только обновления безопасности и надежности. Обновление до новой версии LTSB или развертывание обновлений Текущей ветви требует новой лицензии или подписки Software Assurance.

Для IT-профессионалов, предпочитающих быть впереди планеты всей, Microsoft предлагает более ранний доступ к предварительным сборкам через программу Windows Insider. Участники этой программы могут выбрать скорость поступления обновлений, ее называют *кольцами* (*rings*). При выборе кольца Быстрые (Fast) новые сборки доступны сразу же после выпуска компанией Microsoft; при выборе кольца Медленные (Slow) доступность новой сборки откладывается, пока она не будет тщательно исследована кольцом Быстрые (обнаруженные ошибки будут закрыты промежуточными обновлениями).

Участие в программе Windows Insider является добровольным, программу можно покинуть в любой момент.

Эволюция взаимодействия Windows с пользователем

Кнопка Пуск и меню Пуск существовали в Windows с версии Windows 95. Приняв небесспорное решение, проектировщики Windows 8 полностью убрали кнопку Пуск и меню Пуск, заменив их экраном с живыми плитками вместо значков. Кнопка Пуск вернулась в Windows 8.1, но теперь ее основной функцией было обеспечить доступ к начальному экрану. Теперь, по настойчивым требованиям пользователей, меню Пуск вернулось в Windows 10.

В Windows 10 при щелчке на кнопке Пуск открывается меню, представленное на рис. 1-3.

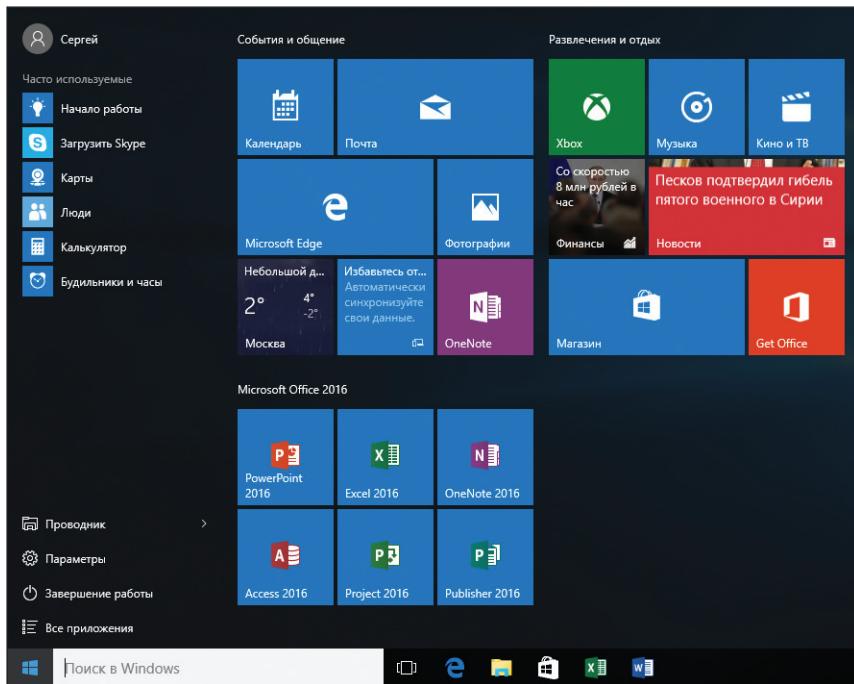


Рис. 1-3. В меню Пуск в Windows 10 смешаны элементы из Windows 7 с живыми плитками, появившимися в Windows 8

Этот дизайн меню Пуск (который неоднократно менялся в ходе длительного предварительного периода до официального выпуска Windows 10) содержит такие знакомые элементы, как ссылки на типичные расположения, список часто используемых приложений и программ, элементы управления питанием. Объекты справа – это живые плитки, которые работают аналогично плиткам на начальном экране Windows 8.1.

Поле поиска, сразу справа от кнопки Пуск, предлагает быстрый доступ к локальной файловой системе и веб-контенту. Применив несколько быстрых настроек, можно включить Кортану (Cortana)*, голосового личного помощника, который появился в Windows Phone, а теперь является важной частью большей платформы Windows 10.

На ПК с клавиатурой и указывающим устройством можно изменить высоту и ширину меню Пуск. Отдельная опция, которая называется *Режим планшета* (Tablet Mode), разворачивает меню Пуск на весь экран. Дополнительные изменения повышают удобство использования Windows 10 на планшетах, гибридных ПК и других устройствах с сенсорным экраном. Режим планшета в действии представлен на рис. 1-4.

* Доступна не во всех регионах

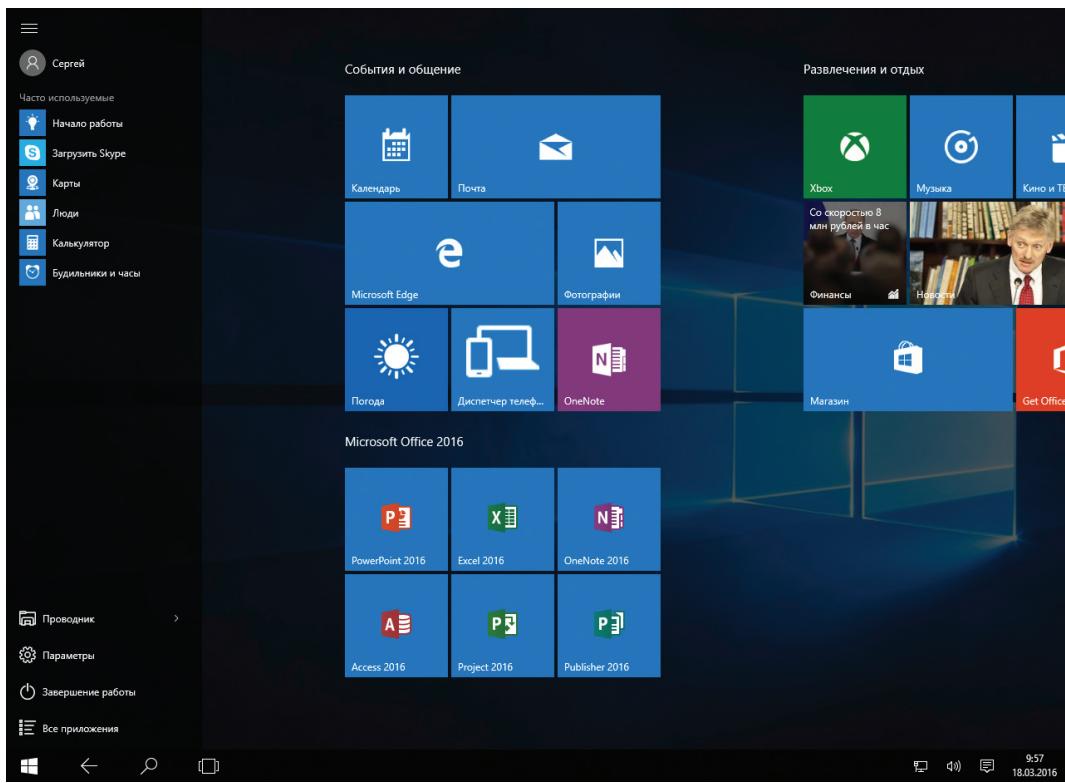


Рис. 1–4. В режиме планшета поле поиска сворачивается, меню Пуск и программы заполняют весь экран

Несколько элементов управления навигацией, которые были добавлены в Windows 8, в Windows 10 были убраны. Меню Чудо-кнопки (Charms) заменено Центром уведомлений (Action Center) с правого края экрана, в нем показываются уведомления и содержатся ярлыки типичных задач. Элементы управления Windows 8, связанные с наведением указателя мыши на углы, заменены новым Представлением задач (Task View), которое также поддерживает несколько виртуальных рабочих столов.



Дополнительная информация. За дополнительной информацией о работе Windows 10 обратитесь к главе 2.

Учетные записи пользователей и синхронизация

При переходе к Windows 10 с Windows 7 необходимо уделить особое внимание новому типу учетных записей, который появился в Windows 8. Вход в систему с учетной записью Microsoft вместо локальной учетной записи предлагает тесную интеграцию с облачными службами, а также легкую синхронизацию настроек и программ между устройствами.

Windows 10 поддерживает вход с учетной записью Azure Active Directory, что позволяет администраторам управлять ПК или мобильным устройством, не присоединяя его к домену. Кроме того, имеется возможность добавить рабочую или учебную учетную запись, чтобы облегчить вход в Office 365 и другие облачные службы.

На рис. 1-5 эта возможность показана в разделе Электронная почта и учетные записи (Your Email And Accounts) в приложении Параметры (Settings). В данном случае у автора подключена учетная запись Google Apps для доступа к электронной почте, календарям и контактам, а также учетная запись Office 365, управляемая через Azure AD.

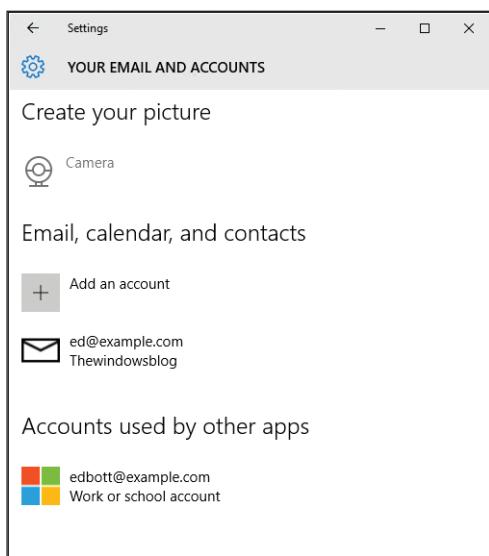


Рис. 1-5. Подключение учетных записей к основной учетной записи облегчает доступ к электронной почте и корпоративным приложениям. Логотип Windows на Учетной записи компании или учебного заведения (Work Or School Account) означает, что она управляемается Azure AD

Список настроек, которые могут синхронизироваться, включает макет начального экрана и приложения; ранее приобретенные приложения могут загружаться и устанавливаться из магазина Store при входе на новое устройство с использованием учетной записи Microsoft. Эта возможность позволяет легко переключаться между устройствами, получая на каждом из них свои персональные настройки, программы, вкладки, историю и Избранное браузера. Для корпоративных пользователей Windows 10 включает возможность управлять этим процессом для IT-профессионалов.

Одна из ключевых возможностей в Windows 10 – это универсальный клиент синхронизации для управления доступом к облачному файловому хранилищу в OneDrive и OneDrive for Business. Клиент OneDrive for Business Next Generation Sync Client был выпущен для Windows 10 в декабре 2015.

В корпоративных развертываниях можно связать учетную запись домена Windows с учетной записью Microsoft, обеспечив безопасность и эффективное управление сетью, но не потеряв преимуществ синхронизации с учетной записью Microsoft.

Windows-приложения

Windows 10 включает поддержку практически всех настольных приложений, совместимых с Windows 7. Она также поддерживает самое последнее поколение Windows-приложений (иногда их называют приложениями *Trusted Windows Store*, или *современными приложениями*). Эти приложения распространяются через магазин Windows Store. (В корпоративных развертываниях IT-профессионалы могут использовать Windows Store для доставки пользователям нужных бизнес-приложений.)

Самая последняя платформа разработки для Windows 10 называется *Universal Windows Platform (UWP)*. Используя интерфейс прикладного программирования (API) UWP, разработчики могут создать единый пакет приложения, который будет выполняться на устройствах с разными размерами и возможностями, включая телефоны, планшеты, ПК и даже консоли Xbox One. Универсальные приложения доставляются через магазин Windows Store.

В Windows 8 и 8.1 современные приложения работают в одном из двух режимов: полноэкранном или прикрепленном к краю экрана. В Windows 10 эти приложения могут выполняться в окне. На рис. 1-6 представлено бесплатное приложение Word Mobile, работающее в окне изменяемого размера на ПК с Windows 10.

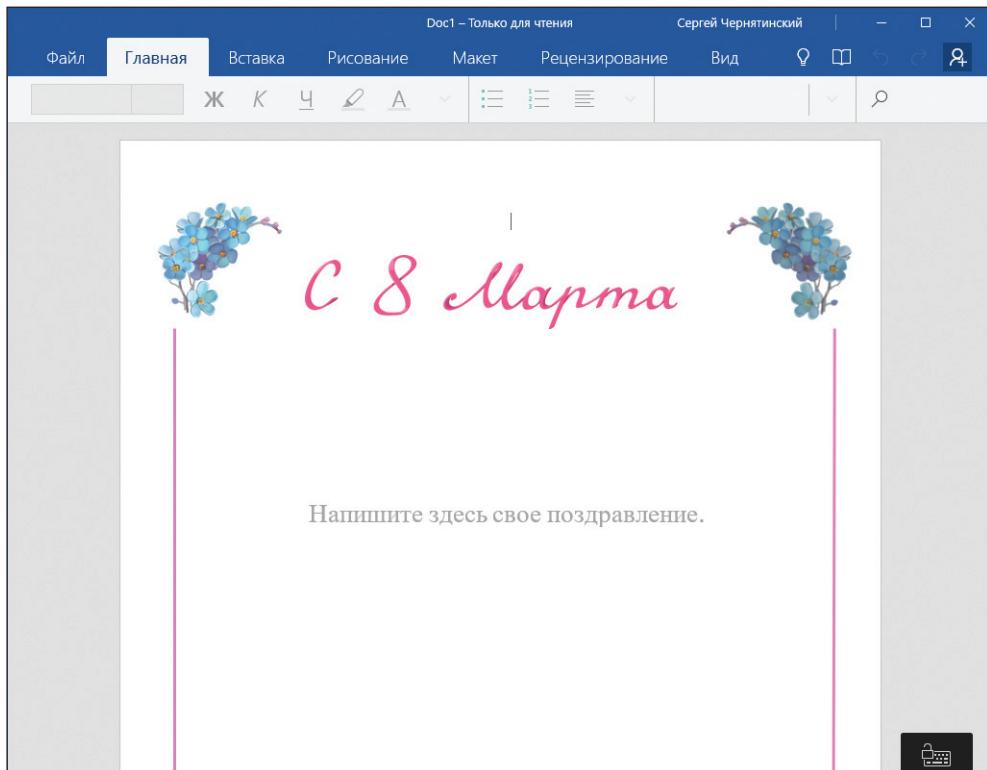


Рис. 1–6. Приложение Word Mobile доступно через Windows Store. Как и любое другое современное приложение в Windows 10, оно может работать в окне изменяемого размера

Как и в большинстве современных приложений, мобильные приложения Microsoft Office, доступные в Windows Store (вместе с Word идут еще Excel и PowerPoint), позволяют эффективно работать с приложениями Office на устройствах с маленькими сенсорными экранами. Эти облегченные приложения идеальны для чтения и несложного редактирования.

Windows Store был полностью переделан для Windows 10. На рис. 1-7 представлен типичный элемент в новом магазине, который теперь имеет более логичный дизайн и предлагает не только приложения, но и гораздо более широкий набор продуктов.

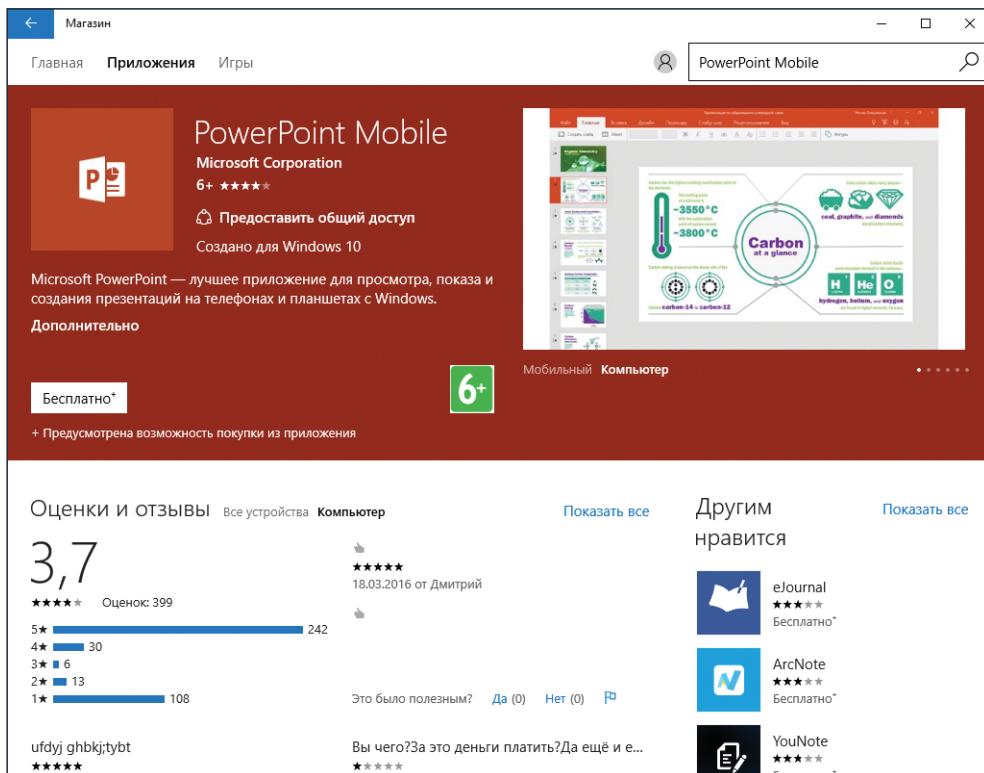


Рис. 1-7. В Windows Store можно купить или арендовать не только приложения, но и игры

 **Дополнительная информация.** За дополнительной информацией об этих приложениях и изменениях в Windows Store, в том числе Windows Store for Business, обратитесь к главе 11.

Новый браузер по умолчанию

Одна из самых важных возможностей Windows 10 – это новый браузер по умолчанию, Microsoft Edge. Хотя его движок EdgeHTML основывается на движке Trident, который был частью Internet Explorer с самого начала, новый движок создан с учетом соответствия современным веб-стандартам.

Команда разработки Internet Explorer говорит, что убрала 220 000 строк кода, когда начала менять движок Trident для EdgeHTML. Такая глобальная чистка была необходима, чтобы избавить новый браузер от багажа совместимости, благодаря которому Internet Explorer приобрел плохую репутацию в сообществе веб-разработчиков. Пройдя этот шаг, они добавили новые и полезные возможности, такие как интеграцию с Кортаной*, новый список чтения, возможность добавлять на веб-страницы аннотации и делиться веб-страницами. Новый браузер предлагает отличную поддержку современных веб-стандартов и лучшую совместимость с другими современными браузерами.

Microsoft Edge разрабатывался с бешеною скоростью, поскольку его первое появление на публике (с неполным набором возможностей) состоялось в предварительном выпуске Insider в апреле 2015 года. Первый выпуск Текущей ветви Windows 10 (Июль 2015) включал версию 12 браузера Edge; версия 1511 Windows 10, являясь главным обновлением, содержит версию 13 браузера Edge. На рис. 1-8 представлен дружественный к сенсорным экранам и незагроможденный (практически спартанский) интерфейс браузера Microsoft Edge.

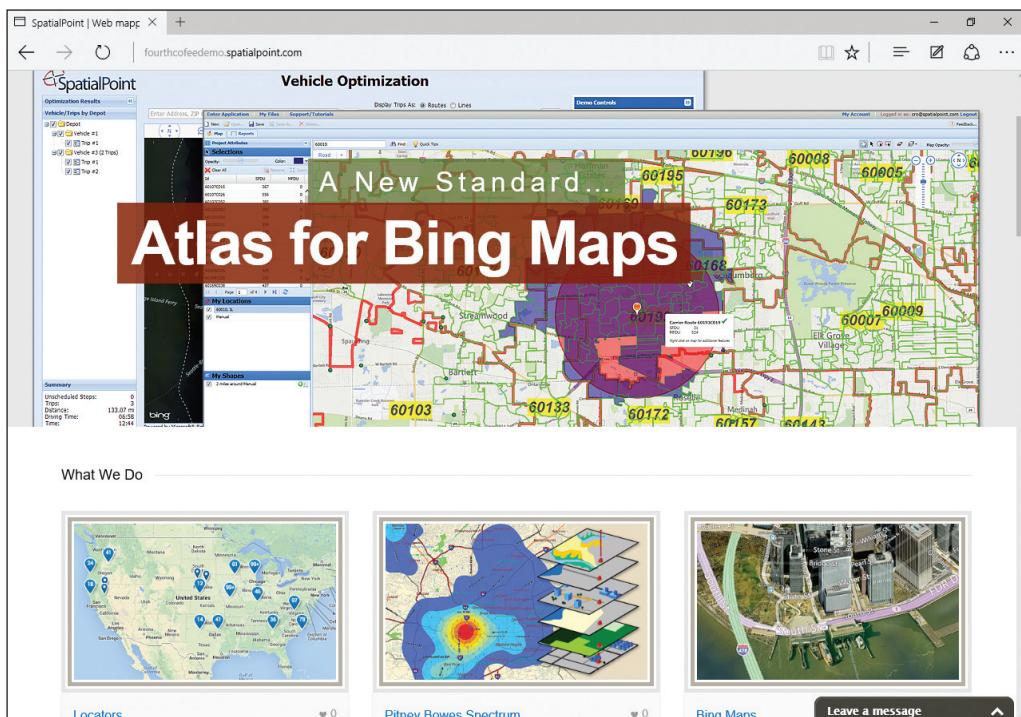


Рис. 1-8. Microsoft Edge, браузер по умолчанию для устройств с Windows 10, включает простой дизайн с возможностью открыть любую страницу в Internet Explorer

Если читателя интересует вопрос, что же случилось с Internet Explorer, то вы не единоки. Многим бизнес-приложениям в корпоративных развертываниях требуется Internet Explorer. Некоторым приложениям требуются версии более старые, чем Internet Explorer 11, который с января 2016 является единственной поддерживаемой версией.

* Доступна не во всех регионах

Хорошие новости для IT-профессионалов состоят в том, что в корпоративных средах Internet Explorer останется доступным и в Windows 10, а такая возможность, как Enterprise Mode, позволит корректно работать более старым приложениям.



Дополнительная информация. Дополнительная информация об этой двухбраузерной стратегии приводится в главе 6.

Что нового для IT-профессионалов?

IT-профессионала первым делом беспокоят пользователи, которых он поддерживает. Какой объем обучения потребуется? Какие из бизнес-приложений будут работать корректно, а какие потребуют изменения или замены? Сколько усилий понадобится на широкомасштабное развертывание? И, что наиболее важно, удастся ли сохранить бизнес-данные и сети в безопасности и доступности?

Эти вопросы становятся еще более важными, когда пользователи приносят свои персональные устройства – смартфоны, планшеты и ПК – и ожидают, что на этих устройствах можно будет быстро переключаться между работой и личными задачами. Такая гибкость стала настолько распространенной в современной эре, что феномен даже получил свое название – консьюмеризация ИТ. Для пользователей стратегия известна под более звучным названием *Bring Your Own Device (BYOD) (принеси свое собственное устройство)*.

Подход к консьюмеризации ИТ компании Microsoft – попытка удовлетворить и пользователей, и IT-профессионалов. Цель пользователей – сохранить знакомые методы работы со старыми и новыми устройствами. В распоряжении IT-профессионалов имеется соответствующий ассортимент корпоративных решений для управления этими устройствами и защиты при подключении к корпоративной сети.

Лучший контроль над обновлениями

С точки зрения администратора сети, вероятно, самое важное улучшение в Windows 10 – это Windows Update for Business, появившееся в Текущей ветви в версии 1511.

Windows Update for Business (доступно только для редакций Pro, Enterprise и Education) использует настройки групповых политик, которые позволяют администраторам отложить обновления вплоть до четырех недель (с интервалами в одну неделю). Те же настройки позволяют отложить обновления в Текущей ветви для бизнеса (которая уже на несколько месяцев отстает от выпуска Текущей ветви) до восьми дополнительных месяцев, с интервалами в месяц. На рис. 1-9 представлены эти настройки политики в Редакторе локальной групповой политики (Local Group Policy Editor) в Windows 10 Pro.

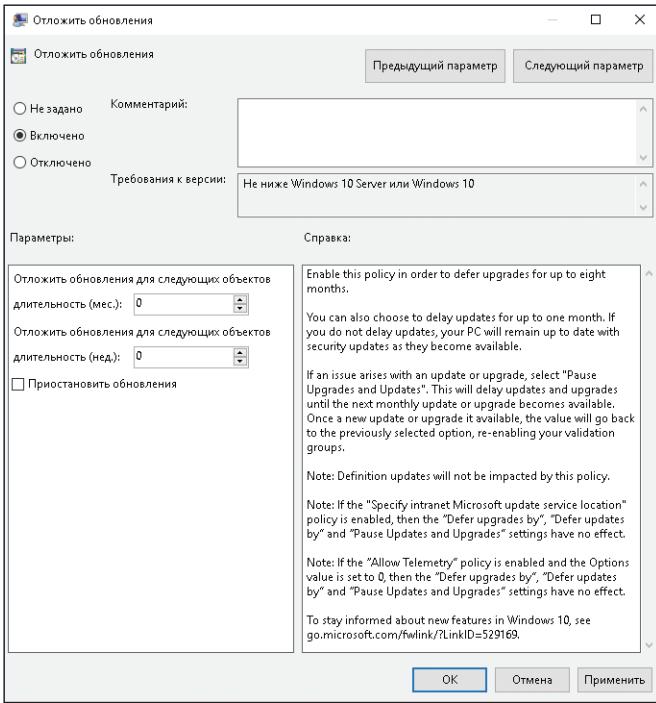


Рис. 1-9. Настройка Отложить обновления (Defer Upgrades And Updates) локальной групповой политики позволяет сетевым администраторам отложить обновления вплоть до четырех недель и отложить обновления Текущей ветви для бизнеса вплоть до восьми месяцев



Дополнительная информация. Дополнительная информация о настройках групповой политики приводится в главе 15.

Улучшения безопасности

Игра в кошки-мышки между онлайн-преступниками и экспертами по компьютерной безопасности затрагивает каждый популярный программный продукт. Microsoft относится к защите Windows очень серьезно. Как часть непрекращающихся усилий по защите вычислительных систем, в Windows 8 были представлены новые функции защиты, в Windows 8.1 были добавлены еще некоторые усовершенствования, в Windows 10 безопасность продолжала улучшаться.

Наиболее значимой функцией защиты в Windows 10 является усовершенствование аутентификации на основе биометрических факторов.

На устройствах с Windows 10 с соответствующим оборудованием появились две новые функции, которые значительно упростят процесс аутентификации для устройства и онлайн-служб.

- **Windows Hello.** Эта функция использует для разблокировки устройств биометрическую аутентификацию – распознавание лица, сканирование радужной оболочки глаза или отпечатка пальца. Технология гораздо более сложная, чем существующие биометрические методы,

которые поддерживаются для базовой аутентификации в Windows 8.1. Например, Windows Hello требует камеру, поддерживающую инфракрасный диапазон, чтобы злоумышленник не мог пройти идентификацию, просто подставив фотографию.

Включение Windows Hello регистрирует устройство с Windows 10 (ПК, планшет или телефон) как надежное для целей аутентификации. В таком сценарии зарегистрированное устройство само по себе работает как дополнительное доказательство идентичности, поддерживая мультифакторную аутентификацию.

- **Microsoft Password.** Вторая функция основывается на новом API, который работает совместно с биометрической аутентификацией на зарегистрированном устройстве для входа в любую поддерживаемую мобильную службу. Инфраструктура Passport позволяет корпоративным ИТ-администраторам, разработчикам и администраторам веб-сайтов предоставлять более защищенную альтернативу паролям. В процессе аутентификации пароль не отправляется по проводам и не сохраняется на удаленных серверах, что закрывает два наиболее распространенных пути для брешей безопасности.

Windows 10 также использует возможности защиты в современном оборудовании (изначально включенные в Windows 8 и 8.1) для гарантии того, что процесс загрузки не будет скомпрометирован руткитами и другим агрессивным злонамеренным ПО. На устройствах с UEFI (Unified Extensible Firmware Interface) процесс Secure Boot проверяет и гарантирует, что загрузочные файлы, включая загрузчик ОС, являются доверенными и правильно подписаны, тем самым предотвращает запуск системы с недоверяемой операционной системы. После того, как загрузчик ОС передает контроль Windows 10, становятся доступны две дополнительные функции обеспечения безопасности.

- **Надежная загрузка (Trusted boot).** Эта функция защищает целостность остальной части процесса загрузки, включая ядро, системные файлы, критичные для загрузки драйверы и даже само антивирусное ПО. Драйверы Early Launch Antimalware (ELAM) инициализируются раньше, чем запускаются другие сторонние приложения и драйверы режима ядра. Такая конфигурация не дает внести изменения в антивирусное ПО и позволяет операционной системе выявлять и блокировать попытки внесения изменений в процесс загрузки.
- **Измеряемая загрузка (Measured boot).** На устройствах с Trusted Platform Module (TPM) Windows 10 производит сложные измерения цепочек целостности в процессе загрузки и безопасно сохраняет эти результаты в TPM. При последующих загрузках система измеряет компоненты ядра операционной системы и всех загрузочных драйверов, включая сторонние драйверы. Эта информация может анализироваться удаленной службой для подтверждения того, что ключевые компоненты не были некорректно модифицированы, и для дальнейшей проверки целостности компьютера перед предоставлением доступа к ресурсам. Этот процесс носит название *удаленной аттестации* (*remote attestation*).

Для блокировки вредоносного ПО по окончании процесса загрузки Windows 10 включает две новые (по сравнению с Windows 7) возможности цифровых подписей.

- **Защитник Windows (Windows Defender).** Предыдущие версии Windows включали ограниченную антивирусную функцию, которая называлась Защитник Windows (*Windows Defender*). Начиная с Windows 8, это полнофункциональная антивирусная программа, наследница

Microsoft Security Essentials. Защитник Windows ненавязчив в повседневном использовании, оказывает минимальное воздействие на системные ресурсы и регулярно обновляет как базу сигнатур, так и антивирусный движок. Защитник Windows также включает средства мониторинга поведения сети. При установке другого антивирусного решения Защитник Windows отключает свою защиту в реальном времени, но остается доступным.

- **Windows SmartScreen.** Windows SmartScreen – это функция безопасности, которая использует технологии на базе репутации приложений для защиты от вредоносного ПО. Эта независимая от браузера технология проверяет перед установкой все новые приложения, блокируя потенциально рискованные, не имеющие репутации. Функция репутации приложений Windows SmartScreen работает вместе с функцией SmartScreen в браузере Windows по умолчанию, что также защищает пользователей от веб-сайтов, которые хотят получить персональную информацию – имена пользователей, пароли, платежные данные.

Совершенно новая функция в Windows 10, Защита учетных данных (Credential Guard), использует защиту на базе виртуализации для изоляции секретных данных (включая пароли доменов), так что обращаться к ним может только привилегированное системное ПО. Эта функция предотвращает распространенные атаки на учетные данные, такие как Pass-The-Hash и Pass-The-Ticket. Охранник должен быть включен для каждого ПК в организации и работает только в редакции Windows 10 Enterprise.

Windows 10 добавляет возможности защиты информации, которые позволяют защищать корпоративные данные даже на персональных устройствах сотрудников. Сетевые администраторы могут определить политики, которые автоматически шифруют важную информацию, включая корпоративные приложения, данные, электронную почту и содержимое сайтов интрасети. Поддержка такого шифрования встроена в типичные элементы управления Windows, такие как диалоговые окна открытия и сохранения документов.

Для большей безопасности администраторы могут создавать списки приложений, которым разрешен доступ к зашифрованным данным, а также приложений, которым доступ запрещен. Администратор сети может, например, запретить доступ к пользовательской службе облачного хранилища, чтобы важные файлы не могли покинуть пределы организации.

Две функции будут особо интересны всем, кто отвечает за корпоративные данные.

- **Enterprise Data Protection.** Функция дистанционного удаления бизнес-данных (Remote Business Data Removal, RBDR) была введена в Windows 8.1 и значительно усовершенствована для Windows 10. С помощью этой функции администраторы могут помечать и шифровать корпоративные данные, чтобы отличать их от обычных пользовательских данных. Политики управляют тем, что сотрудники могут делать с помеченными данными; когда отношения между организацией и пользователем заканчиваются, зашифрованные корпоративные данные становятся недоступны теперь уже неавторизованному пользователю. Это очень важная новая функция, которую планируется добавить в Windows 10 в 2016 году. Она еще недоступна в текущих выпусках.
- **Всеобъемлющее шифрование устройства (Pervasive Device Encryption).** Шифрование устройства доступно во всех редакциях Windows 10.

Оно включено «из коробки» и может настраиваться с дополнительной защитой BitLocker и возможностями управления в редакциях Pro и Enterprise. Устройства, которые поддерживают функцию InstantGo (ранее известную как Connected Standby), автоматически шифруются и защищаются при использовании учетной записи Microsoft.

Организации, которым нужно управлять шифрованием, могут с легкостью включить дополнительные опции защиты BitLocker и управлять этими устройствами. На неуправляемых устройствах с Windows 10 шифрование BitLocker Drive Encryption может быть включено пользователем (при этом ключ восстановления пользователь может сохранить в учетной записи Microsoft).

BitLocker в Windows 10 поддерживает зашифрованные диски, т.е. жесткие диски, которые поставляются производителями уже зашифрованными. На таких устройствах хранения BitLocker получает оборудованию выполнять криптографические операции, увеличивая производительность шифрования и уменьшая нагрузку на ЦП и потребление электроэнергии.

На устройствах беспапаратурного шифрования BitLocker шифрует данные быстрее, чем в среде Windows 7. BitLocker позволяет шифровать только используемое пространство на диске, а не весь диск. В такой конфигурации свободное пространство шифруется при первом использовании, поэтому сам процесс шифрования выполняется гораздо быстрее.

Последнее средство безопасности подходит для организаций с повышенными требованиями к безопасности, таких как подрядчики министерства обороны и правительственные учреждения, которые должны противостоять онлайн-шпионажу. Редакция Windows 10 Enterprise позволяет администраторам использовать функцию Device Guard для полной блокировки устройств, чтобы они не могли выполнять неподписанный код.

В такой конфигурации разрешено выполнение только тех приложений, которые подписаны сертификатом, выданным компанией Microsoft. Сюда включаются приложения из Windows Store и настольные приложения, создатели которых обратились в компанию Microsoft за сертификатом подписи кода. Такие подписанные приложения могут доставляться сотрудникам через настроенный Business Store. Внутренние бизнес-приложения организации могут быть подписаны сертификатом организации.



Дополнительная информация. За дополнительной информацией о возможностях защиты обратитесь к главе 5.

Развертывание и управляемость

Развертывание Windows 10 в организации выполняется быстрее и легче, чем Windows 7. Усовершенствования в процессах развертывания для Windows 10 облегчают стандартизацию в корпоративной конфигурации.

Традиционный вариант «очистить и загрузить» все еще доступен для обновлений Windows 10. Этот процесс включает сбор данных и настроек из существующего устройства, развертывание собственного образа операционной системы, внедрение драйверов и установка приложения, а затем – восстановление данных и настроек.

Дополнительный вариант – обновление «на месте» (in-place upgrade), в котором Windows управляет процессом переноса приложений и данных из существующего образа в новый (стандартный) образ. Этот процесс похож на процесс обновления через Windows Update, но управляется диспетчером System Center Configuration Manager и инструментарием Microsoft Deployment Toolkit.

Windows 10 добавляет новый вариант инициализации, который преобразует устройство с OEM-установкой Windows 10 в корпоративное устройство. Эта процедура убирает ненужные объекты из OEM-конфигурации и добавляет объекты, приложения и детали конфигурации, которые являются частью стандартного настроенного образа. Результат тот же, что и у развертывания путем очистки и загрузки, но процесс проще и гораздо гибче.



Дополнительная информация. За дополнительной информацией о планировании и непосредственном выполнении развертывания Windows 10 обратитесь к главе 3.

На неуправляемых устройствах новые варианты восстановления в Windows 10 помогают упростить процесс переустановки операционной системы. Эти варианты значительно эволюционировали по сравнению с оригинальными версиями в Windows 8, они позволяют пользователям восстановить или исправить устройство Windows 10 без обращения в службу поддержки. Новые варианты восстановления в Windows 10 имеют значительное преимущество: восстановленная система будет содержать все обновления, кроме самого последнего накопительного обновления, а это значит, что пользователю не понадобится выполнять обновление системы после восстановления.

Как и в случае с Windows 8.1, опция сброса включает функции по удалению корпоративных данных, что позволяет пользователю передать устройство новому владельцу, не беспокоясь о том, что вместе с устройством непреднамеренно будут переданы важные персональные или бизнес-данные.

Виртуализация

Windows 10 включает надежную встроенную платформу виртуализации. Эта возможность называется Клиентский Hyper-V (Client Hyper-V). Она будет знакома организациям, которые тестировали или развертывали Windows 8.1; для тех, кто обновляется с Windows 7, это одно из главных добавлений в платформу. Клиентский Hyper-V использует тот же гипервизор, что и в Windows Server, он может использоваться для создания виртуальных машин (VM), позволяющих выполнять 32-разрядные и 64-разрядные клиентские и серверные операционные системы Windows. IT-профессионалы и разработчики могут создавать надежные тестовые стенды для анализа и отладки программного обеспечения и служб, не боясь затронуть производственную среду.

На рис. 1-10 Windows 10 версии 1511 предлагает поддержку Trusted Platform Module (TPM) для виртуальных машин, позволяя им использовать полное шифрование.

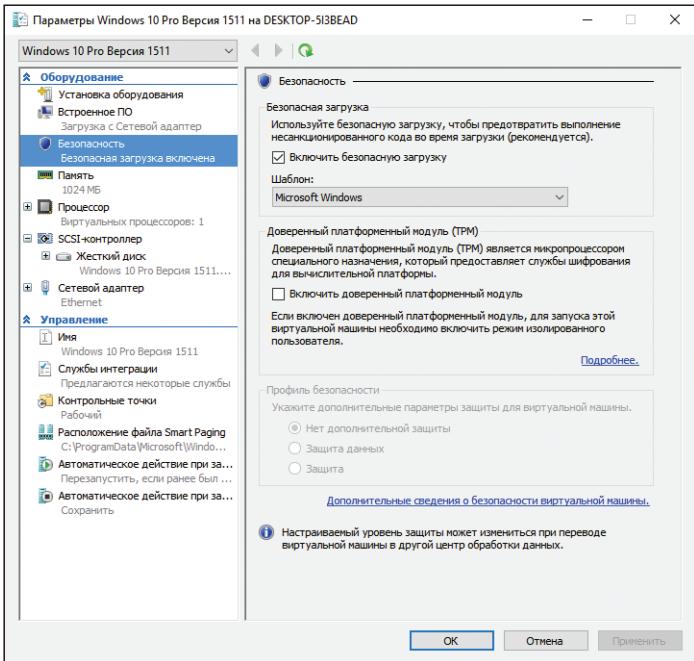


Рис. 1-10. Обновление Windows в ноябре 2015 года, версия 1511, включает значительные усовершенствования в безопасности Hyper-V, в том числе – поддержку безопасной загрузки и шифрования на основе TPM

Клиентский Hyper-V использует инфраструктуру безопасности Windows 10 и легко управляется существующими IT-инструментами, такими как System Center. Виртуальные машины можно переносить между настольным ПК, работающим под управлением Windows 10, и средой Hyper-V на Windows Server. Клиентский Hyper-V требует Windows 10 Pro, Enterprise или Education; хост должен поддерживать определенные аппаратные возможности.

Вместе с Windows Server 2012 и более поздними выпусками, Windows 10 поддерживает альтернативную форму виртуализации: Инфраструктуру виртуальных рабочих столов (Virtual Desktop Infrastructure, VDI). Настройка среды VDI выполняется очень просто, благодаря простому мастеру. Унифицированные возможности управления позволяют легко управлять средой VDI.

Клиент удаленного рабочего стола в Windows 10 позволяет пользователям подключаться к виртуальному рабочему столу по любому типу сети, по локальной или глобальной сети. Microsoft RemoteFX предлагает возможности, сравнимые с локальным рабочим столом, в том числе воспроизведение мультимедиа, отображение 3D-графики, использование периферийных USB-устройств и ввод с сенсорных устройств. Диски профилей пользователей и Fair Share гарантируют высокую производительность и гибкость, позволяя уменьшить стоимость VDI. Все эти преимущества доступны в различных типах рабочих столов VDI (персональная ВМ, ВМ в составе пула, рабочие столы на основе сеансов).



Дополнительная информация. За дополнительной информацией об этих возможностях обратитесь к главе 8.

ГЛАВА 2

Взаимодействие с пользователем в Windows 10

Ваша реакция на Microsoft Windows 10 будет зависеть от того, как в последние несколько лет выглядел ваш рабочий стол Windows.

Если вы и ваша организация все еще используете Windows 7 (и перешли с Windows XP незадолго до конца поддержки в 2014 году), то вам придется привыкнуть к нескольким новым способам работы. Переделанное меню Пуск (Start) – наиболее очевидное изменение, за которым идет перенос многих системных настроек из Панели управления (Control Panel) в современное приложение Параметры (Settings).

Как ни странно, но тем, кто работал с Windows 8, переучиваться сложнее. Им потребуется не только изучить новые элементы Windows 10, но и отучиться от некоторых приемов, к которым за время работы в Windows 8 и Windows 8.1 уже выработалась привычка.

После выпуска Windows 8 по откликам, пришедшим в корпорацию Microsoft, стало ясно, что такая радикальная переделка взаимодействия системы с пользователями вызвала у них значительную растерянность. Изменения были очень существенны для всех, кто привык к виду рабочего стола и меню Пуск (Start).

Взаимодействие с пользователем в Windows 10 объединяет лучшие элементы Windows 7 и Windows 8.1 и сглаживает переход между способами использования рабочего стола и новыми методиками работы с устройствами с сенсорным экраном.

В Windows 10 пользователи ощутят преимущества новых Windows-приложений на традиционных настольных ПК или ноутбуках, взаимодействуя с новыми и старыми приложениями в окнах изменяемого размера. На мобильном устройстве с сенсорным экраном можно включить режим планшета и работать с приложениями на полный экран, не загромождая экран и не отвлекаясь на ненужное.

Новый набор приемов навигации заменяет методики «горячих углов» из Windows 8, а добавление виртуальных рабочих столов в Windows 10 позволяет переключаться между группами приложений, а не жонглировать окнами.

Независимо от стартовой точки, переход к Windows 10 требует продуманного плана обучения новых пользователей, особенностей если они работают в традиционной настольной среде. В этой главе описываются основные изменения во взаимодействии с пользователем в Windows 10.

Обзор нового взаимодействия с пользователем в Windows

Начальный экран (Start screen) ушел. Рабочий стол вернулся.

Новое меню Пуск (Start), представленное на рис. 2-1, разделено по вертикали на две части, как было и в Windows 7, но его содержимое слегка отличается.

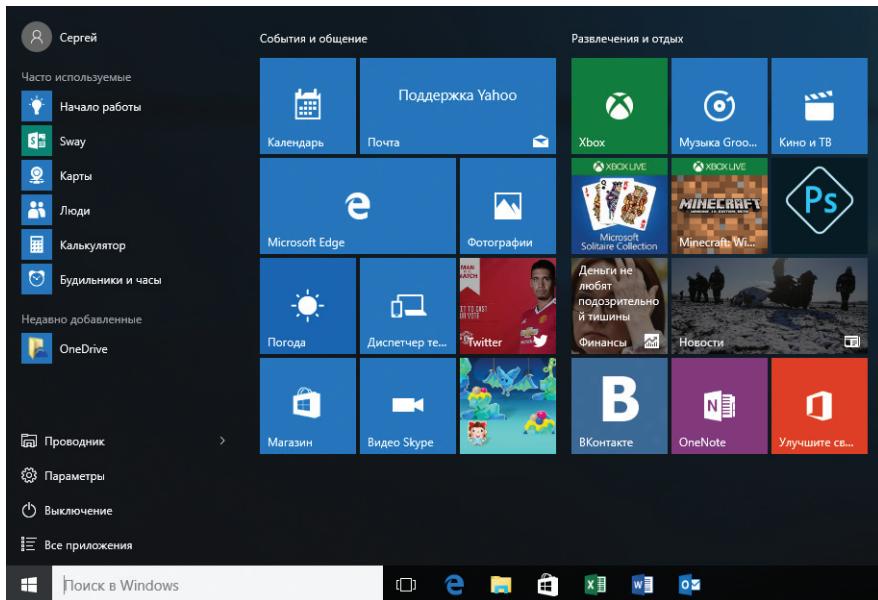


Рис. 2-1. Новое меню Пуск (Start) объединяет лучшие возможности своих предшественников – Windows 7 и Windows 8.1

По умолчанию левый столбец содержит следующие элементы (сверху вниз).

- Значок для текущего пользователя, при щелчке или касании на котором открывается меню с командами блокировки ПК, завершения сеанса, переключения между учетными записями или изменения настроек учетной записи.
- Ярлыки часто используемых и недавно добавленных приложений.
- Ярлыки для Проводника (File Explorer) (пользователям Windows 7 следует обратить внимание на изменение названия) и приложения Параметры (Settings), а также кнопка Выключение (Power).
- Ярлык Все приложения (All Apps), который заменяет левую сторону меню Пуск прокрученным списком с установленными приложениями и сохраненными ярлыками – все, что было на собственном экране в Windows 8.1.

Управление этим списком выполняется в категории Персонализация (Personalization) приложения Параметры (Settings). Также имеется возможность задать стандартный макет меню Пуск (Start) (и запретить пользователям менять его) с помощью групповой политики. (За дополнительной информацией по этой возможности обратитесь к главе 15.)

Ярлыки системных настроек из меню Пуск (Start) в Windows 7 недоступны в меню Пуск, они находятся в скрытом меню для опытных пользователей, которое открывается при щелчке правой кнопкой мыши на кнопке Пуск (Start) или при нажатии комбинации клавиш [Windows]+[X]. На рис. 2-2 представлено это меню, которое в Windows 10 версии 1511 было переключено на темную тему.

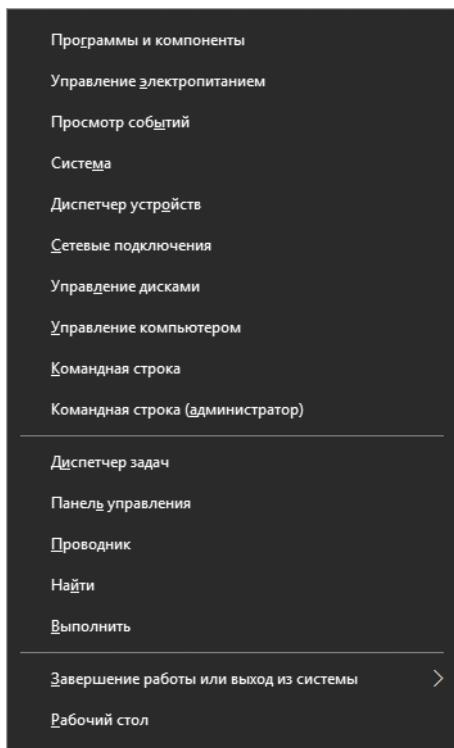


Рис. 2-2. Это меню быстрых ссылок отображается, если нажать комбинацию клавиш [Windows]+[X] или щелкнуть правой кнопкой мыши на кнопке Пуск (Start)

Стандартное меню Пуск (Start) содержит кнопку Выключение (Power) с командами Спящий режим (Sleep), Завершение работы (Shutdown) и Перезагрузка (Restart). Размер меню Пуск (Start) можно менять, перетаскивая верхнюю и правую границы. (В категории Персонализация [Personalization] имеется настройка, позволяющая развернуть меню Пуск [Start] на полный экран, не включая режим планшета. Она будет описана далее в этой главе.)

Живые плитки работают более или менее аналогично плиткам в Windows 8.1. Допускается менять размер каждой плитки, упорядочивать их по группам, задавать для каждой группы описательное название.

Приложение Параметры

Ярлык Параметры (Settings) в Windows 10 – аналог приложения Параметры ПК (PC Settings) из Windows 8. Значки, представленные на рис. 2-3, значительно отличаются от Панели управления (Control Panel) в Windows 7.

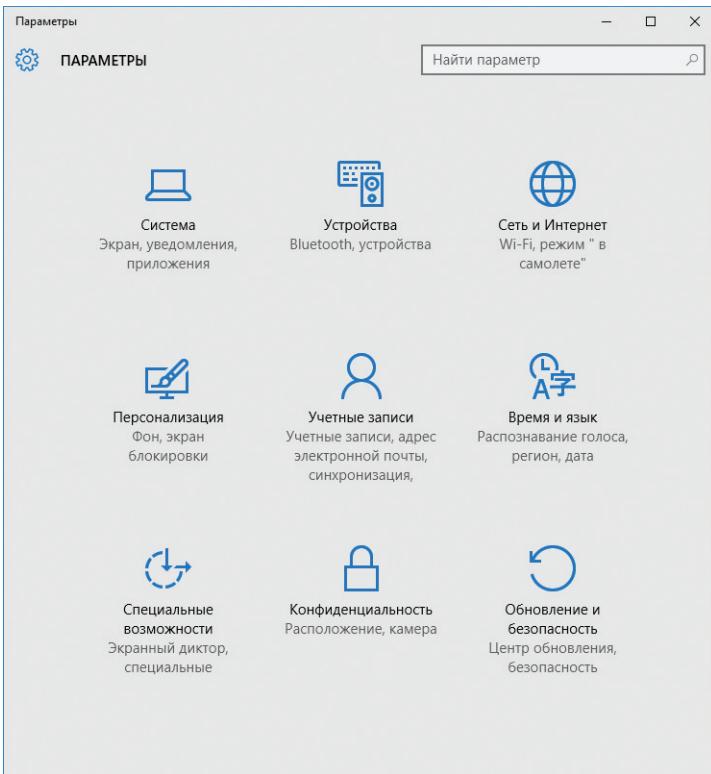


Рис. 2-3. Приложение Параметры (Settings) спроектировано с учетом сенсорного ввода и позволяет выполнять самые распространенные задачи конфигурации

Роль Панели управления (Control Panel) в Windows 10 существенно уменьшилась. Начиная с Windows 8, настройки постепенно переносились в приложение Параметры (Settings), и чаще всего соответствующий элемент удалялся из панели управления. Этот процесс продолжается и после выпуска Windows 10.

Панель Система (System), представленная на рис. 2-4, – типичный пример этого процесса. В самом последнем выпуске Windows 10 щелчок или касание пункта Питание и спящий режим (Power & Sleep) вызывает только ограниченные опции. Ярлык внизу Дополнительные параметры питания (Additional Power Settings) ведет на знакомую страницу Электропитание (Power Options) в Панели управления (Control Panel) (см. рис. 2-5).

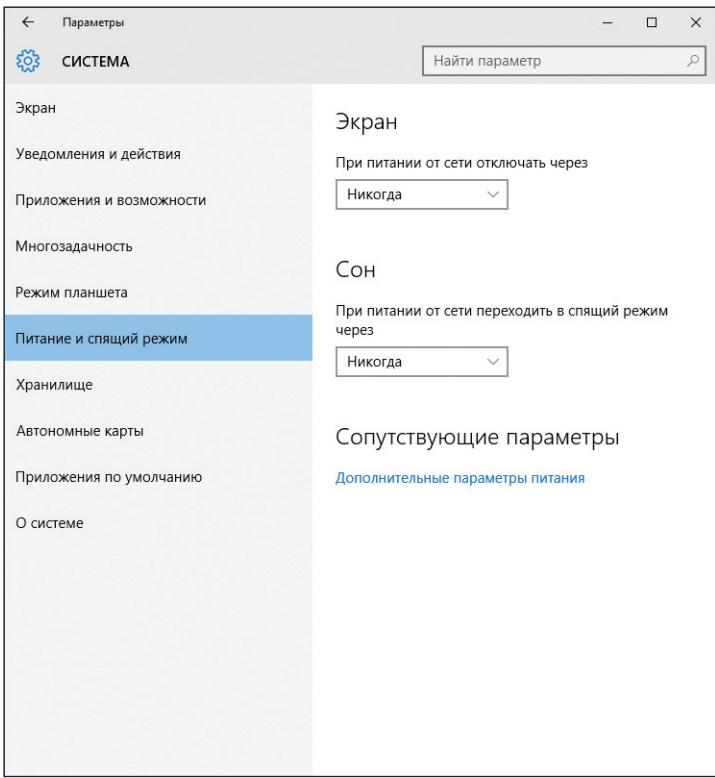


Рис. 2-4. Число опций в приложении Параметры (Settings) постоянно растет, но некоторые задачи все равно предлагают только ограниченный набор настроек

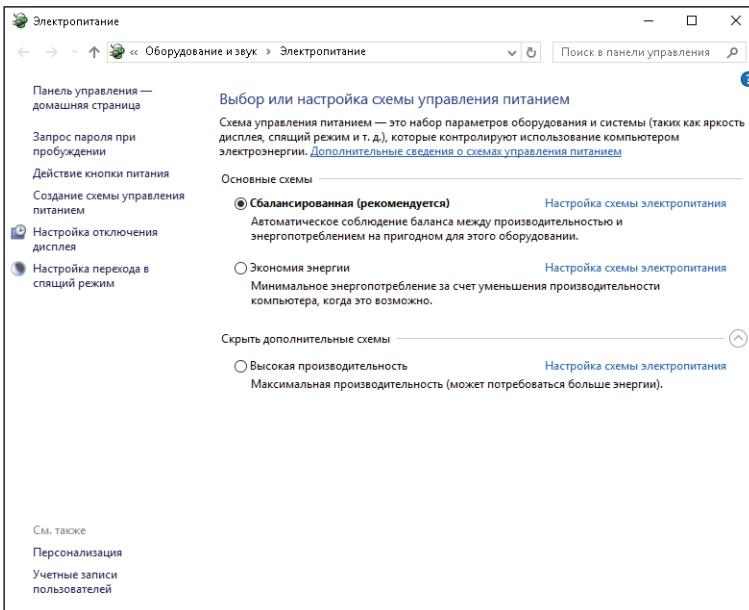


Рис. 2-5. Редко используемые задачи конфигурации все еще требуют обращения к Панели управления (Control Panel)

В общем, ярлыки на типичные задачи находятся в новом приложении Параметры (Settings), а более сложные или редкие задачи (особенно задачи по администрированию) требуют обращения к настольной Панели управления (Control Panel) и связанным утилитам.

Уведомления и кнопки действий

В Windows 10 полностью убрано меню Чудо-кнопки (Charms) – значимая возможность Windows 8 и 8.1. На планшете или ПК с сенсорным экраном, работающими под управлением Windows 10, жест смахивания с правого края экрана влево открывает Центр уведомлений (Action Center), в котором группируются уведомления приложений, а внизу находятся кнопки действий.

Значок слева от системных часов «подсвечивается», если имеются новые уведомления, и снова становится темным, когда пользователь очищает список.

Пример центра уведомлений представлен на рис. 2-6. Группа кнопок действий развернута и показывает полную коллекцию кнопок на этом устройстве. (По умолчанию видны только первые четыре.)

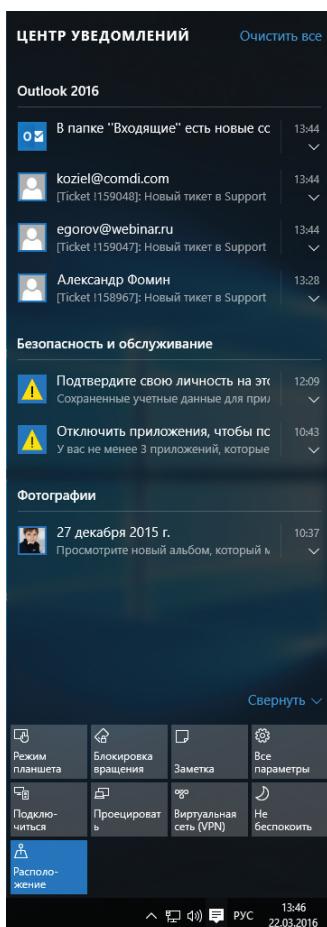


Рис. 2-6. В области уведомлений показываются сообщений от приложений, онлайн-служб, самой операционной системы, а также содержатся кнопки действий

Список из четырех кнопок действий, которые показываются по умолчанию, можно изменить, можно также развернуть всю группу. (Доступный список зависит от самого устройства.)

Кортана*

Кортана – одна из самых важных возможностей Windows 10. Она объединяет локальный и веб-поиск с возможностью распознавания голосовых команд и преобразования этих команд в задачи, встречи или инструкции. По сути, Кортана действует как персональный ассистент, изредка показывая свой «дерзкий» характер (имя и голос взяты из игры Halo на Xbox). (Прим. переводчика: Кортана для русскоязычных пользователей недоступна.)

На рис. 2-7 представлена организационная работа Кортаны.

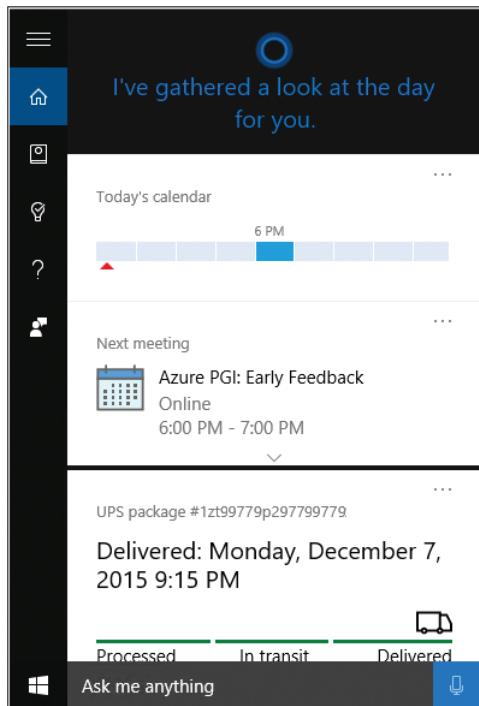


Рис. 2-7. Кортана позволяет управлять календарем, отслеживать путевые листы и отправления, читать новости, производить вычисления и искать ответы на вопросы в Интернете

По умолчанию на Windows 10 Кортана не включена. При первом щелчке в поле справа от кнопки Пуск (Start) Кортана дает возможность включить себя. Запретить пользователям в организации общаться с Кортаной можно с помощью групповой политики. На рис. 2-8 представлен параметр Разрешить использование Кортаны (Allow Cortana), который доступен по пути Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Найти (Computer Configuration > Administrative Templates > Windows Components > Search).

* Доступна не во всех регионах

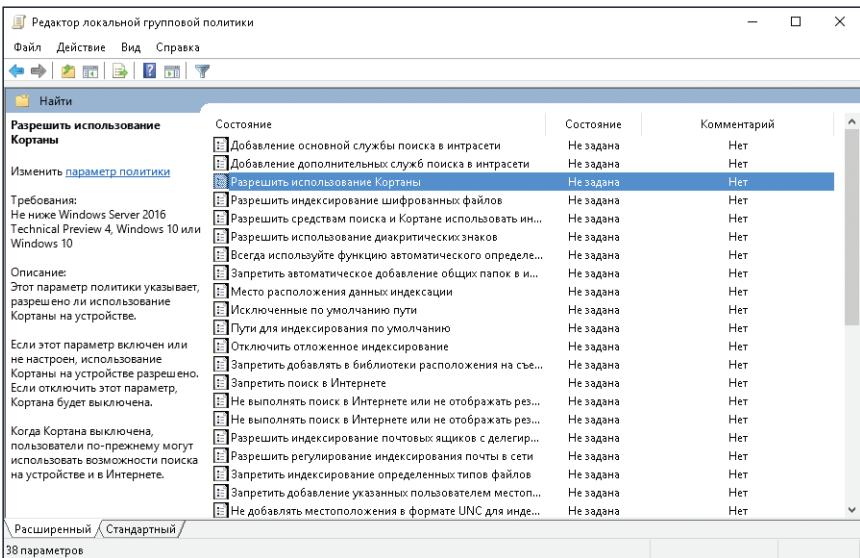


Рис. 2-8. Эта настройка групповой политики позволяет отключить службу Кортаны на управляемых ПК

Если Кортана не включена, то поле справа от кнопки Пуск (Start) позволяет выполнять простой поиск по локальной файловой системе, настройкам и веб-контенту без персонализации и подключения к личным данным.

Кортана была частью Windows Phone около года, а в предварительном выпуске Windows 10 она появилась в конце января 2015. Поскольку «магия» Кортаны связана с веб-службами, с возрастом она становится умнее. То, что доступно в текущих выпусках, – лишь доля того, что будет через год (два, три) постоянных совершенствований.

Чтобы запустить Кортану, введите что-нибудь в поле справа от кнопки Пуск (Start) или щелкните на значке микрофона и произнесите что-нибудь.

Немного освоившись, посмотрите на записную книжку Кортаны (значок сразу под кнопкой Домой [Home] в панели навигации слева). Здесь можно настроить информацию – новости, предстоящие встречи, погоду, напоминаний и т. д. (Эта сводка заменяется результатами поиска, как только пользователь начинает что-то вводить.)

Список категорий записной книжки, представленный на рис. 2-9, не является полным. Каждая категория будет дополняться опциями по ходу развития Кортаны. Воспользовавшись прокруткой, вы увидите такие дополнительные категории, как Weather, Sports и Reservations, в них вы можете разрешить Кортане сканировать электронную почту для поиска определенных тем.

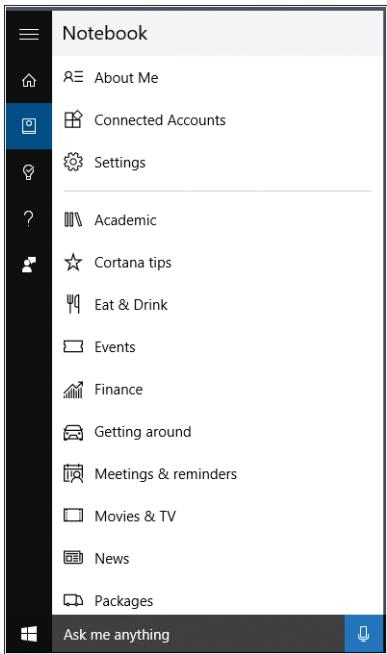


Рис. 2-9. Записная книжка предлагает пользователям детальный контроль над тем, какую информацию должна сортировать Кортана

Универсальные приложения в окнах изменяемого размера

Если вы поддерживаете группу пользователей, работающих с Windows 8 или Windows 8.1, то вы уже знаете о преимуществах приложений из Windows Store – легкая установка, повышенная безопасность, проще использование на устройствах с сенсорным экраном. Вам наверняка знакомы и основные жалобы: работа с приложениями из Windows Store, которые в основном работают на полном экране, радикально отличается от работы с настольными приложениями Windows. Необходимость переключения между этими режимами сильно раздражает, особенно тех пользователей, которые большую часть времени пользуются рабочим столом.

Другой проблемный момент использования приложений из Windows Store в Windows 8 и Windows 8.1 – это переход между приложениями. На сенсорном экране это весьма простой процесс: достаточно смахнуть экран с левого края вправо. Но при использовании мыши или трекпада жест переключения к другому приложению потребует перемещения указателя мыши в верхний левый угол, ожидания, пока появится строка с миниатюрами, а затем выбор миниатюры нужного приложения.

В Windows 10 все эти проблемы решены.

Приложения из Windows Store теперь могут выполняться в окнах изменяемого размера, которые можно перетаскивать по рабочему столу, закреплять в панели задач, сворачивать и раз-

ворачивать, а также использовать любые другие доступные для настольных приложений методы управления.

Стандарты дизайна современных приложений развиваются, но один элемент встречается все чаще и чаще. В верхнем левом углу, сразу под строкой заголовка, имеется «гамбургер-меню», названное так из-за трех горизонтальных линий, которые напоминают котлетку между двумя булочками. При щелчке или касании «гамбургера» обычно открывается меню вдоль левого края экрана, которое сворачивается в узкую строку значков, когда не используется. На рис. 2-10 представлены «гамбургер-меню» из трех встроенных приложений: Почта (Mail), Новости (News) и Фотографии (Photos).

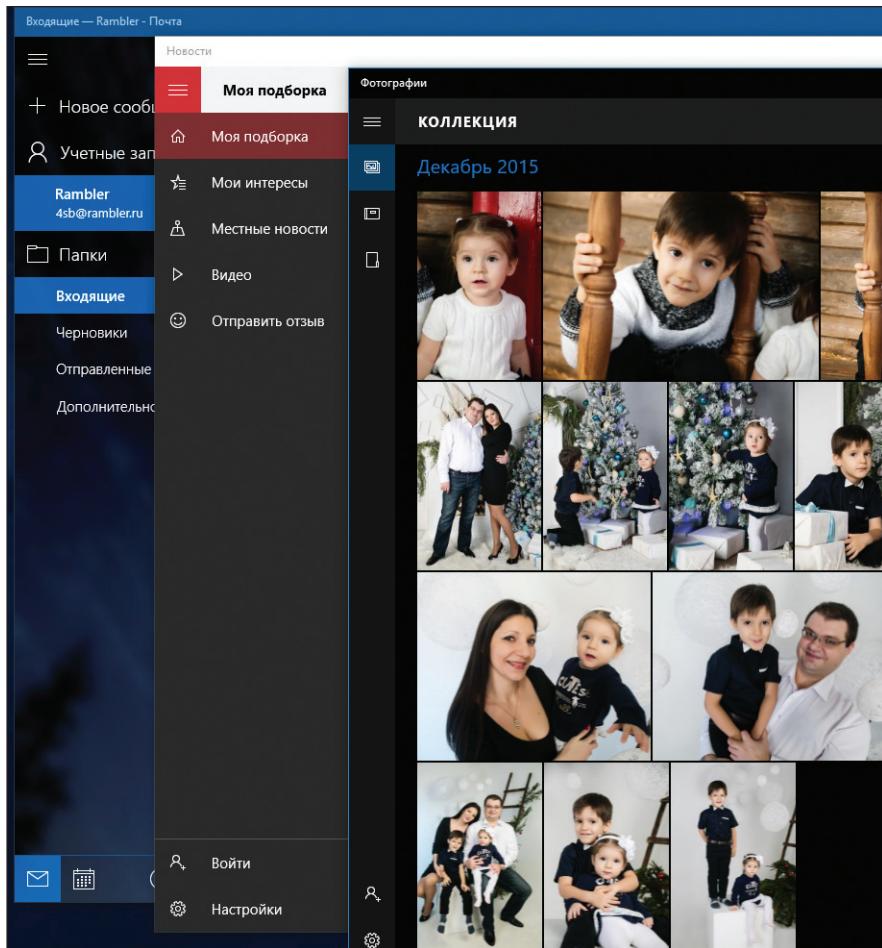


Рис. 2-10. Windows-приложения, которые могли работать только на полный экран или будучи привязанными к одной из его сторон, теперь могут работать в окнах изменяемого размера. Для поиска настроек и команд приложения используйте «гамбургер-меню» в верхнем левом углу

Навигация

Как уже упоминалось ранее, навигация в стиле «горячих углов» из Windows 8 больше не поддерживается. Вместо этого в Windows 10 можно переключиться в представление задач и щелкнуть или коснуться нужного приложения из коллекции миниатюр пропорционального размера, показвающих все открытые окна.

На планшете или устройстве с сенсорным экраном открыть представление задач позволяет жест смахивания с левого края экрана вправо. При использовании мыши и клавиатуры нужно нажать комбинацию клавиш `Windows + Tab`. Можно также щелкнуть или прикоснуться к кнопке Представление задач (Task View) на панели задач сразу справа от поля поиска.

На рис. 2-11 представлено представление задач на ПК с Windows 10 версии 1511 с семью доступными для переключения окнами задач.

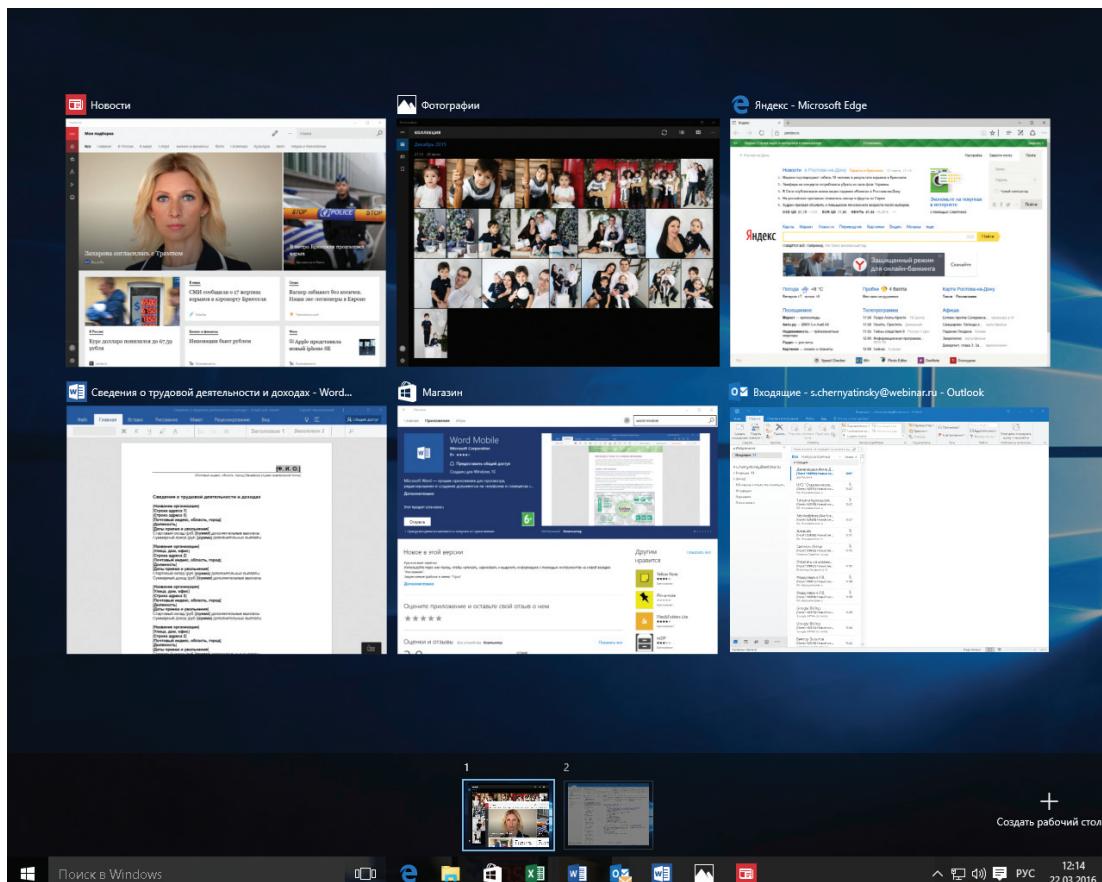


Рис. 2-11. В представлении задач каждое работающее приложение и каждая открытая страница настроек или окно Проводника (File Explorer) получают свою собственную миниатюру для быстрого переключения между задачами

Если на рис. 2-11 вы видите только шесть задач, присмотритесь. На втором виртуальном рабочем столе, переключиться к которому можно с помощью щелчка или касания, тоже выполняется программа.

В Windows 10 также усовершенствовано поведение прикрепления окон (функция Aero Snap) из Windows 7. В Windows 10 окно можно прикрепить к любой из сторон, чтобы оно заняло половину экрана, или же к любому из четырех углов, чтобы оно заняло квадрант экрана.

При прикреплении окна к любой из сторон Windows 10 предполагает, что пользователь хочет прикрепить рядом другое окно, вероятно, чтобы скопировать данные из веб-страницы и вставить их в документ Microsoft Word или же переместить файлы между окнами Проводника. Чтобы облегчить выбор второго приложения, Windows 10 показывает миниатюры всех других окон рядом с прикрепленным, как показано на рис. 2-12. (Щелкните на пустом месте, чтобы отказаться от прикрепления второго окна.)

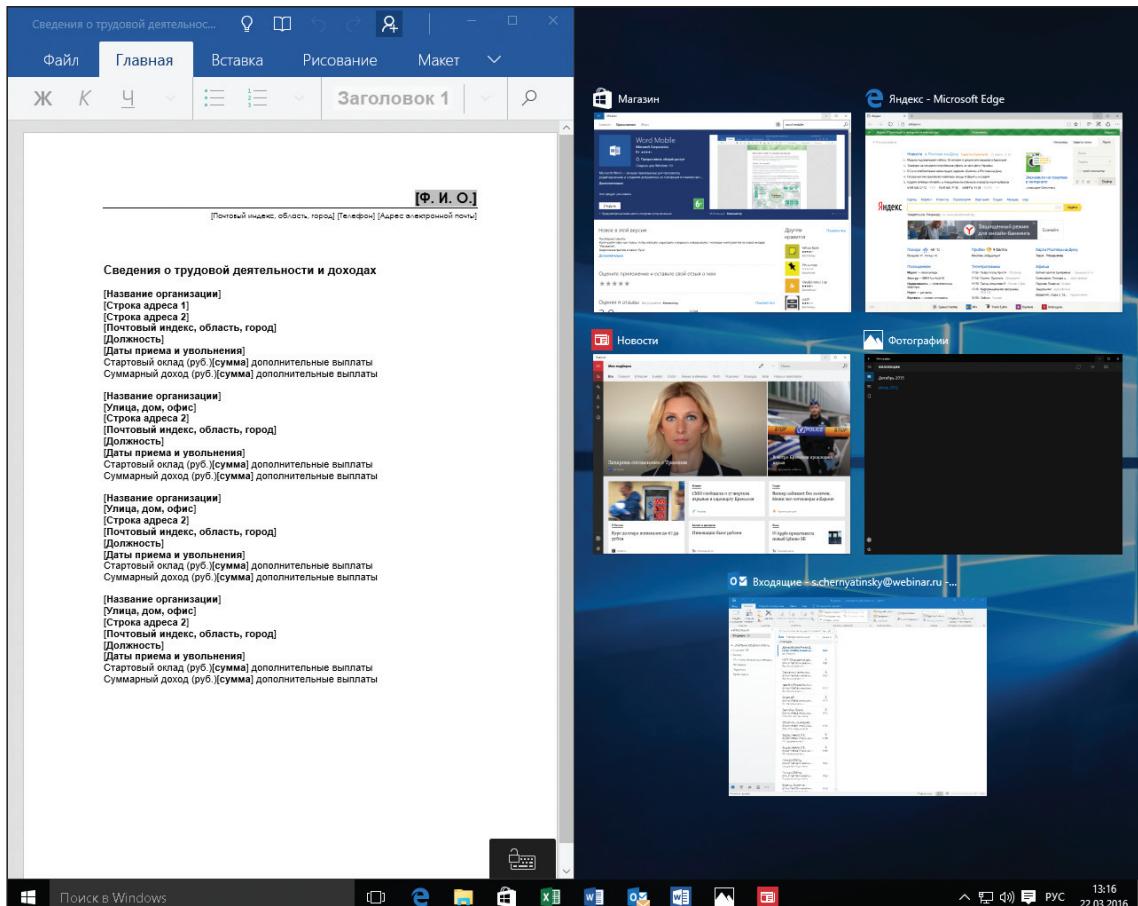


Рис. 2-12. При прикреплении окна к одной из сторон экрана Windows 10 предполагает, что пользователь хочет прикрепить второе окно рядом, и отображает миниатюры доступных окон

Режим планшета

Большинство описанных изменений предлагают явные преимущества для людей, использующих ПК или ноутбук в традиционной манере: с помощью клавиатуры и мыши или трекпада.

В случае планшета (или гибридного устройства с поворотным сенсорным экраном) методы навигации меняются.

Войдите в режим планшета (Tablet Mode), выполнив смахивание с правого края экрана и коснувшись кнопки действия Режим планшета (Tablet Mode) внизу области уведомлений. (Режим планшета подходит для некоторых задач на традиционном ПК: выполните важное приложение на полном экране, чтобы увеличить доступное пространство и не отвлекаться ни на что другое. Эта опция недоступна с несколькими мониторами.)

Когда включен режим планшета, меню Пуск (Start) разворачивается на полный экран, поле поиска сворачивается в значок, и каждое приложение выполняется в полноэкранном режиме. Можно прикрепить окно к одной из сторон экрана, но в этом случае оно будет занимать полную высоту экрана, а между прикрепленными окнами будет толстая черная полоска, как показано на рис. 2-13.

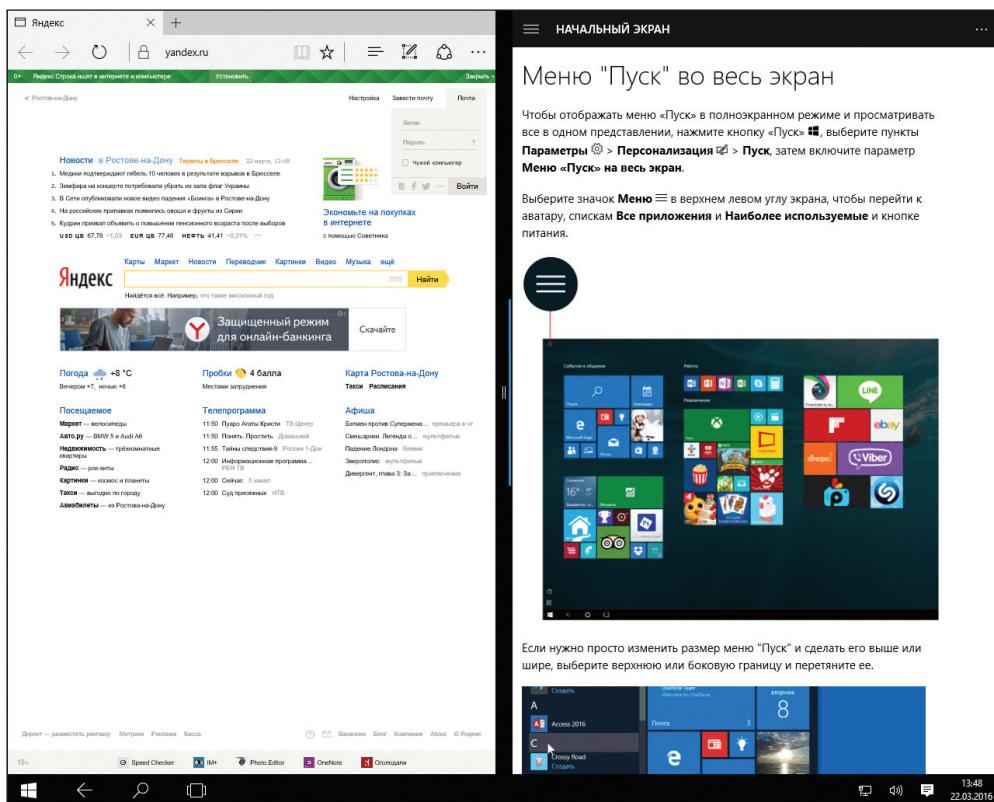


Рис. 2-13. В режиме планшета изменять размеры окон нельзя. Приложения работают в полноэкранном режиме, если не закрепляются рядом друг с другом, как показано здесь

Проводник

IT-профессионалы и опытные пользователи проводят немало времени, управляя файлами, поэтому стоит упомянуть о некоторых изменениях в Проводнике (File Explorer) в Windows 10.

При переходе с Windows 7 на Windows 10 новинкой будет смена названия с Windows Explorer на File Explorer. Следующее изменение, уже знакомое тем, кто использовал Windows 8.1, – это добавление лент в стиле Microsoft Office вместо меню и панелей инструментов.

На рис. 2-14 представлено типичное окно проводника с выбранной контекстной вкладкой Средства работы с рисунками (Picture Tools).

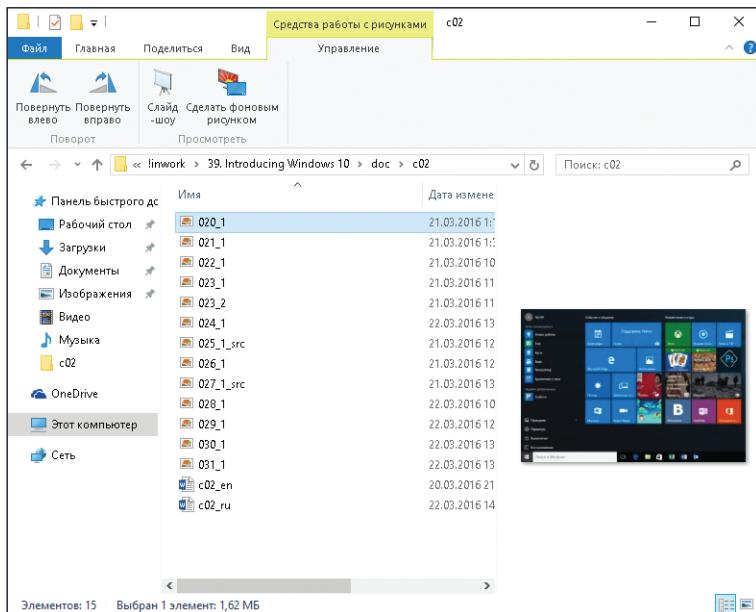


Рис. 2-14. Для тех, кто переходит с Windows 7, размещение команд в лентах – это самое большое изменение в Проводнике

В панели слева настраиваемый список быстрого доступа заменил список Избранного из предыдущих версий. Библиотеки можно отобразить или скрыть. (По умолчанию они скрыты.)

Поиск файлов стал гораздо проще благодаря опциям «наведи и щелкни» на ленте Поиск (Search), которая была введена в Windows 8. Лента Средства поиска (Search Tools), представленная на рис. 2-15, отображается автоматически при щелчке в поле поиска. Дополнительные фильтры поиска «наведи и щелкни» доступны из самого поля поиска.

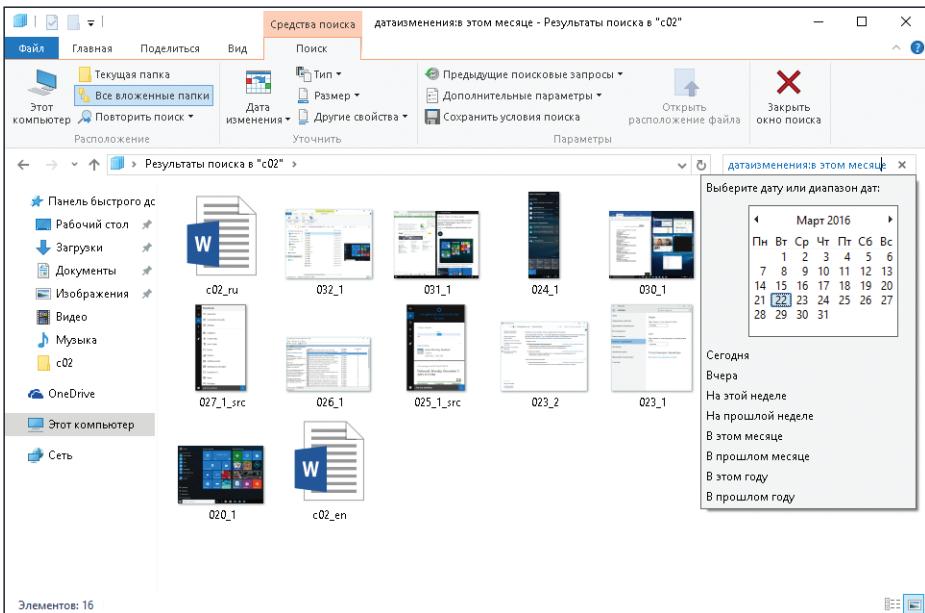


Рис. 2-15. В Windows 10 при щелчке в поле поиска в Проводнике открывается вкладка Средства поиска (Search Tools) ленты с опциями «наведи и щелкни» для фильтрации и поиска файлов

Другие, не столь значительные, изменения Проводника в Windows 10 включают новый значок Поделиться (Share), который позволяет поделиться файлом, группой файлов или папкой с любым приложением, которое поддерживает эту функцию. В диалоговом окне Параметры папок (Folder Options) теперь имеется раскрывающийся список, позволяющий выбрать объект верхнего уровня при открытии нового окна проводника.

Подключения к облаку

Долгосрочная дорожная карта для Windows 10 включает универсальный клиент синхронизации, который объединяет доступ к файлам на одной или обеих службах облачного хранения компании Microsoft. OneDrive – это бесплатная пользовательская служба, которая предлагает 5 ГБ бесплатного места. Дополнительное пространство приобретается за плату или вместе с подпиской Office 365 Home или Personal. OneDrive for Business – это функция подписок Office 365 Business и Enterprise, которая предлагает хранилище как часть рабочей или школьной учетной записи.

С декабря 2015 клиент синхронизации OneDrive обновляется независимо от Windows.

Теперь доступен новый унифицированный клиент OneDrive. Он поддерживает подключение к пользовательским учетным записям и к учетным записям OneDrive for Business, а также задание узлов верхнего уровня в Проводнике. При начальной настройке клиента синхронизации (или в любое время позднее) можно воспользоваться опцией сохранения пространства, выбрав для сохранения в OneDrive конкретные папки, а не все содержимое, как показано на рис. 2-16.

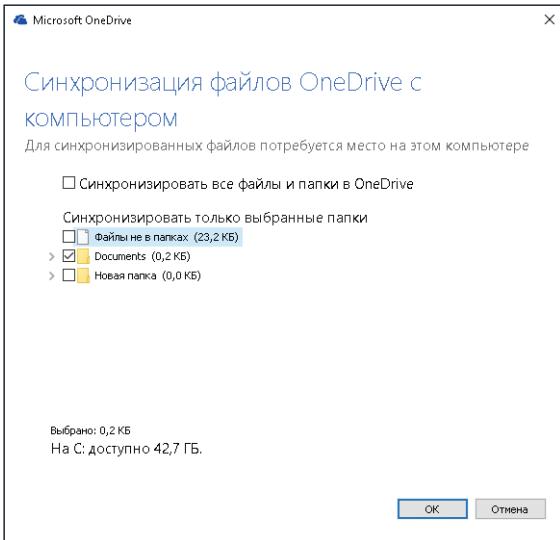


Рис. 2-16. Новый универсальный клиент синхронизации OneDrive, поставляемый вместе с Windows 10, позволяет пользователям OneDrive for Business экономить место, выбрав конкретные папки вместо синхронизации всей библиотеки файлов

Заполнители файлов (file placeholders) – функция, которая была доступна в Windows 8.1 и ранних предварительных выпусках Windows 10. Эта функция позволяла Проводнику отображать полное содержимое хранилища данных OneDrive без фактической синхронизации файлов. Эта функция была убрана из Windows 10 в предварительном выпуске в конце 2014 года. Microsoft объяснила это решение тем, что с ней было слишком много проблем в плане удобства использования и надежности. Команда разработчиков OneDrive обещает вернуть эту возможность (или ее эквивалент) в будущем выпуске клиента синхронизации.

Установка и активация

Установка и активация Microsoft Windows 10 необходимы для любого ПК. В зависимости от того, обновляете ли вы свой собственный ПК или выполняете развертывание Windows 10 в организации, вам понадобятся разные инструменты и методики. В этой главе рассматриваются интерактивные методы установки (чистая установка и обновление) для отдельных ПК. В главе 4 рассматриваются инструменты и методики развертывания в организации.

Для малого бизнеса и домашних офисов, не имеющих формальной IT-инфраструктуры, использовать инструменты развертывания непрактично. Но даже если у вас имеется спреда развертывания, полезно понимать, как установить Windows 10 ПК с нуля. Эти навыки позволяют управлять пилотными проектами в организации, а также поддерживать системы дома или во внебиржевое время.

В этой главе рассматриваются три самых распространенных варианта установки: обновление с предыдущей версии операционной системы, чистая установка и предустановленная Windows 10 на новом ПК. Сюда также включено детальное обсуждение активации Windows, поскольку детали установки и активации в Windows 10 существенно отличаются.

Совместимость и подготовка

Если вы уже начали планирование широкомасштабного развертывания Windows 10, примите наши поздравления! Вы опередили абсолютное большинство коллег. Если же вы еще не готовы начать миграцию, сделайте сейчас две вещи, чтобы облегчить себе жизнь в будущем.

- Во-первых, проведите инвентаризацию существующего оборудования и определите, что нужно докупить или заменить.
- Во-вторых, начните несколько пилотных проектов, чтобы познакомиться с Windows 10.

Существующие устройства с сенсорным экраном и Windows 8.1 предлагают прямой путь обновления до Windows 10 с помощью Windows Update.

Для традиционных настольных ПК и ноутбуков (без сенсорного экрана), работающих под управлением Windows 7 Service Pack 1, тоже имеется прямой путь до Windows 10. В действительности Windows 10 доступна как бесплатное обновление для любого ПК с правильно активированной копией Windows 7 или Windows 8.1 («Подлинной Windows»).

Windows 10 также совместима с большинством ПО виртуализации, в том числе Hyper-V в Windows Server и Windows 8.1.

Системные требования

Аппаратные требования для Windows 10 идентичны требованиям Windows 7 и Windows 8.1, поэтому любое устройство, на которых может работать одна из этих операционных систем, может работать и под управлением Windows 10. Кроме того, большинство настольных приложений, которые работают на Windows 7, также должны работать на Windows 10.

Для установки Windows 10 понадобится свободное место (как минимум 16 ГБ для 32-разрядных версий и 20 ГБ для 64-разрядных) и достаточный объем ОЗУ (как минимум 1 ГБ для 32-разрядных версий, 2 ГБ для 64-разрядных), иначе установка будет заблокирована.

С Windows 10 несовместимы следующие типы устройств.

- Surface RT и другие устройства с Windows RT несовместимы с Windows 10.
- В некоторых более старых ЦП нет функций, которые нужны для Windows 10. Процессор должен поддерживать Physical Address Extensions (PAE); Data Execution Protection через функцию защиты страниц No-eXecute (NX) или функцию eXecute Disable (XD) bit; инструкции SIMD Extensions 2 (SSE2). Кроме того, на некоторые модели старых ПК нельзя установить 64-разрядную версию, поскольку их процессоры не поддерживают такие инструкции, как CMPXCHG16b, PrefetchW и LAHF/SAHF.
- Операционная система Windows 10 Mobile, хотя и тесно связанная во многих отношениях с Windows 10, доставляется отдельно. Редакции Windows 10, созданные для установки на ПК, не будут работать на телефонах.

Поддерживаемые пути обновления

Обновление через Windows Update – это самый простой вариант, поскольку позволяет сохранить все установленные настольные программы, приложения из Windows Store, персональные файлы и настройки. При использовании этого варианта для обновления используется та же редакция Windows 10, что и для предыдущей системы. Так, Windows 7 Home Premium обновляется до Windows 10 Home, а Windows 7 Professional и Ultimate или Windows 8.1 Pro обновляются до Windows 10 Pro.

Можно также произвести обновление с меньшей редакции до большей – например, с Windows 8.1 Core до Windows 10 Pro. Дополнительная информация о вариантах обновления будет приведена далее в этой главе.

Создание и использование установочного носителя

Начиная с Windows 10, Microsoft делает установочный носитель широко доступным. (См. страницу <https://www.microsoft.com/ru-ru/software-download/windows10>.) Чтобы обновить один ПК с наименьшими усилиями, щелкните на кнопке Обновить сейчас и следуйте подсказкам.

Чтобы найти более гибкий набор вариантов, включая возможность создать загрузочный USB-накопитель или DVD с установочными файлами Windows 10, прокрутите эту страницу и загрузите небольшую утилиту Средство для создания носителя (Media Creation Tool). На рис. 3-1 представ-

лено это средство после выбора опции Создать установочный носитель для другого компьютера (Create Installation Media For Another PC).

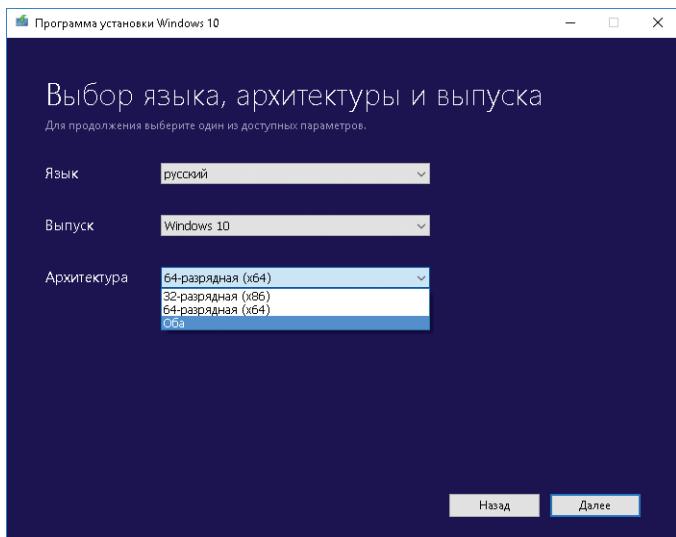


Рис. 3-1. Средство для создания носителя загружает установочные файлы Windows 10, которые могут использоваться на нескольких ПК и в виртуальных машинах

Если вы загружаете установочные файлы для обновления нескольких ПК, выберите нужные опции в трех списках на этой странице: язык (на декабрь 2015 доступно около 40 языков), редакцию (большинство выбирает Windows 10, а не урезанную редакцию Windows 10 N), а также архитектуру (32-разрядную, 64-разрядную или обе архитектуры).

Следующий набор параметров, представленный на рис. 3-2, позволяет загрузить файлы и немедленно создать загрузочный USB-диск для установки на нескольких компьютерах или загрузить файлы в файл образа диска (ISO).

Формат ISO – наиболее универсальный вариант. Если дважды щелкнуть на ISO-файле, можно подключить его как диск в Windows 8.1 или Windows 10, а затем запустить программу установки с подключенного диска. ISO-файл также можно подключить к виртуальной машине (ВМ) как виртуальный DVD-диск, чтобы выполнить чистую установку или обновление в этой ВМ.

Из ISO-файла очень легко создать загрузочный флэш-диск. Выберите опцию из Windows 8.1 или Windows 10 для создания диска восстановления (но не выбирайте опцию копирования системных файлов). Затем подключите ISO-образ в Проводнике и перетащите содержимое диска восстановления, перезаписывая существующие файлы. По окончании копирования вы получите загрузочный установочный диск Windows 10.

Установочный носитель для Windows 10 Enterprise через это средство недоступен. Используйте один из следующих вариантов.

- Клиенты с соглашением Volume License могут получить самые последние ISO-файлы из центра Volume Licensing Service Center.

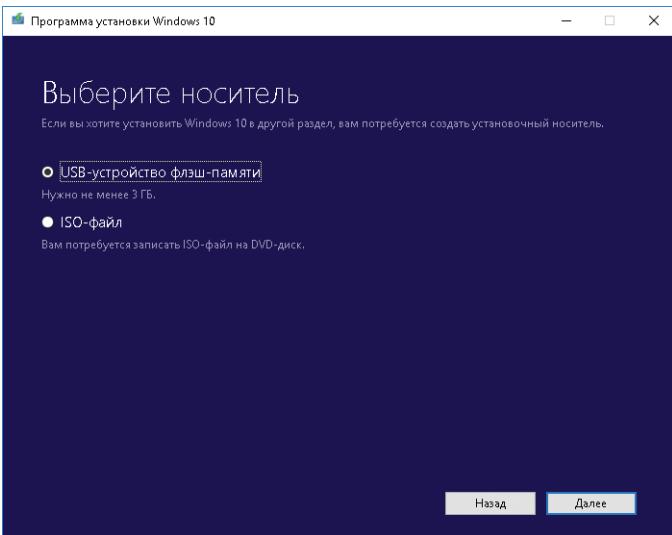


Рис. 3-2. Средство для создания носителя позволяет создать загрузочное USB-устройство флэш-памяти или сохранить установочные файлы в образе диска ISO

- MSDN-подписчики могут войти в центр загрузок MSDN и найти широкий диапазон файлов, в том числе редакции Enterprise и Education для использования в разработке и тестировании приложений.
- Если ни один из этих платных вариантов не подходит, можно загрузить ознакомительную версию Windows 10 Enterprise, доступную для 90-дневного неограниченного использования. Детали и ссылки для загрузки см. по адресу: <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>.

Новые правила активации

Все последние 15 лет, начиная с Windows XP активация продукта была частью Windows. Windows 10, как и ее предшественницы, требует активации как часть лицензионного соглашения. Обычно этот процесс выполняется автоматически – Windows проверяет ключ продукта (или другой авторизованный метод) на сервере активации, чтобы убедиться, что установленная версия соответствует ключу продукта и устройству разрешено использовать соответствующую лицензию Windows.

Windows 10 позволяет выполнить установку без ввода ключа продукта. Причины этого мы обсудим чуть позднее в этом разделе. Можно пропустить ввод ключа и продукта и отложить активацию, но в этом случае определенные возможности будут недоступны.

Проверить статус активации устройства с Windows 10 позволяет вкладка Активация (Activation) в разделе Обновление и безопасность (Update & Security) приложения Параметры (Settings). На рис. 3-3 представлена эта информация для системы, которая была обновлена с Windows 8.1 Pro до Windows 10 Pro.

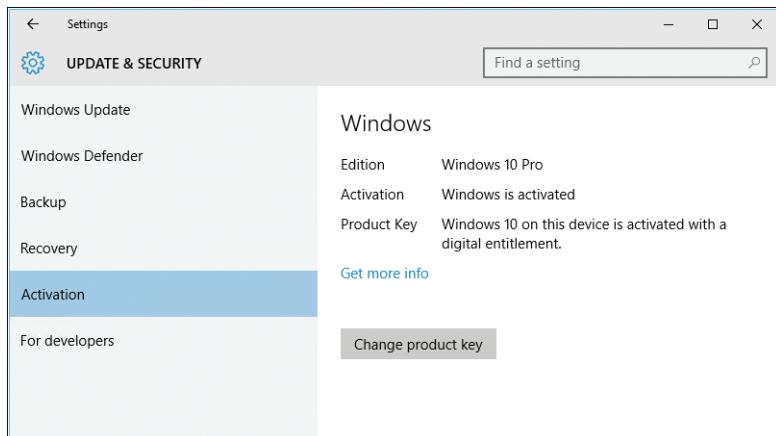


Рис. 3-3. Windows 10 добавляет новый тип активации, «цифровое разрешение», при котором не требуется вводить ключ продукта для активации

Концепция активации с использованием «цифрового разрешения» (digital entitlement) является новой в Windows 10. Она создана, чтобы можно было обновить ПК, на котором работает правильно активированная копия Windows 7 или Windows 8.1. При запуске программы установки из-под этих версий Windows вводить ключ не понадобится. Windows проверяет правильность активации и создает цифровое разрешение на основе уникального идентификатора оборудования.

При использовании загрузочного установочного носителя для выполнения чистой установки на ПК, который ранее был обновлен и получил цифровое разрешение, не нужно вводить ключ продукта. По окончании установки Windows свяжется с серверами активации и отправит идентификатор оборудования. (Передается кэш идентификатора, поэтому никто не сможет определить конкретное устройство.) Когда сервер находит сохраненное цифровое разрешение для этого идентификатора оборудования, система активируется автоматически.

При использовании загрузочного установочного носителя для выполнения чистой установки на ПК, который не был обновлен до Windows 10 и активирован, понадобится ввести ключ продукта для активации системы. Если установочный носитель соответствует Windows 10 версии 1511 (сборка 10586) или выше, то можно ввести ключ продукта соответствующей редакции Windows 8, Windows 8 или Windows 8.1. В этом случае также будет создано цифровое разрешение, и в будущем не потребуется вводить ключ продукта.

Чтобы просмотреть детальную информацию по активации текущей установки Windows, понадобится открыть окно командной строки с правами администратора и ввести команду `slmgr.vbs /dlv`. На рис. 3-4 представлен полный вывод для той системы, статус активации которой показан на рис. 3-3.

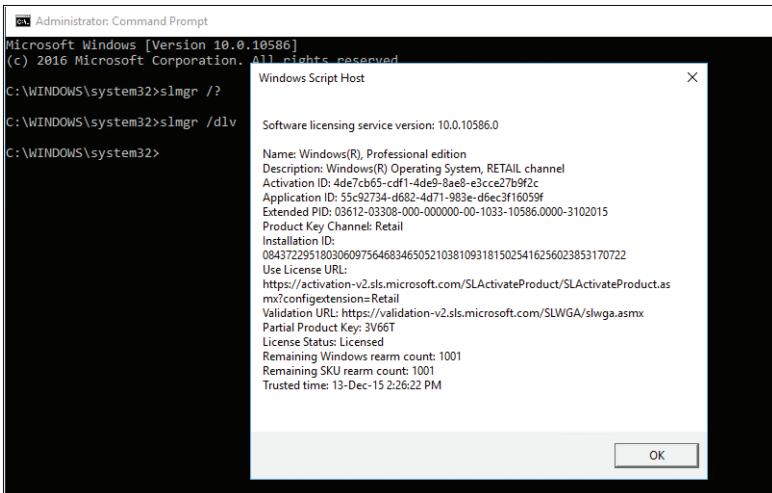


Рис. 3-4. Используйте сценарий slmgr.vbs для просмотра статуса лицензирования. (Чтобы просмотреть все доступные опции, воспользуйтесь переключателем -?)

Доступны и другие варианты активации.

- Новые ПК с предустановленной производителем Windows 10 активируются автоматически. Лицензионная информация закодирована в прошивку устройства, что позволяет переустановить ту же редакцию Windows без ввода ключа продукта.
- Розничные и OEM-копии, доступные через реселлеров, включают ключ продукта, которые могут использоваться для активации конкретной редакции Windows 10, которая никогда не активировалась.
- Клиенты с Volume License могут использовать MAK-ключи (Multiple Activation Keys) или Key Management Server для активации правильно лицензированных копий Windows 10 Enterprise.

Варианты установки Windows 10

На новом ПК, который поставляется с предустановленной Windows 10, вся работа по установке и активации уже выполнена производителем. Единственная задача пользователя – пройти через запуск при первом включении компьютера (out of box experience, OOBE), чтобы создать новую учетную запись пользователя или войти в существующую.

Обновление и чистая установка, напротив, требуют полной установки, которая проходит в несколько этапов. Скорее всего, вы уже сталкивались с этим, поэтому я не буду рассказывать, как работает программа установки Windows. Вместо этого позвольте рассказать о нескольких интересных опциях установки.

Самый простой вариант – это обновление на месте (in-place upgrade). Для развертывания большего размера можно автоматизировать этот процесс на устройствах с Windows 7 или

Windows 8.1, используя инструментарий Microsoft Deployment Toolkit (MDT), диспетчер System Center Configuration Manager или альтернативный инструмент распространения ПО. (Дополнительная информация приводится в главе 4.)

Для одного устройства разумнее всего инициализировать обновление до Windows 10 с помощью Windows Update. В период предварительного ознакомления и в первые несколько месяцев после официального выпуска Windows 10 (в июле 2015) Microsoft доставляла утилиту Get Windows 10 на все подходящие ПК. Эта утилита помещала значок в область уведомлений и предлагала пользователю зарезервировать обновление. В конце 2015 Microsoft начала предлагать вариант обновления как Необязательное (Optional) обновление и планирует доставлять программу установки как Рекомендуемое (Recommended) обновление в начале 2016 года.

На рис. 3-5 представлено обновление, готовое для установки на ПК с Windows 7.

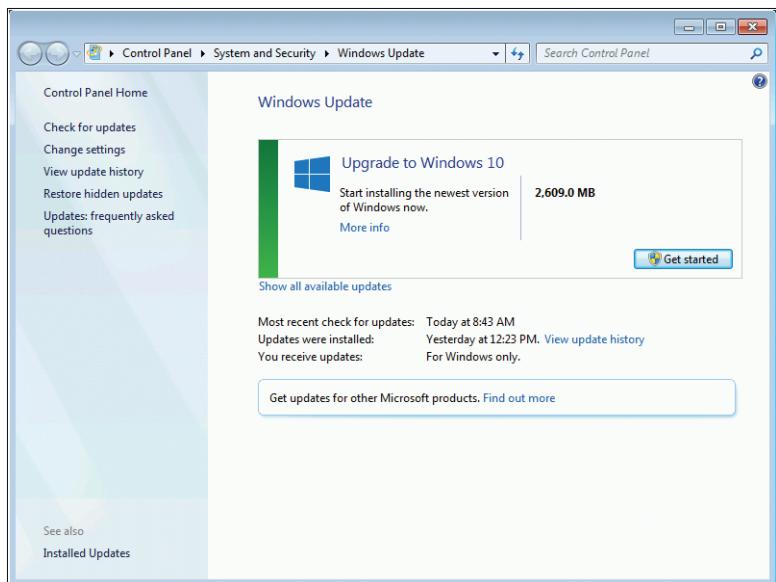


Рис. 3-5. Несмотря на значительную разницу в номерах версий, обновления с Windows 7 до Windows 10 полностью поддерживаются через Windows Update

Процесс обновления, запущенный из Windows Update, не предлагает никаких опций. Будут перенесены все учетные записи пользователей, настольные программы, приложения и файлы данных. Как правило, процесс установки не занимает больше пары часов (обычно гораздо быстрее). Установка на основе образа была протестирована за последние несколько лет на сотнях миллионов ПК. Если что-то пойдет не так, программа установки выполнит автоматический откат к предыдущей версии Windows, оставив неизменными все файлы данных и детали конфигурации.

Примечание. Не торопитесь с переходом к Windows 10 на устройстве с зашифрованным хранилищем. Процесс обновления на месте должен без проблем работать на системах, защищенных с помощью шифрования BitLocker, но программа установки

Windows не сможет получить доступ к дискам, зашифрованным сторонним ПО. Самый безопасный вариант – отключить все шифрование перед обновлением, а затем снова запустить его по окончании обновления. Перед обновлением удостоверьтесь у производителя ПО шифрования, что ПО совместимо с Windows 10.

Процесс обновления с Windows 7 или Windows 8.1 можно начать, используя физический установочный носитель или подключенный ISO-файл и дважды щелкнув на Setup на установочном носителе. Этот вариант вызывает знакомый процесс обновления Windows. В начале будут предложены дополнительные опции, как показано на рис. 3-6.

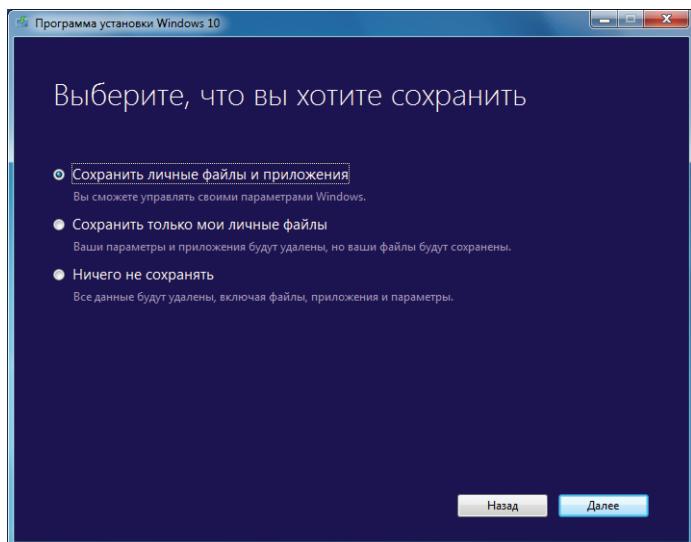


Рис. 3-6. При запуске обновления из-под Windows 7 или Windows 8.1 выбор последнего переключателя в списке эквивалентен чистой установке

Если нужно получить чистый старт, не сохраняя ранее установленные приложения или настройки, выберите опцию Сохранить только личные файлы (Keep Personal Files Only). Этот вариант сохранит все файлы данных (включая загрузки), но во всем остальном создаст стандартную установку Windows 10. Выбор последнего варианта, Ничего не сохранять (Nothing), эквивалентен чистой установке.

После выбора опций программа установки выполняет ряд операций и затем предлагает войти в учетную запись.

В любом из сценариев, если операция завершилась успешно, то на устройстве будет установлена та же редакция Widnows (Core, Pro или Enterprise), что и раньше. Файлы данных, приложения и настройки должны быть полностью перенесены.

Чтобы выполнить чистую установку, понадобится загрузиться с установочного носителя (USB-накопителя флэш памяти, DVD или ISO-файла в случае виртуальной машины). Если выбрать форматирование целевого диска, то все приложения и данные будут удалены. Если выбрать существующий том, но не очищать его, существующие файлы будут перемещены в папку Windows.old, откуда они могут быть восстановлены при необходимости.



Примечание. Не удаляйте папку Windows.old без крайней необходимости. В Windows 10 наличие этой папки позволит откатиться к предыдущей версии Windows с помощью опции Восстановление (Recovery) в приложении Параметры (Settings). (Дополнительная информация по этой возможности приводится в главе 9.) Если эти файлы больше не нужны, и требуется очистить занимаемое ими места, запустите утилиту очистки диска Windows (Cleanmgr.exe) от имени администратора. Выберите опцию Предыдущие установки Windows (Previous Windows Installation[s]), чтобы полностью удалить папку Windows.old и все ее содержимое.

Создание и управление учетными записями пользователей

При обновлении Windows 10 сохраняет существующий профиль пользователя и просит выполнить вход с использованием тех же учетных данных. На чистой установке понадобится создать первую учетную запись с нуля. В Windows 10 имеется три варианта.

- **Учетная запись Microsoft.** Это стандартный вариант для персонального устройства, которое не подключено к домену. Учетная запись Microsoft (является прямым потомком служб Passport и Windows Live ID) использует адрес электронной почты и пароль для включения различных облачных служб. Устройства с Windows 10 могут приобретать приложения и цифровое содержимое в Windows Store и синхронизировать настройки и файлы (используя OneDrive) между устройствами, вход на которое выполнен с одной и той же учетной записью. Политика сети может позволить вам связать учетную запись Microsoft с учетной записью домена, чтобы подключенная к домену машина могла пользоваться преимуществами синхронизации настроек.
- **Рабочая учетная запись.** Как IT-профессионал, вы наверняка знакомы с учетными записями домена, в которых используются учетные данные Active Directory для аутентификации пользователей и предоставления доступа к ресурсам в общей корпоративной среде. Windows 10 также включает возможность подключения к учетной записи Azure Active Directory, которая позволяет использовать облачные ресурсы, такие как Office 365. При создании рабочей учетной записи может использоваться ПО управления мобильными устройствами в корпоративной сети для разрешения устройству доступа к сети под управлением политик компании.
- **Локальная учетная запись.** Этот вариант учетной записи трудно найти в некоторых конфигурациях установки Windows, но включить учетную запись такого типа все еще можно. Учетные данные сохраняются только на локальном устройстве.

Какой тип учетной записи следует использовать?

Для ознакомления с Windows 10 в корпоративной среде подключение устройства к домену и вход с учетной записью домена – это лучший способ добиться совместимости с существующей сетью. Этот вариант требует, чтобы сначала была создана локальная учетная запись.

Вход с учетной записью Azure AD подходит для компаний, в которых все устройства управляются через Azure Active Directory.

Во всех остальных случаях лучший выбор – это учетная запись Microsoft, особенно если владелец устройства уже использует службы Microsoft и планирует использовать Windows 10 на других устройствах с той же учетной записью.

Опытным пользователям Windows бывает нелегко отказаться от локальных учетных записей, особенно если они опасаются, что персональные или деловые данные могут случайно попасть в оценочную среду.

В таком случае лучше создать не локальную учетную запись, а новую учетную запись Microsoft с помощью бесплатного адреса Outlook.com, и использовать бесплатное хранилище и электронную почту строго для тестирования. Такой вариант позволит увидеть преимущества учетной записи Microsoft с минимальным риском.

В этой стратегии есть еще одно преимущество: она позволяет включить шифрование BitLocker для поддерживаемых тестовых устройств и сохранить ключ восстановления в защищенном онлайн-хранилище.

Если используется Windows 10 Enterprise, то программа установки предполагает, что установка делается на рабочем устройстве. Если используется Windows 10 Pro, то пользователю представляется выбор, показанный на рис. 3-7.

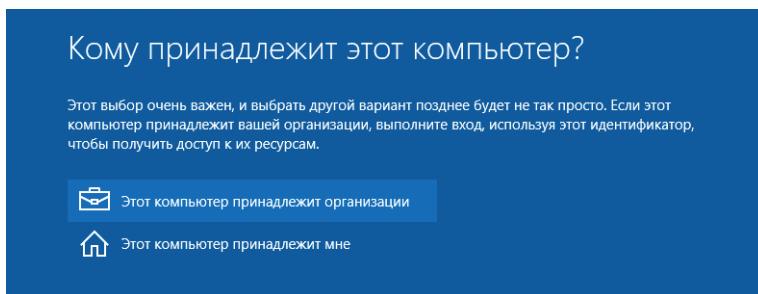


Рис. 3-7. Этот выбор доступен только при выполнении чистой установки Windows 10 Pro

При выборе первого варианта Этот компьютер принадлежит организации (My Organization) и щелчке на кнопке Далее (Next) будет открыта вторая страница с вариантами подключения к Azure AD или домену, как показано на рис. 3-8.

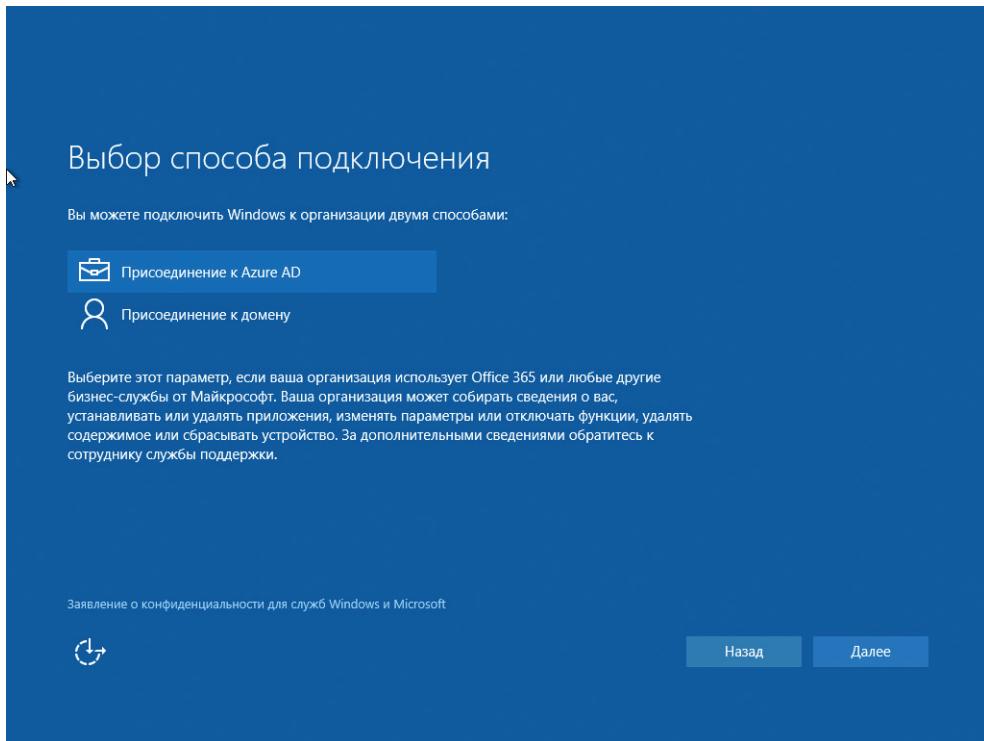


Рис. 3-8. Выбирайте первый вариант только в том случае, если компьютером и его настройками должен управлять администратор Azure Active Directory

Первый вариант работает только с существующими учетными данными Azure Active Directory, например, со связанными с учетной записью Office 365. Второй вариант помогает создать локальную учетную запись, которую затем можно подключить к домену. Введите данные вашей рабочей учетной записи в поле, представленном на рис. 3-9, только если у вас есть учетные данные Azure Active Directory, например Office 365 Business, Enterprise или Education, и вы хотите использовать эту учетную запись в качестве основного адреса входа, а не связывать его с рабочей учетной записью.

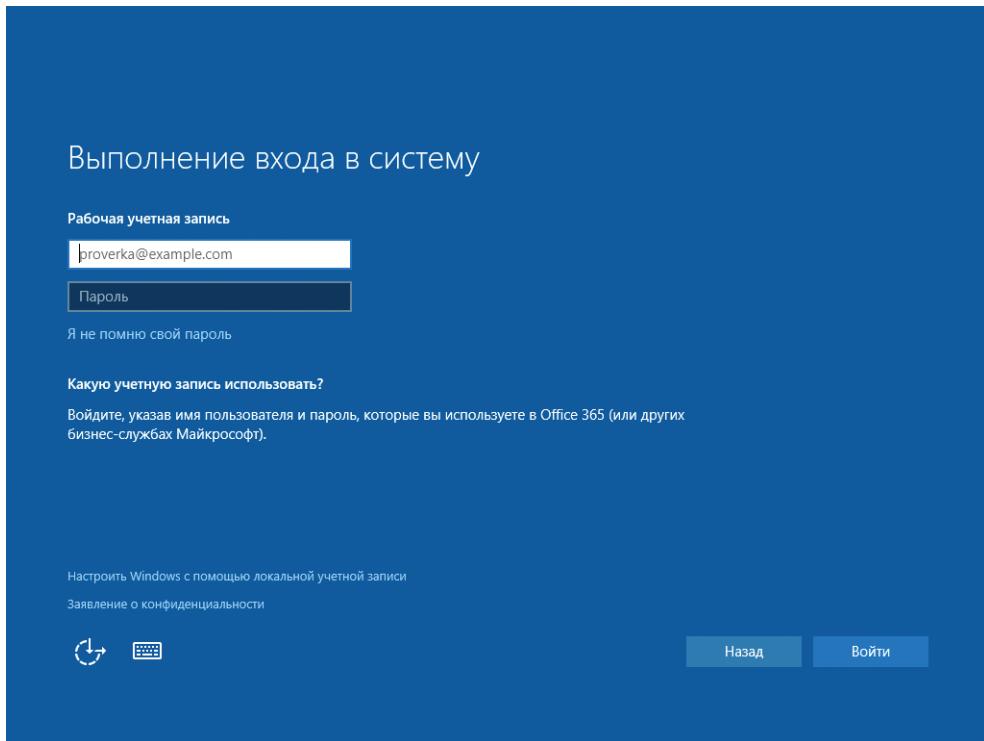


Рис. 3–9. Введите здесь учетные данные, только если у вас есть учетная запись Azure Active Directory. Если вы планируете присоединиться к локальному домену Active Directory, выберите вариант локальной учетной записи

Если вы решили создать локальную учетную запись, открывается страница, знакомая любому, кто устанавливал Windows в последние два десятилетия. Эта страница показана на рис. 3–10.

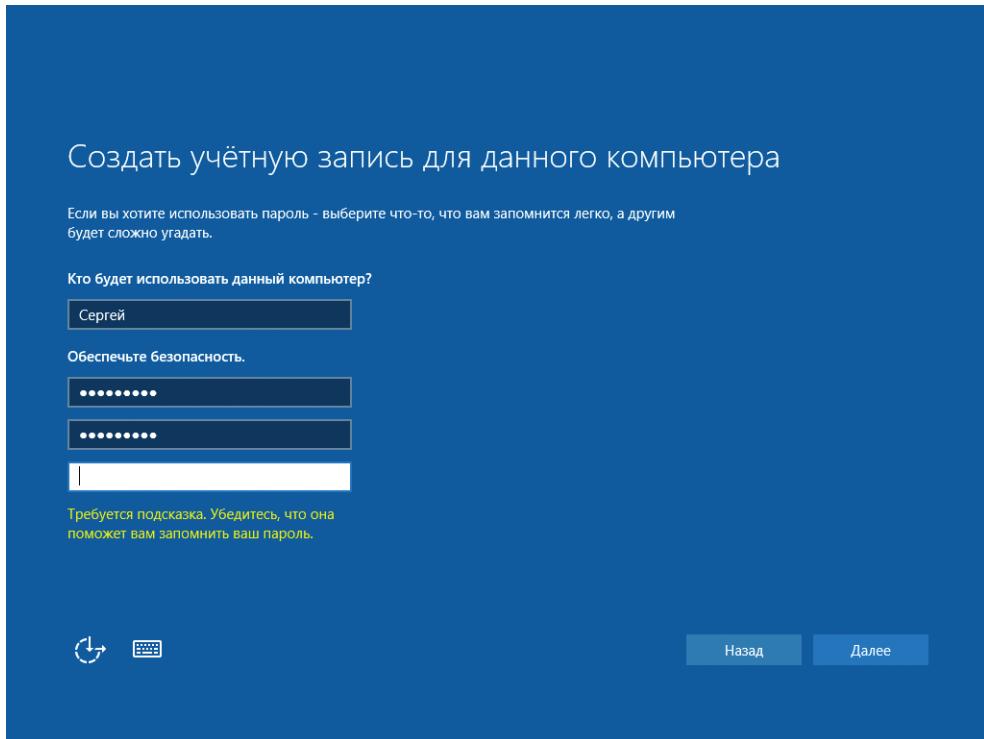


Рис. 3-10. Вариант создания локальной учетной записи хорошо скрыт, но все еще доступен

Если вы сообщили Windows, что используете персональное устройство, то будет открыта страница установки, которая настоятельно советует использовать существующую учетную запись Microsoft или создать новую. Доступные опции представлены на рис. 3-11.

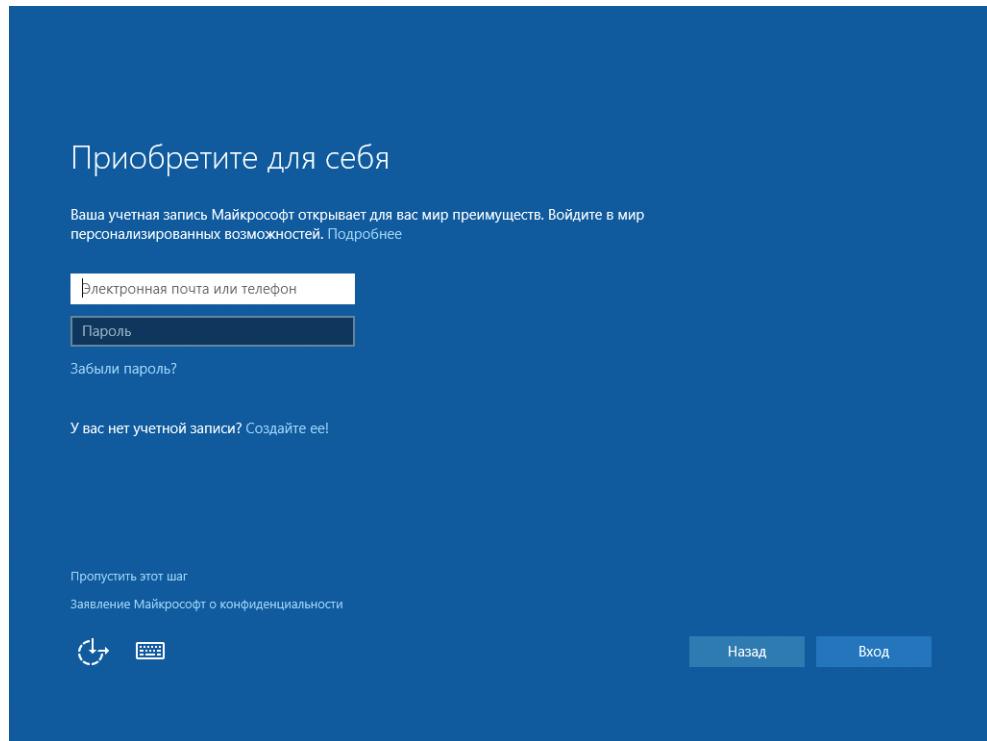


Рис. 3-11. Для большинства персональных устройств предпочтительнее использование учетной записи Microsoft

При входе с использованием учетной записи Microsoft, уже имеющейся на других устройствах, все настройки, которые были выбраны для синхронизации, будут скопированы на новое устройство. У вас будет доступ к Windows Store и любым другим облачным службам, которые связаны с этой учетной записью Microsoft, включая электронную почту Outlook.com (ранее Hotmail), OneDrive и Xbox.

На этом экране также можно создать новую учетную запись Microsoft, используя любой адрес электронной почты, даже личный адрес на стороннем домене, использовать домены Microsoft – Outlook.com, Live.com и Hotmail.com – необязательно.

Хотя это и неочевидно, но на этой странице также есть возможность создать локальную учетную запись. Щелкните или коснитесь Пропустить этот шаг (Skip This Step), чтобы открыть форму создания локальной учетной записи, представленную ранее на рис. 3-10.

ГЛАВА 4

Развертывание Windows 10 в организации

Для IT-профессионалов задача по развертыванию вычислительных ресурсов в организации повторяется циклически. Новая волна аппаратных средств становится катализатором для главного обновления операционной системы, затем приоритет смещается к сохранению платформы (за исключением обновлений безопасности), а потом приходит следующая волна обновлений, и все начинается по новому кругу.

Этот ритм радикально меняется с выпуском Microsoft Windows 10. Для корпоративных клиентов с операционными системами Windows 7 или Windows 8.1 первый шаг – перевести организацию на Windows 10. После завершения перехода целью становится поиск ритма обновлений, который позволил бы организации своевременно получать новые возможности. Даже если вы предпочтете отставать на несколько месяцев от самого передового цикла обновлений для клиентов (Текущая ветвь), почувствуйте разница между этим отставанием и работой на версиях операционных систем, которым больше пяти лет.

Новый процесс разработки компании Microsoft, со свободно доступными предварительными выпусками, позволяет вам тестировать бизнес-приложения на сборках, которые попадут в выпуск только спустя несколько месяцев. Теперь для тестирования не нужно дожидаться главного выпуска.

Инфраструктура развертывания и управления, используемая в вашей корпоративной сети, также сдвигается к более быстрому темпу разработки, соответствующему темпу обновления Windows 10. И следующая версия Windows Server, построенная на том же фундаменте, что и Windows 10, находится сейчас в состоянии технического предварительного выпуска (Technical Preview), ее заключительный выпуск состоится в 2016 году. Некоторые возможности в Windows 10 Enterprise, требующие дополнительных возможностей на стороне сервера, также будут добавлены в выпуск Windows 10 в 2016 году. Эти новые возможности иногда могут требовать обновлений в текущих версиях Windows Server.

Вот пример того, как быстро движется цикл разработки. В декабре 2015 Microsoft выпустила новую версию диспетчера System Center Configuration Manager (SCCM) с поддержкой развертывания, обновления и управления Windows 10. Менее чем через две недели появилось предварительное обновление с важными новыми возможностями. Последние обновления для старых редакций инфраструктуры System Center также включают поддержку для Windows 10.

В этой главе мы познакомимся с новыми инструментами развертывания и управления как частью пилотной программы.

Сценарии развертывания

До появления Windows 10 существовали два варианта развертывания Windows.

- Сценарий «очистка и загрузка», который начинается со стандартного образа, созданного для работы с оборудованием и приложениями компании. Используя инструменты развертывания, вы полностью заменяете существующий образ на новом ПК (или на ПК, образ на котором нужно заменить по причинам поддержки или как часть процесса переназначения новому сотруднику).
- Обновления на месте, которых исторически остерегались IT-профессионалы. Все мы слышали массу ужасных историй о неудачных обновлениях. Однако начиная с Windows 8 процесс обновления был полностью переделан – теперь он быстр и чрезвычайно надежен, содержит возможности легкого отката для тех редких случаев, когда что-то все таки пойдет не так.

Windows 10 добавляет третий вариант развертывания: создание пакетов подготовки, которые могут трансформировать существующий образ на новом ПК. Этот вариант все еще находится в начале своего развития, но имеет огромный потенциал.

Годами многие IT-профессионалы, ответственные за большие сети на основе Windows, использовали вариант «очистка и загрузка» как стандартное решение для развертывания новых операционных систем. Этот вариант подходит для развертываний «раз в три года» и для эпизодической подготовки новых устройств. Это также прекрасный способ перехода с Windows 7 или Windows 8.1 на Windows 10, особенно если новые приложения вводятся как часть обновления операционной системы.

Однако такой вариант затратен и неэффективен, когда операционная система получает несколько обновлений в год – вам придется каждые четыре-шесть месяцев создавать новые образы и управлять переносом данных и переустановкой приложений для множества развертываний в организации.

В эру «Windows как услуга» гораздо более рациональная альтернатива – обновление на месте.

Microsoft уже сделала это при развертывании Windows 10 на десятках тысяч устройств по всему миру. При развертывании использовалась функция Operating System Deployment (OSD) в System Center 2012 R2 Configuration Manager SP1 для предложения автоматических обновлений на месте пользователям с Windows 7, Windows 8 и Windows 8.1.

Microsoft предлагала два варианта развертывания. Пользователи могли инициировать обновление из Software Center в удобное для них время. На рис. 4-1 показано, как работает этот инициируемый пользователем (pull, извещающий) вариант.

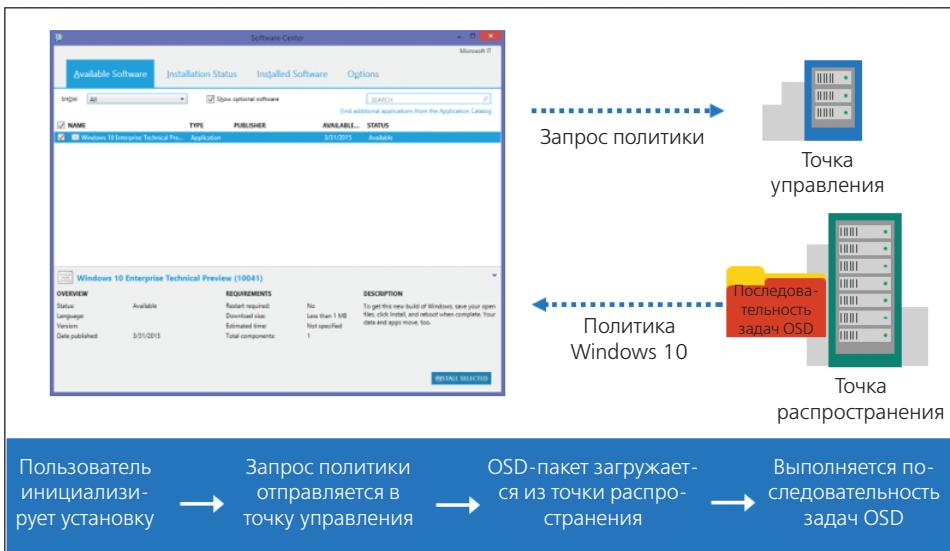


Рис. 4-1. IT-персонал компании Microsoft использовал этот процесс, чтобы пользователи сами выбирали, когда они хотят начать процесс обновления до Windows 10

Эти инициируемые пользователем обновления использовали тот же движок установки Windows, что и в потребительских версиях Windows 10. Он выполняет ряд проверок совместимости, чтобы избежать известных проблем с приложениями, драйверами, версиями BIOS и других проблем, которые могут помешать успешной установке. Если целевая система проходила эти проверки, программа установки производила обновление.

На рис. 4-2 представлена последовательность задач OSD в диспетчере Configuration Manager. Построение этой последовательности управляется мастером, который позволяет определить задачи, которые должны быть выполнены перед обновлением, и действия, которые должны быть выполнены в случае сбоя.

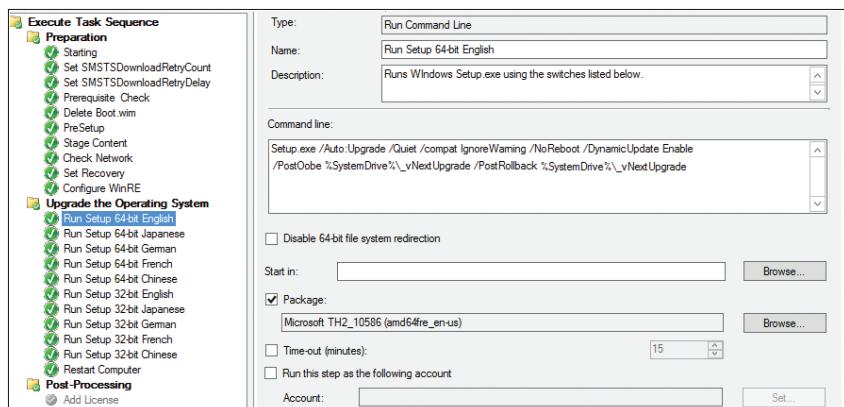


Рис. 4-2. Используйте мастер для создания последовательности задач, которая позволит развернуть обновление Windows 10 с помощью методик «pull» (извещающий) или «push» (проталкивающий)

Установочные файлы доставлялись через корпоративную сеть, содержимое для обновления бралось с публичных серверов Windows Update.

Если сотрудники не произвели обновление к определенной дате, IT-персонал Microsoft мог «протолкнуть» (push) для них пакет обновления как запланированное действие. Обычно эти принудительные обновления планировались во вторники и четвергги во время обеда. Вернувшись с обеда пользователи могли наблюдать заключительные шаги установки и начать работать с Windows 10.



Примечание. Детальное обсуждение того, как IT-персонал компании Microsoft выполнил обновление до Windows 10, см. в документе (в формате .docx) по адресу: <https://www.microsoft.com/en-us/download/details.aspx?id=50377>.

Результат? Приблизительно 85 % всех компьютеров сотрудников были обновлены в течение четырех недель. Для сравнения, в 2009 году на развертывание Windows 7 традиционным методом с настраиваемыми образами на 80 % всех компьютеров сотрудников ушел почти год.

Обзор средств развертывания в организациях

Средства развертывания в организациях от компании Microsoft охватывают все сценарии, которые обсуждались ранее в этой главе. Как и со множеством Windows-задач, имеется масса средств на выбор. Нельзя сказать, что какие-то методы правильные, а какие-то неправильные, хотя некоторым инструментам отдается предпочтение. В общем, следует выбирать инструменты, которые наилучшим образом работают с вашей существующей или планируемой инфраструктурой.

Эти инструменты могут использоваться и индивидуально, но они наиболее эффективны, когда вы создаете решение с использованием инструмента управления, такого как Microsoft Deployment Toolkit (MDT) или Microsoft System Center Configuration Manager.

Microsoft Deployment Toolkit 2013

На момент написания этой книги (начало 2016 года) самая последняя доступная версия – это Microsoft Deployment Toolkit 2013 Update 2. (За полной информацией по MDT обратитесь по адресу: <https://technet.microsoft.com/en-us/windows/dn475741.aspx>. Ссылка для загрузки: <https://www.microsoft.com/en-us/download/details.aspx?id=50407>.)

Не позволяйте более старой дате одурачить себя. Этот выпуск поддерживает развертывание и обновление всех редакций Windows 10, включая редакции Enterprise LTSB и Education. Инструментарий также поддерживает Windows ADK для Windows 10 и включает самые последние двоичные файлы последовательностей задач для интеграции с System Center 2012 R2 Configuration Manager SP1 и позднее для развертываний Windows 10.

На рис. 4-3 представлен ход создания настраиваемого образа с опцией использования собственных драйверов вместо применения драйверов с помощью Plug and Play.

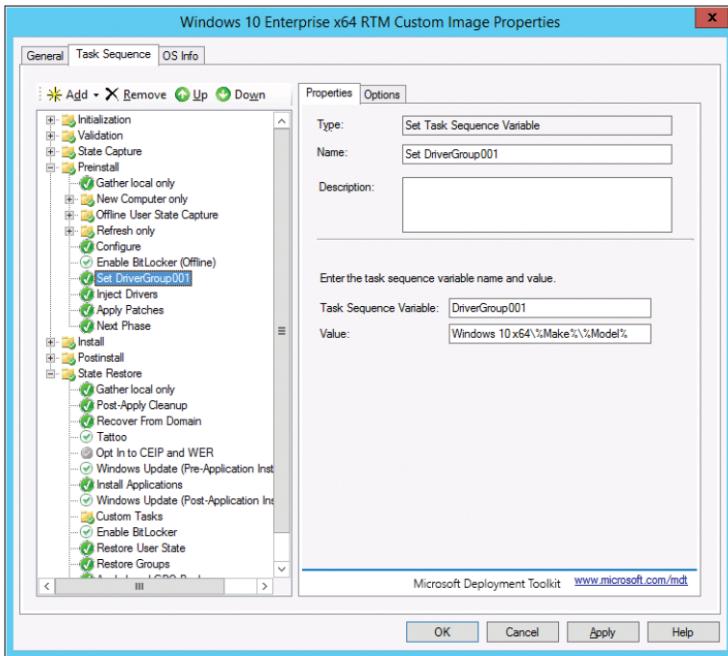


Рис. 4–3. Microsoft Deployment Toolkit предлагает возможность создания последовательностей задач, которые могут применяться к обновлению операционной системы на ПК в сети

Windows Assessment and Deployment Kit

Инструментарий Windows Assessment and Deployment Kit (ADK) для Windows 10 содержит основные инструменты для автоматизации широкомасштабного развертывания Windows 10. Независимо от используемого диспетчера развертывания (MDT или SCCM), для выполнения развертывания понадобятся части ADK.

Если вы уже использовали ADK с предыдущими развертываниями Windows, вам определенно понравится самая последняя версия. Новый ADK включает значительные усовершенствования.

- **Поддержка подготовки.** Эта функция позволяет создавать специальные пакеты для настройки новых устройств Windows 10 и «подготовки» их для использования в организации без необходимости очищать предустановленный OEM-образ и загрузки собственного образа.
- **Сжатие системных файлов.** Windows 10 может выполнятся напрямую из сжатых файлов. Эффект похож на функцию WIMBoot, которая была введена в обновлении Windows 8.1. Новый процесс гораздо элегантнее (и гораздо эффективнее), поскольку используются отдельные файлы вместо статичного образа Windows Image (WIM). При обновлении системных файлов Windows 10 заменяет старые файлы, а не хранит обе копии.

Кроме того, ADK содержит документацию для двух полезных возможностей, которые входят в состав Windows 10.

- **Быстрый сброс параметров** (Push-button reset). Эта функция, доступная с версии Windows 8, теперь включает по умолчанию системные обновления. Когда пользователь использует опцию Сбросить (Reset) для восстановления, новый образ остается актуальным, так что переустанавливать новые обновления не потребуется.
- **Частичные языковые пакеты.** Вместо добавления полных языковых пакетов (которые могут занимать достаточно много места на диске) можно добавить только основные файлы пользовательского интерфейса для языка. При необходимости Windows загрузит полные языковые пакеты через Windows Update при включении таких функций, как рукописный ввод или распознавание речи.

Если вы знакомы с предыдущими выпусками ADK, то в этом выпуске вы найдете несколько интересных добавлений, включая Windows Imaging and Configuration Designer, Windows Assessment Toolkit, Windows Performance Toolkit и несколько новых и улучшенных инструментов развертывания. Последние включают обновленный Windows Driver Kit (WDK), Hardware Lab Kit (HLK), Software Development Kit (SDK) и Assessment and Deployment Kit (ADK).

Начиная с этого выпуска, документация Windows ADK доступна в центре MSDN Hardware Dev Center – [https://msdn.microsoft.com/library/windows/hardware/dh927348\(v=vs.85\).aspx](https://msdn.microsoft.com/library/windows/hardware/dh927348(v=vs.85).aspx).

На рис. 4-4 представлены опции, доступные в ходе установки Windows ADK.

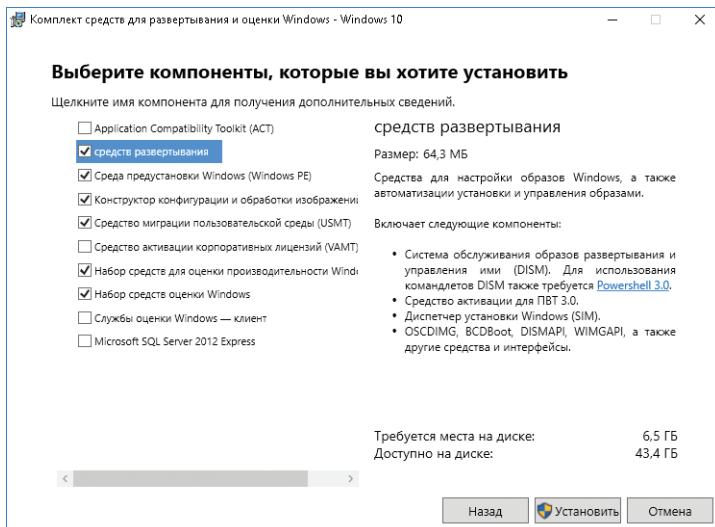


Рис. 4-4. Новый Windows Assessment and Deployment Kit предлагает опции для IT-профессионалов и производителей аппаратных средств

Ниже приводятся ключевые части ADK и их роль для задач развертывания, включая управление настраиваемыми образами.

- **Deployment Image Servicing and Management (DISM).** Этот инструмент используется для подключения и обслуживания образов Windows. С его помощью можно настраивать автономный образ и добавлять драйверы, включать или отключать компоненты Windows, добав-

лять или удалять пакеты и универсальные приложения Windows, а также обновить редакцию Windows. DISM также включает командлеты PowerShell.

- **Windows Preinstallation Environment (Windows PE).** Это (очень) маленькая операционная система, которая обычно размещается на загрузочном устройстве, таком как USB-диск, флэш-память или DVD. Она используется для загрузки компьютера, на котором еще не установлена Windows. Windows PE также используется для восстановления данных и операций исправления.
- **Windows System Image Manager.** Этот инструмент используется для создания и настройки файлов ответов, которые изменяют настройки Windows и выполняют сценарии в ходе установки.
- **Windows Imaging and Configuration Designer (Windows ICD).** Будучи новинкой в Windows 10, этот инструмент позволяет создавать пакеты подготовки для настройки устройств с Windows 10 без удаления старого и записи нового образа. Он также позволяет создавать и развертывать образ для настольных редакций Windows 10. Этот инструмент мы рассмотрим чуть ниже.
- **User State Migration Tool (USMT).** Цель этого инструмента – перенос профилей пользователей из старой операционной системы в новую, обычно как часть развертывания вида «очистка и загрузка».
- **Windows Assessment Toolkit и Windows Performance Toolkit.** Эти инструменты предназначены, главным образом, для OEM-производителей для оценки качества и производительности систем или компонентов.

Windows ICD заслуживает более глубокого обсуждения и пристального внимания во время оценки, см. рис. 4-5.

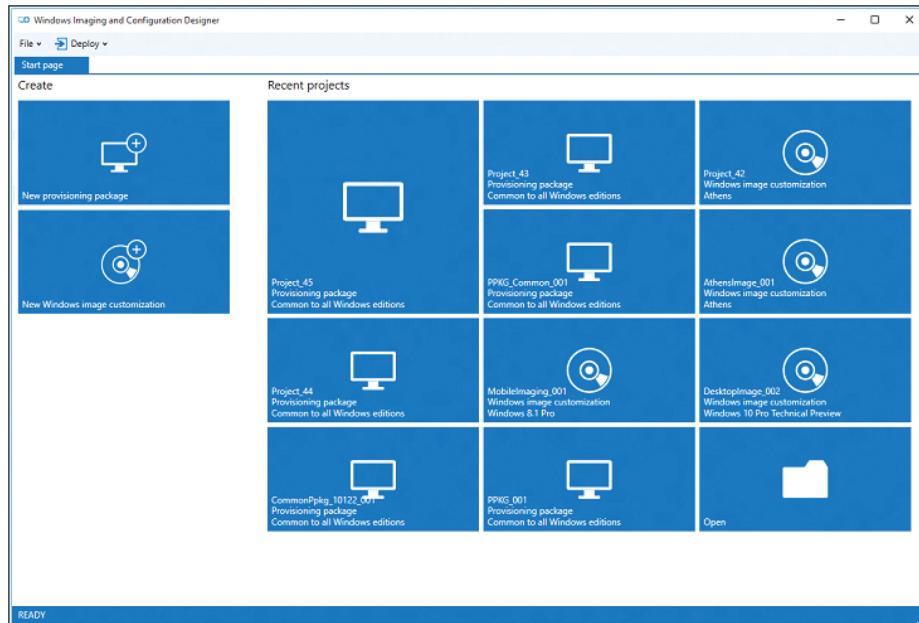


Рис. 4-5. Windows Imaging and Configuration Designer (ICD) может создавать пакеты подготовки, которые позволяют настраивать существующий образ или могут применяться к работающей системе

Использование Windows ICD требует установки дополнительных возможностей ADK, в частности коллекции Deployment Tools, Windows PE и USMT.

На странице Customizations, представленной на рис. 4-6, можно определить настройки в подготовительном пакете; также можно добавить приложения, драйверы, компоненты по запросу, языковые пакеты и обновления Windows.

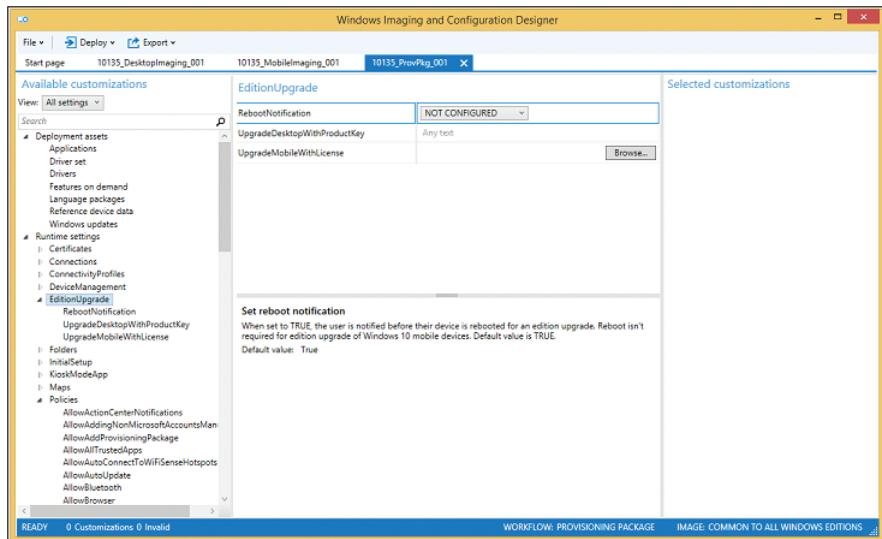


Рис. 4–6. Варианты настройки Windows ICD позволяют обновить редакцию как часть применения пакета

ГЛАВА 5

Защита и конфиденциальность в Windows 10

Мicrosoft Windows 10 гораздо эффективнее, чем ее предшественницы, защищает организацию и пользователей и от распространенных, и от экзотических угроз. Конечно, это неудивительно. После запуска в 2002 году инициативы Trustworthy Computing каждая новая версия Windows включает значительные усовершенствования безопасности.

Для обеспечения безопасности предназначены наборы элементов управления или предупреждений, такие как Защитник Windows (Windows Defender) и фильтр SmartScreen, который блокирует потенциально опасные загрузки. Windows 10 также включает очень важную для обеспечения безопасности аппаратную защиту, которая работает до загрузки Windows, и возможности защиты на базе сети, которые могут определяться и применяться администраторами с помощью групповой политики и инструментов управления.

Windows 10 также включает новую функцию безопасности, которая позволяет защитить самое слабое звено в современной компьютерной безопасности. Новые функции идентификации в Windows 10, созданные на основе сложных биометрических сенсоров и легкой в применении мультифакторной аутентификации, могут полностью заменить пароли, устранив тем самым целый класс угроз безопасности.

В наше время, когда известия о новых брешах в защите данных появляются практически каждую неделю, забота о конфиденциальности становится первоочередной задачей. Чтобы обеспечить подход «Windows как услуга», Windows 10 собирает данные диагностики и аналитики с ПК, включая информацию о возможностях устройства, сообщения об ошибках и данные по использованию.

В этой главе автор предлагает обзор нескольких уровней безопасности в Windows 10 и детально описывает опции конфиденциальности для отдельных ПК и управляемых сетей.

Эволюция многообразия угроз

Эксперты компьютерной безопасности любят говорить о «многообразии угроз» (threat landscape) – широком и постоянно растущем наборе способов, с помощью которых злоумышленники могут атаковать устройства и сети. В прошлом основным мотивом хакерства была личная слава. Сегодня организованные криминальные группы превратили киберата-

ки в большой бизнес, получая прибыль с помощью выкупа (ransomware), накручивания числа кликов по ссылке (click fraud) и кражи конфиденциальных данных. Атакующие могут интересоваться кражей секретов или причинением вреда и разрушением и по политическим мотивам.

Вредоносное ПО и фишинговые атаки неразборчивы в целях. Целевые атаки, напротив, нацелены на выявление слабых мест в больших организациях. Государственные организации и компании, ведущие бизнес в важных областях промышленности – оборона, банки и энергетика - всегда должны быть готовы противостоять потенциальным атакам хорошо финансируемых и технически грамотных аутсайдеров.

Не стоит рассчитывать на то, что ваша организация слишком маленькая и не может стать целью компьютерного преступления. Если ваш малый бизнес связан с одной из больших целей, даже не напрямую, как субподрядчик или часть цепочки поставщиков, – то вы можете попасть под прицел как промежуточная задача на пути к большой цели.

Многообразие угроз включает вредоносное ПО и вторжения, а также утечку данных, неавторизованный доступ к локальным и сетевым ресурсам, физические кражи.

В общем, атаки могут происходить на любом уровне стека. Вредоносные агенты могут внедряться в ПО, во внешне невинные веб-страницы или документы, вложенные в электронные сообщения, или в пакеты в сети.

Они могут быть нацелены на уязвимости в операционной системе или в популярных приложениях. Часть наиболее успешных атак в последние годы связана с так называемой социальной инженерией (social engineering), где атакующий представляется не тем, кем является, например, подделывает имя отправителя в электронном сообщении, чтобы убедить получателя открыть вложение или посетить скомпрометированный веб-сайт.

Масштаб повреждений быстро вырастает, если атакующему удается украдь роль специалиста поддержки или администратора сети, которые вошли в скомпрометированное устройство, используя учетные данные с большим доступом к сетевым ресурсам.

Вы можете стать жертвой не по своей вине, если третья сторона хранит учетные данные незащищенными, что влечет за собой утечку данных.

Защита аппаратного обеспечения

Первый уровень защиты для устройства Windows 10 – это само оборудование. Ключевые возможности безопасности в Windows 10 (изначально представленные в Windows 8.1) используют преимущества современного аппаратного обеспечения. Хотя Windows 10 можно установить и использовать на более старом оборудовании, наилучшие результаты будут достигнуты, если присутствуют следующие возможности.

- **Единый расширяемый интерфейс прошивки (Unified Extensible Firmware Interface, UEFI).** Спустя 30 лет BIOS, наконец, устарел. Его замена – UEFI, интерфейс прошивки, который берет на себя функции, традиционно выполняемые BIOS. UEFI играет ключевую роль в защите

с Windows 10, предлагая, например, функцию Secure Boot и поддержку самостоятельно шифрующихся дисков. (Дополнительная информация об этих возможностях приводится далее в этой главе.) UEFI является обязательным требованием к OEM-производителям для сертификации системы или аппаратного устройства для Windows 8 или выше в программе Windows Hardware Certification (ранее известную как Windows Logo).

- **Trusted Platform Module (TPM).** TPM – это аппаратный чип, который поддерживает высоко-классное шифрование и предотвращает подмену или неавторизованный экспорт сертификатов и ключей шифрования. TPM может быть реализован как автономный микроконтроллер или включен как часть другого компонента, такого как сетевой модуль или система на чипе (system on chip, SoC).

TPM выполняет криптографические операции и хранит ключи для томов BitLocker и виртуальных смарткарт. TPM также может подписывать данные цифровой подписью, используя закрытый ключ, к которому у программного обеспечения нет доступа.

Наличие TPM задействует несколько ключевых возможностей в Windows 10, в том числе шифрование диска BitLocker, Measured Boot и Device Guard. Они обсуждаются далее в этой главе.

Кроме того, Windows 10 предлагает поддержку аппаратных устройств, позволяющих идентифицировать пользователей с помощью биометрической информации: отпечатка пальца, распознавания лица или сканирования радужной оболочки глаза. Windows включает поддержку биометрии с Windows XP. Windows 10 значительно совершенствует точность и целостность процесса идентификации; она позволяет зарегистрировать устройство как доверенное, поэтому биометрическая информация становится частью простых в использовании мультифакторных схем аутентификации. (Эти возможности обсуждаются в деталях далее в этой главе в разделе «Защита личности».)

При наличии аппаратной поддержки Windows 10 также может использовать преимущества технологий виртуализации для изоляции ключевых служб операционной системы, чтобы защитить их от атаки даже в случае компрометации ядра Windows 10. Служба Hypervisor Code Integrity гарантирует, что весь код, работающий в режиме ядра, включая драйверы, работает так, как задумано. Кроме того, новая функция Credential Guard изолирует службу Local Security Authority (LSA) для защиты учетных записей домена и записей, которые хранятся в Credential Manager.

Защита процесса загрузки

Самые агрессивные формы вредоносного ПО пытаются встроиться в процесс загрузки на как можно более раннем этапе, чтобы взять контроль над системой и помешать работе антивирусного ПО. Этот тип вредоносного кода часто называют руткит (rootkit) (или bootkit). Самый лучший способ избежать этого – защитить процесс загрузки с самого начала.

Windows 10 поддерживает несколько уровней защиты загрузки, которые были представлены в Windows 8.1 и недоступны в Windows 7 и более ранних версиях. Некоторые из них будут доступны, только если установлено специальное оборудование. На рис. 5-1 показано, как работает процесс загрузки в Windows 8.1 и Windows 10.

Архитектура целостности платформы Windows (Windows 8.1 и позднее)

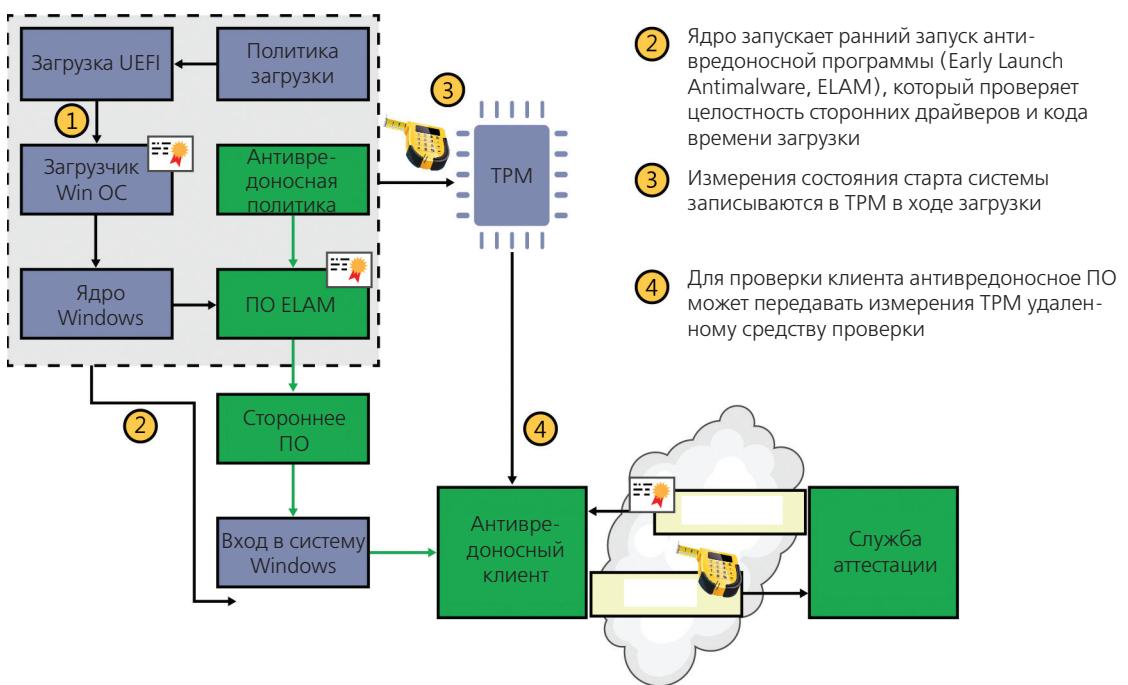


Рис. 5-1. Средства безопасности в Windows 10, задействованные на современном оборудовании, помогают предотвратить изменение процесса загрузки вредоносным ПО

Ниже приводится описание четырех пронумерованных элементов, показанных на рис. 5-1.

- **Безопасная загрузка (Secure Boot).** Самая базовая защита – это функция Secure Boot, которая является стандартной частью архитектуры UEFI. (Она определена в главе 27 спецификации UEFI 2.3.1.) На ПК с традиционным BIOS любой, имеющий контроль над процессом загрузки, может загрузиться с помощью альтернативного загрузчика ОС, потенциально получая доступ к системным ресурсам. Когда включена функция Secure Boot, то загрузиться можно только посредством загрузчика ОС, который подписан с использованием сертификата, сохраненного в прошивке UEFI. Естественно, в этом же хранилище находится сертификат Microsoft для цифровой подписи загрузчиков ОС Windows 8.1 и Windows 10, и прошивка UEFI проверяет его как часть своей политики безопасности. Эта функция должна быть включена по умолчанию на всех устройствах, сертифицированных для Windows 8.1 или Windows 10 по программе Windows Hardware Certification Program.
- **Ранний запуск антивредоносной программы (Early Launch Antimalware, ELAM).** Антивредоносное ПО, совместимое с расширенными возможностями безопасности в Windows 8 и более поздними версиями, может быть сертифицировано и подписано компанией Microsoft. Защитник Windows (Windows Defender) – антивредоносное ПО, которое включено в Windows 10 – поддерживает эту возможность; его можно заменить сторонним решением, если оно предпочтительнее для вашей организации. Эти подписанные драйверы загружаются

перед всеми остальными сторонними драйверами или приложениями, позволяя антивредоносному ПО обнаруживать любой неподписанный или недоверенный код и блокировать любые попытки изменить ход загрузки.

- **Надежная загрузка (Trusted boot).** Эта функция проверяет компоненты загрузки Windows на целостность и доверяемость. Перед загрузкой ядра загрузчик проверяет его цифровую подпись. Ядро, в свою очередь, проверяет все остальные компоненты процесса загрузки Windows, включая загрузочные драйверы, загрузочные файлы и компонент ELAM.
- **Измеряемая загрузка (Measured boot).** Эта функция, требующая наличия TPM на устройстве с Windows 8.1 или Windows 10, по ходу загрузки измеряет прошивку UEFI и каждого компонента Windows и антивредоносного ПО. Когда эти показатели собраны, их значения подписываются цифровой подписью и безопасно сохраняются в TPM. Они не могут быть изменены, пока система не будет сброшена. В ходе каждой последующей загрузки те же компоненты измеряются, и текущие значения сравниваются со значениями в TPM.

Для обеспечения дополнительной безопасности значения, записанные в ходе измеряемой загрузки, могут быть подписаны и переданы на удаленный сервер, который затем выполняет сравнение. Этот процесс, который называется удаленной аттестацией (remote attestation), позволяет удостовериться, что клиент Windows защищен.

Для устройств с Windows 10 Microsoft представила новый публичный API, который позволяет ПО, управляющему мобильными устройствами, обращаться к удаленной службе аттестации Windows Provable PC Health (PPCH). PPCH может управлять доступом устройств к сетям и службам, основываясь на подтверждении их надежности. На рис. 5-2 показано, как PPCH работает с облачной службой управления Microsoft Intune.



Рис. 5-2. PPCH проверяет удаленные устройства на признаки злонамеренного вмешательства и соответствие политикам и управляет доступом к сетям и службам на основе полученных результатов

Блокировка корпоративных ПК с помощью Device Guard

Device Guard – это новая функция, которая позволяет IT-профессионалам ограничивать возможности устройства так сильно, что оно не сможет выполнять недоверенное ПО, по сути, нейтрализуя любого атакующего или эксплойт, который работает, убеждая пользователей выполнить злонамеренную программу. В такой конфигурации, единственными программами, которым разрешено выполнение, – это доверенные программы, и даже программы, которые обходят другие уровни безопасности, эксплуатируя уязвимость нулевого дня, нейтрализуются.

Даже если атакующему удастся взять под контроль ядро Windows, благодаря ключевой архитектурной возможности Device Guard ему не удастся выполнить злонамеренный или неизвестный код. Решение о том, доверять приложению или нет, выполняется с обращением к службам Windows Code Integrity, которые работают в режиме Virtual Secure Mode – защищенном гипервизором Hyper-V контейнере. Эта служба принимает решение о доверии на основе подписей, которые защищены прошивкой UEFI и функциями защиты от несанкционированного вмешательства.

Чтобы развернуть Device Guard, аппаратное и программное обеспечение должно отвечать следующим требованиям.

- Устройство должно работать под управлением Windows 10 Enterprise.
- Прошивка UEFI должна быть версии 2.3.1 или выше, функция Secure Boot должна быть включена. Для дополнительной защиты от физических атак Microsoft рекомендует защищать вход в прошивку, чтобы не допустить изменения настроек UEFI и блокировать загрузку других операционных систем.
- Возможности безопасности на базе виртуализации требуют Hyper-V, который работает только на 64-разрядных ПК, поддерживающих расширения виртуализации Intel VT-x или AMD-V и Second Level Address Translation.
- Модуль управления памятью ввода/вывода VT-d или AMD-Vi для дополнительной защиты от атак памяти.
- Trusted Platform Module необязателен, но настоятельно рекомендуется.

Помимо Hyper-V, вам также понадобится включить функцию Режим изолированного пользователя (Isolated User Mode), как показано на рис. 5-3.

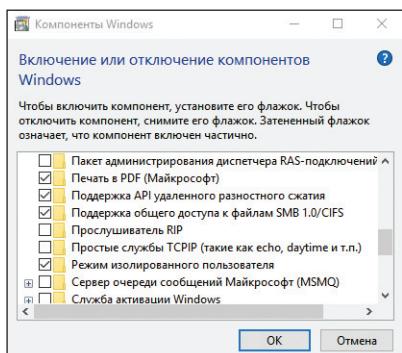


Рис. 5-3. Включение функции Режим изолированного пользователя (Isolated User Mode) необходимо для настройки режима Device Guard

Эти функции можно сконфигурировать вручную через командлеты Windows PowerShell или Deployment Image Servicing and Management.

При настройке Device Guard в качестве доверенных можно указать и Universal Windows Platform (UWP), и классические настольные программы Windows. Эта связь доверия требует, чтобы приложение или классические программы были подписаны с использованием цифрового сертификата, который организация определяет как заслуживающий доверия. Для UWP-приложений процесс публикации Windows Store использует совместимые подписи, которые могут проверяться центром сертификации Microsoft или центром сертификации вашей организации. Независимые поставщики ПО могут подписывать настольные приложений Windows с помощью сертификатов, инфраструктуры открытых ключей или стороннего заверителя ключей, который затем добавляется в список доверенных заверителей.

Microsoft анонсировала защищенную веб-службу, которую разработчики ПО и организации смогут использовать для подписи классических Windows-приложений.

Заключительный шаг в Device Guard – создание политики целостности кода (Code Integrity), которая состоит из двоично-закодированного XML-документа с настройками конфигурации для обоих режимов User и Kernel в Windows 10 Enterprise и серверами сценариев Windows 10. Эта политика ограничивает коды, выполняющиеся на устройстве.

После включения этих конфигураций и политик можно приступать к развертыванию Device Guard. За подробным руководством по развертыванию обратитесь к документу <http://bit.ly/DG-deploy>.

Защита данных на локальных запоминающих устройствах

Безумные гениальные киберпреступники существуют по большей части в фильмах и бульварных романах. В реальности намного более вероятно, что ваши данные может украдь обычный старомодный вор, не обладающий никакими техническими навыками. Чем больше мы полагаемся на мобильные устройства, тем выше риск.

Если сотрудник разгуливает с ноутбуком или планшетом с конфиденциальной корпоративной информацией, вы будете лучше спать, если данные на этом устройстве зашифрованы и защищены стойким паролем. Вы бы спали еще лучше, если бы смогли очистить конфиденциальные данные удаленно из панели администрирования.

В определенных областях наличие всеобъемлющего и эффективного плана защиты данных – не просто хорошая идея, а требование закона, согласно которому халатность карается уголовной ответственностью.

Windows 10 включает надежные варианты шифрования данных для всех устройств. Шифрование устройства теперь является стандартной возможностью во всех редакциях Windows (если оборудование поддерживает его). В предыдущих версиях эта функция традиционно резервиро-

валась для бизнес/корпоративных редакций. Шифрование включено по умолчанию на устройствах с Windows 10 Home, которые включают TPM. Редакции Pro и Enterprise могут настраиваться с дополнительной защитой BitLocker и возможностью управления.

Шифрование устройства

На любом устройстве, которое поддерживает стандарт InstantGo (ранее известный как Connected Standby) и работает под управлением Windows 8.1 или Windows 10, данные шифруются по умолчанию. На таком устройстве, даже если оно предназначено для обычных пользователей, в ходе установки шифрование автоматически включается для тома с операционной системой.

Это шифрование изначально использует чистый ключ, предоставляя доступ к тому, пока локальный администратор не войдет в систему с помощью учетной записи Microsoft (шифрование будет включено автоматически). Ключ восстановления для неуправляемой системы автоматически сохраняется в хранилище OneDrive на случай, если администратору позднее понадобится восстановить зашифрованные данные (в случае аппаратного сбоя или полной переустановки Windows 10). Если понадобится переустановить операционную систему или подключить диск на новом ПК, можно разблокировать диск с помощью ключа восстановления (который сохраняется на <http://onedrive.com/recoverykey>) и защитить диск с помощью ключа из новой машины.

Шифрование диска BitLocker

С технической точки зрения шифрование диска и BitLocker идентичны. Оба, и шифрование диска, и BitLocker, по умолчанию используют стандарт шифрования Advanced Encryption Standard (AES) с длиной ключа 128 бит, но BitLocker может быть настроен на использование AES-256.

Самыми важными преимуществами для BitLocker в корпоративных сценариях являются контроль и управляемость. BitLocker предлагает длинный список возможностей, которые подходят для защиты данных корпоративного класса, включая возможность хранить ключи шифрования, используя Active Directory для восстановления данных (например, если утерян пароль, или сотрудник увольняется и руководству нужно получить доступ к зашифрованным файлам на устройстве компании). Функция Network Unlock позволяет управлять устройствами с BitLocker в среде домена, обеспечивая автоматическую разблокировку томов с операционной системой при загрузке системы, когда она подключается к доверенной проводной корпоративной сети.

Обычно BitLocker использует программное шифрование для защиты содержимого томов с операционной системой Windows и с данными. На устройствах без поддержки аппаратного шифрования BitLocker в Windows 10 шифрует данные гораздо быстрее, чем в Windows 7 и более ранних версиях. BitLocker в Windows 10 позволяет шифровать только используемое пространство на диске, а не весь диск. В такой конфигурации свободного пространства шифруется, когда оно используется в первый раз. В результате процесс шифрования выполняется гораздо быстрее, чтобы организации могли предоставлять защиту BitLocker, не затрачивая лишнее время.

При включенном шифровании BitLocker администратор может указать в настройках групповой политики, шифровать ли только используемое дисковое пространство или весь диск. Путь к настройкам групповой политики: Конфигурация компьютера > Административные шаблоны >

Компоненты Windows > Этот параметр политики позволяет выбрать шифрование диска BitLocker (Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption) в редакторе локальной групповой политики:

- Несъемные диски с данными > Применить тип шифрования диска к несъемным дискам с данными (Fixed Data Drives > Enforce drive encryption type on fixed data drives).
- Диски операционной системы > Применить тип шифрования диска к дискам операционной системы (Operating System Drives > Enforce drive encryption type on operating system drives).
- Съемные носители с данными > Применить тип шифрования диска к съемным носителям с данными (Removable Data Drive > Enforce drive encryption type on removable data drives).

Для каждой из этих политик можно также затребовать конкретный тип шифрования для каждого типа диска.

В Windows 8 и более поздних версиях BitLocker поддерживает новый тип накопителей, Зашифрованный жесткий диск (Encrypted Hard Drive), который включает контроллер, использующий аппаратное шифрование. Зашифрованные жесткие диски предлагают Полное шифрование диска (Full Disk Encryption, FDE), т. е. шифруется каждый блок физического диска, а не данные на томах.

Windows 10 может определить зашифрованный диск, ее средства управления дисками могут активировать, создавать и сопоставлять тома при необходимости. Поддержка API в Windows 8.1 и более поздних версиях позволяют приложениям управлять зашифрованными жесткими дисками отдельно от шифрования диска BitLocker. Панель управления BitLocker позволяет пользователям управлять зашифрованными жесткими дисками с помощью средств работы со стандартными жесткими дисками.

Удаленное удаление бизнес-данных

В Windows 8.1 и более поздних версиях администраторы могут помечать и шифровать корпоративные данные, чтобы отличать их от обычных пользовательских данных. Когда отношения между организацией и пользователем заканчиваются, зашифрованные корпоративные данные могут быть удалены по команде с помощью Exchange ActiveSync (с протоколом OMA-DM или без него). Эта функция требует поддержки в клиентском приложении (например, Почта) и в серверном приложении (Exchange Server). Клиентское приложение определяет, сделать ли данные недоступными или полностью удалить их. Эта функция включает поддержку API, который позволяет сторонним приложениям использовать функцию удаленной очистки.

Защита учетных данных

Неэффективность паролей для защиты устройств и данных давно известна. Их так легко украдь: на клиенте – с помощью кейлоггера или фишинговой схемы, на сервере – путем утечек данных, которые дают злоумышленнику доступ к большим наборам имен и паролей пользователей. Поскольку люди часто используют одни и те же пароли для доступа к разным местам, брешь в одном

месте может привести злоумышленника и в другие места, в которых используются те же учетные данные.

Атакующий также может украсть маркер входа пользователя со скомпрометированной машины и использовать этот маркер для кражи дополнительных маркеров. У атакующего нет имени пользователя или пароля, но для доступа достаточно иметь хэшированные учетные данные. Эта методика называется «атакой с передачей хэша» (pass the hash).

В Windows 10 имеются серьезные изменения архитектуры, призванные фундаментально предотвращать обе формы атак.

Начиная с Windows 10, производные учетные данные (хэши), которые используются в атаках с передачей хэшей, перемещены в виртуальный защищенный режим (virtual secure mode) – тот же защищенный Hyper-V контейнер, который используется для служб Windows Code Integrity.

Windows 10 переносит защиту учетных данных на новый уровень, реализуя новые службы, которые называются Microsoft Passport. Эта возможность заменяет пароли стойкой двухфакторной аутентификацией, которая использует в качестве одного фактора зарегистрированное устройство, а в качестве второго фактора – биометрическую информацию (Windows Hello) или ПИН-код. Соответствующие службы доступны на всех редакциях Windows 10, как видно из рис. 5-4, и включаются при необходимости.

Службы (локальные)		
Имя	Описание	
Сервер моделей данных плиток	Сервер плиток для обновления плиток.	
Сетевая служба Xbox Live	Данная служба поддерживает программный интерфейс	
Сетевой вход в систему	Обеспечивает безопасный канал связи между этим компь	
Сетевые подключения	Управляет объектами папки "Сеть и удаленный доступ к с	
Система событий COM+	Поддержка службы уведомления о системных событиях (
Системное приложение COM+	Управление настройкой и отслеживанием компонентов С	
Служба Microsoft Passport	Обеспечивает изоляцию процесса для ключей шифрован	
Служба push-уведомлений Wi-Fi	Эта служба используется для отправки push-уведомлений	
Служба SSTP	Обеспечивает поддержку протокола SSTP (Secure Socket T	
Служба Windows License Manager	Обеспечивает поддержку инфраструктуры для Магазина	
Служба Windows Mobile Hotspot	Позволяет использовать соединение для передачи данны	
Служба автоматического обнаружения	WinHTTP реализует стек клиента HTTP и обеспечивает ра	
Служба автономного WLAN	Служба WLAN SVC предоставляет логику, необходимую д	
Служба базовой фильтрации	Служба базовой фильтрации (BFE) представляет собой сл	
Служба беспроводной связи Bluetooth	Включает беспроводные гарнитуры Bluetooth для работы	
Служба бумажника	Содержит объекты, используемые клиентами бумажника	
Служба виртуализации удаленных рабочих столов	Служба предоставляет платформу для обмена данны	
Служба времени Windows	Управляет синхронизацией даты и времени на всех клиен	
Служба географического положения	Эта служба отслеживает местоположение системы и управ	
Служба данных датчиков	Получение данных различных датчиков	
Служба датчиков	Служба сенсоров управляет различными функциями сен	

Рис. 5-4. Эти службы устраняют необходимость постоянного ввода паролей на совместимых устройствах. (В русской локализации службы разнесены; вторая служба – Контейнер службы Microsoft Passport – прим. перев.)

Мультифакторная защита, доступная для многих устройств и служб, ограничена такими решениями, как смарт-карты и приложения проверки подлинности на устройствах. Windows 10 встраивает мультифакторную аутентификацию в операционную систему и само устройство, устранив необходимость в дополнительной периферии обеспечения защиты.

Ключевым шагом в Windows 10 является регистрация устройства с помощью учетной записи Microsoft, учетной записи Active Directory, учетной записи Microsoft Azure Active Directory или не-Microsoft службы, которая поддерживает аутентификацию Fast Identity Online (FIDO). (Стандарт FIDO поддерживается множеством банков и существующими провайдерами услуг аутентификации, например RSA.) Будучи зарегистрированным, устройство само становится одним из факторов, необходимых для аутентификации. Второй фактор – это ПИН-код (вариант по умолчанию)

или биометрическая аутентификация (на системах с соответствующей аппаратной поддержкой), например, распознавание отпечатка пальцев, распознавание лица или сканирование радужной оболочки глаза.

Существующие сканеры отпечатков пальцев работают с новыми мерами аутентификации. Для распознавания лица используется новое оборудование, включающее инфракрасный диапазон. Например, Microsoft Surface Pro 4 включает встроенную камеру, совместимую с Windows Hello; в качестве опции доступен также Type Cover, который включает встроенный сканер отпечатка пальца. После начальной установки можно сконфигурировать Surface Pro 4 на автоматическую разблокировку после распознавания лица зарегистрированного пользователя, как показано на рис. 5-5.

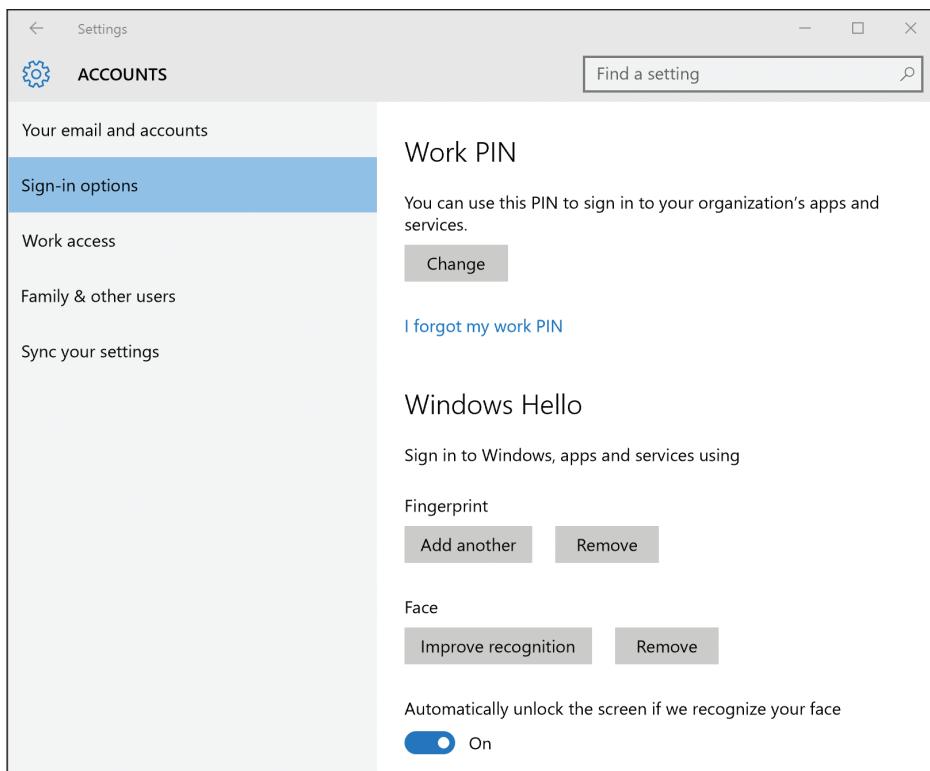


Рис. 5-5. Биометрическая аутентификация встроена в Windows 10. На этом Surface Pro 4 настроены обе функции – сканер отпечатка пальца и распознавание лица, при этом на автоматическую разблокировку устройства настроена фронтальная камера

Windows 10 поддерживает существующие сканеры отпечатков пальцев для аутентификации. В Windows 8.1 был представлен полный процесс регистрации отпечатков пальцев для аутентификации. Эта функциональность доступна и в Windows 10. После настройки биометрических средств доказательства личности эти методы доступны для входа в систему и для любых других действий, требующих аутентификацию, как показано на рис. 5-6.

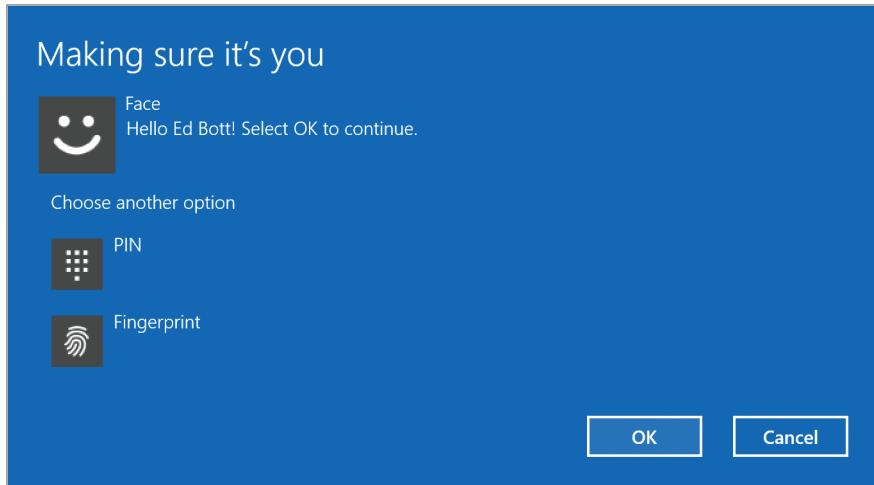


Рис. 5-6. Биометрическая аутентификация заменяет ввод пароля отпечатком пальца или распознаванием лица на зарегистрированном устройстве

Вывод? Атакующим, которые украли кэш имен и паролей пользователей, не повезло. Им потребуется физическое устройство пользователя и возможность передать его учетные данные, и второй шаг требует доступа к ПИН-коду пользователя или биометрической информации.

Эта возможность требует, чтобы устройство было оборудовано TPM; при регистрации устройства создается сертификат, который безопасно сохраняется в TPM и позволяет устройству доказывать свою подлинность удаленному серверу. Атакующий, который знает ваше имя и пароль, не сможет выдать себя за вас и получить доступ к этому ресурсу, поскольку у него нет второй необходимой части ИД – зарегистрированного устройства. Процесс регистрации не требует подключения устройства к домену, что делает эту возможность особенно полезной для сценариев «принеси свое собственное устройство» (Bring Your Own Device, BYOD).

Учетные данные сами по себе могут быть криптографически сгенерированной парой ключей (закрытый и открытый ключи). Ключи может генерировать сама Windows; это также может быть сертификат, выданный устройству существующей инфраструктурой открытых ключей.

В домене можно настроить групповую политику для служб Microsoft Passport. Настройки политики находятся в разделе Конфигурация компьютера > Политики > Административные шаблоны > Компоненты Windows > Microsoft Passport для работы (Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Passport for Work). Доступные настройки позволяют включать или отключать Passport для работы с паролями домена, чтобы разрешить или запретить аппаратные устройства защиты и биометрическую аутентификацию, а также для задания требований к сложности ПИН-кода.

Включить Passport для работы можно также с помощью ПО управления мобильными устройствами (mobile device management, MDM). Эти настройки политики MDM используют поставщика услуг конфигурации PassportForWork (configuration service provider, CSP); описание службы доступно по адресу: <http://bit.ly/PassportForWorkCSP>.

Пользователи могут регистрировать несколько устройств с новыми учетными данными. Microsoft Passport также позволяет использовать устройства с Windows 10 Mobile в качестве удаленных учетных данных при входе в ПК с Windows 10.

Для доступа к Microsoft Passport при входе пользователя персональный компьютер с Windows 10 может подключиться с помощью Bluetooth к устройству с Windows 10 Mobile пользователя. Комбинация зарегистрированного устройства и PIN-кода или биометрической аутентификации позволяет выполнять вход на все ПК, сети и веб-службы, локально или удаленно. Ни одно из этих устройств, сетей или служб не требует сохранения или передачи пароля. Это делает невозможным кражу злоумышленником учетных данных с использованием фишинговых схем, кейлоггеров и других типов атак.

Блокировка вредоносного ПО

Успешное противостояние вредоносному ПО и фишинговым атакам начинается с нескольких фундаментальных возможностей обеспечения безопасности, которые защищали ядро операционной системы в течение нескольких лет. Первые две возможности призваны защищать от эксплоитов, которые используют уязвимости, такие как переполнения буфера в операционной системе и приложениях.

- **Address Space Layout Randomization (ASLR).** Эта функция произвольным образом распределяет важные данные в памяти, делая практически невозможной атаку напрямую в системную память, поскольку вредоносное ПО не может найти конкретное расположение, которое нужно атаковать. Windows 8.1 и Windows 10 значительно увеличивают уровень энтропии по сравнению с Windows 7, еще больше уменьшая шансы большинства эксплоитов. Кроме того, ASLR уникальна для каждого устройства, что затрудняет эксплуату, который работает на одном устройстве, работу на другом.
- **Предотвращение выполнения данных (Data Execution Prevention, DEP).** Эта функция значительно уменьшает диапазон памяти, в которой может выполняться код, включая вредоносный. Начиная с Windows 8, поддержка аппаратного DEP является обязательным; Windows 10 не установится на устройстве, которое не поддерживает эту функцию. На поддерживаемых ЦП DEP использует бит Never eXecute (NX) для пометки таких блоков памяти, которые могут хранить данные, но никогда не выполняют код. Даже если злоумышленнику удастся загрузить вредоносный код в память, он не сможет выполнить его.

Защитник Windows (Windows Defender)

В Windows 7 Защитник Windows (Windows Defender) – это антишпионское решение с очень ограниченными функционалом. Начиная с Windows 8 и продолжая в Windows 10, Защитник Windows (Windows Defender) – это полноценное решение обеспечения безопасности (и потомок Microsoft Security Essentials), ответственное за обнаружение всех видов вредоносного ПО. Поскольку он поддерживает функцию ELAM, описанную ранее в этой главе, он также блокирует руткиты, которые пытаются заразить сторонние загрузочные драйверы. В Windows 10 Защитник Windows также включает мониторинг поведения сети.

Защитник Windows (Windows Defender) не докучает пользователю, обновляется автоматически и отображает сообщения только тогда, когда это действительно нужно. Он предназначен главным образом для неуправляемых ПК. В организациях разумнее применять альтернативное антивирусное решение. Решение System Center Endpoint Protection от компании Microsoft, которое использует тот же движок, что и Защитник Windows (Windows Defender), а также включает поддержку ELAM, предназначено для работы со средствами управления организацией. Доступен также ряд сторонних решений, отвечающих таким же критериям.

SmartScreen и защита от фишинга

Windows 10 включает две отдельных, но связанных функции, которые делят одно название: SmartScreen. Основной принцип безопасности, стоящий за SmartScreen (который был впервые представлен в Windows 8), прост: гораздо эффективнее не дать вредоносному коду запуститься, чем потом вычищать систему от всех его следов.

Microsoft совершенствовала технологию SmartScreen многие годы. Данные берутся из различных источников, включая Microsoft Edge и Internet Explorer, Bing, Защитника Windows (Windows Defender) и Enhanced Mitigation Experience Toolkit (EMET). Эта информация наполняет онлайн-службу, которая эффективно блокирует многие мимолетные атаки в браузере. Когда пользователи, например, посещают веб-страницу, которую SmartScreen идентифицирует как скомпрометированную, содержимое страницы блокируется и показывается сообщение, похожее на то, что представлено на рис. 5-7.

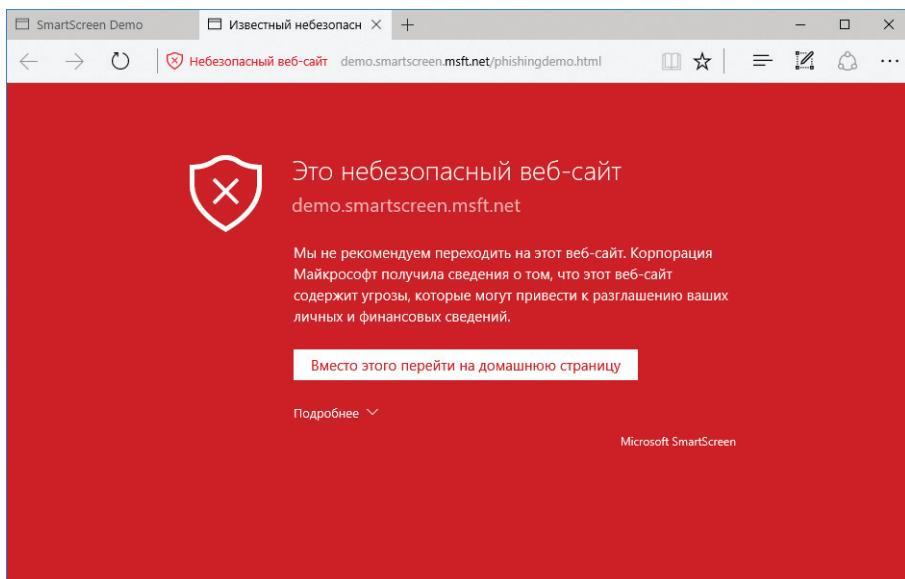


Рис. 5-7. Защита SmartScreen, встроенная в оба браузера – Internet Explorer и Microsoft Edge, блокирует демонстрационную страницу, которая имитирует сайт, скомпрометированный вредоносным ПО

(Для демонстрации работы функции SmartScreen, в браузере и за его пределами посетите страницу <http://demo.smartscreen.msft.net/>. Эти демонстрационные страницы не содержат вредоносного кода и полезны для обучения пользователей тому, как распознавать и отвечать на эти важные предупреждения.)

Вне браузера SmartScreen проверяет при запуске любой исполняемый файл. Если файл помечен как полученный из онлайн-источника, веб-служба проверяет хэш файла в базе репутации приложений. Файлы с положительной репутацией предполагаются безопасными, и им разрешается запуск. Файлы с отрицательной репутацией считаются вредоносными, и их запуск блокируется.

Технология Windows SmartScreen особенно эффективна для предотвращения выполнения файлов неизвестного происхождения необученными пользователями. Когда SmartScreen обнаруживает файл, у которого еще нет репутации, он блокирует его выполнение и отображает предупреждение, похожее на то, что представлено на рис. 5-8.

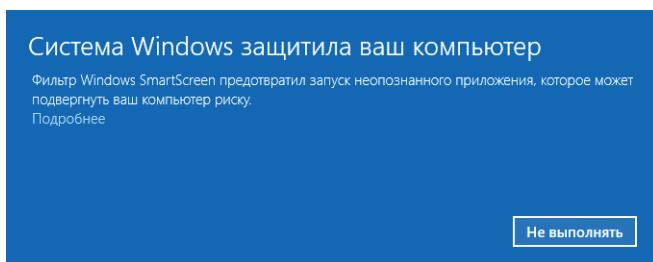


Рис. 5-8. Защита SmartScreen работает даже со сторонними браузерами. Это предупреждение отображается, когда пользователь загрузил и пытается запустить исполняемую программу, которая была помечена как подозрительная

Локальные администраторы могут переопределить блокировку SmartScreen вручную. Отключить технологию SmartScreen или изменить ее поведение (например, запретить пользователям переопределять действия SmartScreen) можно через групповую политику.

Управление конфиденциальностью

За последние три десятилетия связь Windows с онлайновыми источниками информации становилась только теснее. Этот информационный поток работает в обоих направлениях, приложения Windows могут отправлять и получать файлы, сообщения электронной почты и другие данные с помощью подключений к облачным службам. Windows сама регулярно собирает диагностическую информацию как ключевой элемент модели «Windows как сервис».

Обычные пользователи Windows и малый бизнес могут управлять этим информационным потоком с помощью опций в разделе Конфиденциальность (Privacy) приложения Параметры (Settings), как показано на рис. 5-9. Администраторы домена могут использовать групповую политику для дополнительного контроля над настройками конфиденциальности.

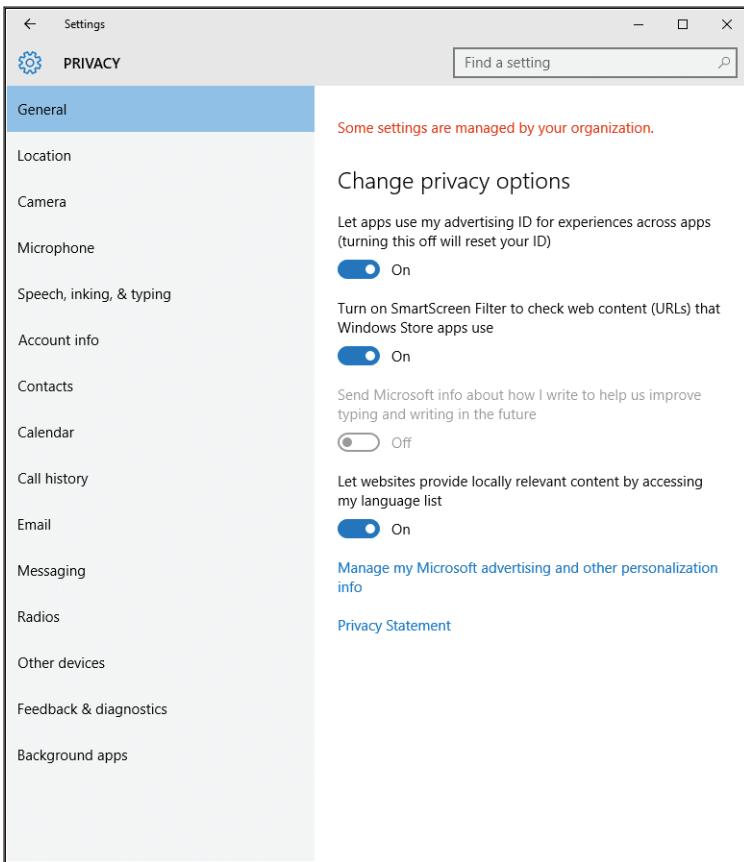


Рис. 5-9. Параметры конфиденциальности организованы в группы, доступ к которым осуществляется через приложение Параметры (Settings). Администраторы могут управлять настройками конфиденциальности через групповую политику или ПО управления мобильными устройствами

Каждая категория внизу содержит ссылку на универсальное соглашение о конфиденциальности Microsoft, которое относится к Windows и большинству служб Microsoft. (Office 365, Azure и другие коммерческие службы используют отдельные соглашения.) Некоторые параметры конфиденциальности также содержат ссылку на страницу FAQ с описанием типа собираемых данных и того, как они хранятся и используются.

Большинство категорий не требуют дополнительных пояснений и содержат как общие, так и специфичные для приложений опции. Например, раздел Камера (Camera), представленный на рис. 5-10, предлагает глобальную опцию Разрешить приложениям использовать камеру (Let Apps Use My Camera) и ползунки для разрешения использовать камеру отдельным приложениям.

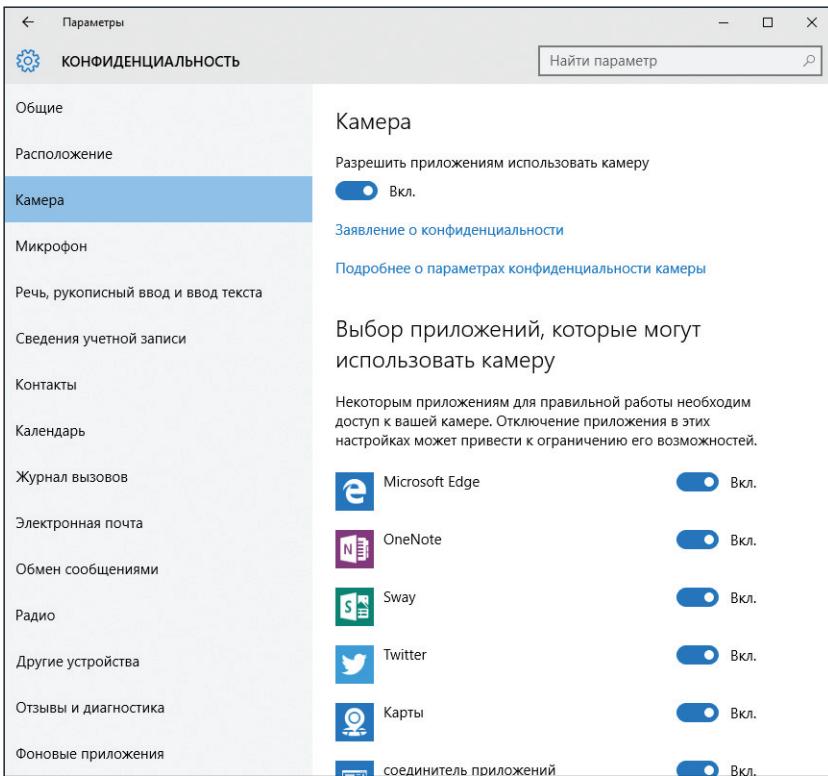


Рис. 5-10. Многие параметры конфиденциальности предлагают как глобальные, так и специфичные для приложений элементы управления. Используя панель Камера (Camera), например, можно отключить доступ к камере для всех приложений или задавать доступ для каждого приложения отдельно

Исторически корпоративные администраторы уделяли особое внимание настройкам отправки сообщений об ошибках и другой диагностической информации. Детальные лампы сбоя иногда включают содержимое памяти на момент сбоя, что помогает инженеру найти причину сбоя, но они также могут содержать части документов с конфиденциальной информацией.

Раздел Отзывы и диагностика (Feedback & Diagnostics) категории Конфиденциальность (Privacy), представленный на рис. 5-11, предлагает три настройки под заголовком Данные диагностики и использования (Diagnostic And Usage Data).

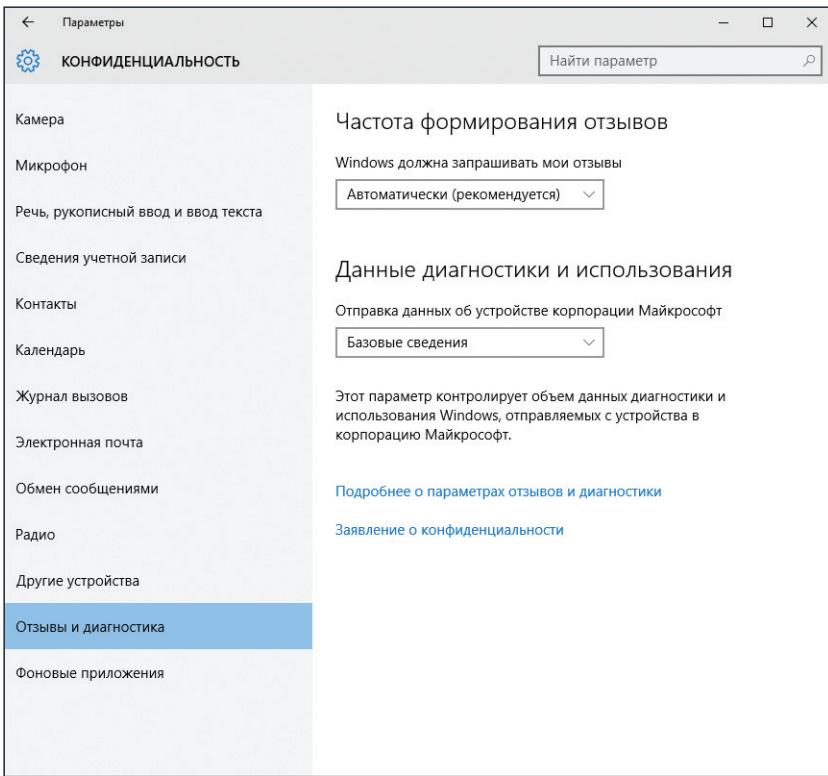


Рис. 5-11. Раздел Отзывы и диагностика (Feedback & Diagnostics) параметров конфиденциальности позволяет управлять объемом диагностических данных, которые отправляются в корпорацию Microsoft. Редакции Windows Enterprise и Education предлагают еще одну дополнительную опцию

Компания Microsoft проделала огромную работу по анонимизации информации, которая передается как часть этой программы (иногда внутри компании ее называют телеметрией), убирая персональные данные и используя уникальный идентификатор устройства, который позволяет аналитикам понять, относятся ли повторяющиеся случаи конкретной проблемы к нескольким устройствам или же это несколько сбоев на одном устройстве.

По умолчанию этот параметр установлен в значение Полные сведения (Full), что позволяет инженерам Microsoft видеть полные сведения о том, как используются функции Windows и приложения, а также передавать дополнительные данные по ошибкам, которые могут включать содержимое пользователя. Этую настройку нельзя изменить для устройств, которые были зарегистрированы в программе Windows Insider.

Если изменить этот параметр на Базовые сведения (Basic), то в Microsoft будет отправляться минимум диагностической информации: характеристики устройства, что установлено и корректно ли работает Windows. Эта опция также включает базовые сообщения об ошибках.

IT-профессионалы имеют одну дополнительную опцию, позволяющую указать, где и как данные телеметрии собираются и отправляются в Microsoft. Детали этой политики находятся по адресу: <http://go.microsoft.com/fwlink/?LinkId=627097>.

Этот четвертый уровень, который называется Безопасность (Security), доступен в редакциях Windows 10 Enterprise, Windows 10 Education, Windows 10 Mobile Enterprise и IoT Core. Установка уровня телеметрии в значение Безопасность (Security) выполняется через групповую политику или политику управления мобильным устройством или же вручную путем внесения изменения в реестр. Следует отметить, что включение этого параметра отключает Windows Update, поэтому его следует применять только в организациях, в которых для управления обновлениями используются службы Windows Server Update Services, System Center Configuration Manager или альтернативные.

ГЛАВА 6

Microsoft Edge и Internet Explorer 11

В прошлые два десятилетия веб все больше проникал в нашу повседневную жизнь. Сегодня приложения, подключенные напрямую к облачным службам, при выполнении некоторых задач могут обходиться без веб, но каждый день мы снова и снова обращаемся к веб-браузерам для поиска информации или выполнения каких-либо задач.

На рабочих местах устаревшие приложения заменяются веб-службами, работа с которыми ведется в окне браузера. Бизнес-задачи, которые раньше размещались на локальном сервере, теперь выполняются из облака, а управление ими ведется – да-да-да» – из окна веб-браузера.

Очевидно, современная реальность делает функции веб-просмотра жизненно необходимыми для любого компьютерного устройства, будь то телефон, планшет, ноутбук или мощная настольная рабочая станция. Щелкая на ссылке, пользователь уверен, что целевая страница будет работать правильно.

Windows 10 включает два веб-браузера. Один, Microsoft Edge, – совершенно новый, он появился только в Windows 10. Другой, предназначенный для организаций, – это добрый старый Internet Explorer 11, к которому добавлен режим предприятия (Enterprise Mode) для облегчения перехода с более старых версий Internet Explorer.

В данной главе описываются причины появления двух браузеров и возможности каждого из них.

Краткая история Internet Explorer

На рубеже веков вебом «рулил» Internet Explorer. Затем, буквально за несколько лет, Microsoft убрала разработку Internet Explorer из первоочередных задач. Началась конкурентная гонка браузеров, и за последние десять лет появилось немало веб-браузеров и инструментов разработки, в том числе и весьма достойные. Для многих разработчиков, особенно тех, кто не работает на Windows платформах, Internet Explorer стал надоедливым пунктиком в списке совместимости, а не платформой для разработки.

В последние годы Microsoft приложила немало усилий, чтобы догнать конкурентов, обеспечив высокую производительность и соответствие стандартам и вернув разработчиков. Internet Explorer 11, доступный для Windows 7, Windows 8.1 и Windows 11, – это отличный конкуренто-способный продукт, быстрый и вполне соответствующий веб-стандартам.

Проблема в том, что большинство корпоративных развертываний Windows не пользуются преимуществами последней версии Internet Explorer, а работают со старой медленной версией, не отвечающей современным веб-стандартам. Чаще всего это вызвано проблемами совместимости со старыми веб-приложениями, которые работают только под Internet Explorer 8.

Проблема усугубляется чрезвычайно быстрым циклом разработки конкурирующих браузеров, таких как Google Chrome и Mozilla Firefox. В последние годы их обновления выпускаются гораздо чаще, чем обновления Internet Explorer.

Быстрый цикл обновлений означает, что пользователь, работающий с Chrome или Firefox, быстрее получит возможности из самых последних веб-стандартов. Чрезвычайно долгий цикл поддержки Microsoft позволил эксплуатировать старые версии Internet Explorer гораздо дольше, чем это имеет смысл в быстро меняющемся современном вебе.

Ситуация радикально изменилась 12 января 2016, когда Microsoft изменила жизненный цикл поддержки для Internet Explorer. Согласно новой политике, только самая последняя версия Internet Explorer, доступная для поддерживаемой операционной системы, будет получать техническую поддержку и обновления безопасности.

Впервые на ПК с Windows 7, Windows 8.1 и Windows 10 официально поддерживается только одна версия Internet Explorer – Internet Explorer 11. Для решения проблемы совместимости в организациях в Internet Explorer 11 имеется новая возможность – Режим предприятия (Enterprise Mode). Она будет обсуждаться далее в этой главе.

Но для новых ПК с Windows 10 веб-браузером по умолчанию является не Internet Explorer, а новый браузер Microsoft Edge. Организации могут сделать Internet Explorer стандартным браузером на всех поддерживаемых версиях Windows, но по большому счету Internet Explorer теперь предназначен для обеспечения совместимости.

Далее мы сравним два браузера в Windows 10.

Браузеры в Windows 10

Стратегия с двумя браузерами не нова. Windows 8 и Windows 8.1 также включали два браузера, один – с традиционным настольным интерфейсом Windows а другой – с современным адаптированным для сенсорного экрана дизайном, предназначенный для полноэкранной работы на планшетах. Несмотря на разный дизайн, оба браузера имеют большой объем общего кода, включая движок Trident, который с самых первых версий был ядром Internet Explorer.

Windows 10 также включает два браузера, каждый со своим дизайном и своими методами взаимодействия с пользователем. Но, что важнее, Windows 10 включает два разных движка.

- **EdgeHTML (Edgehtml.dll)** – это новый HTML-просмотрщик, который начался с движка Trident, но теперь значительно отличается от него. В новом движке убраны большие куски устаревшего кода, эмулирующего более старые версии Internet Explorer, включая режимы документов, которые определяют, как предыдущие версии Internet Explorer отображают страницу.

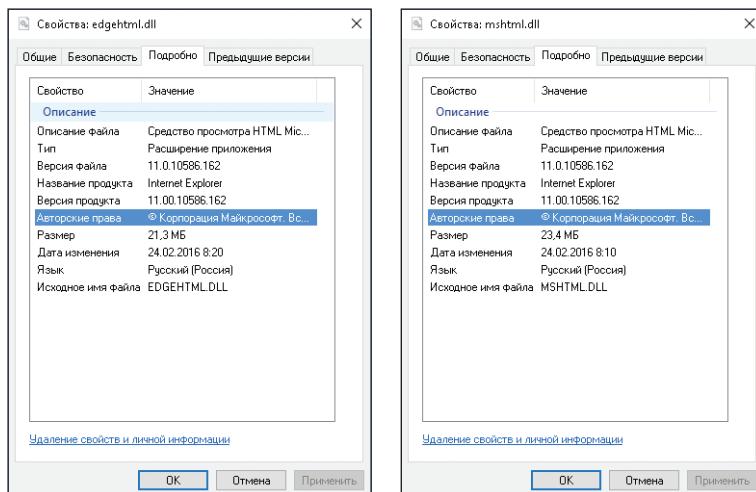
Совместимость со стандартами – важная цель EdgeHTML, но функциональная совместимость еще важнее: разработчики приложили максимум усилий, чтобы EdgeHTML не вызывал проблем с несовместимостью браузеров у разработчиков.

- **Trident (Mshtml.dll)** – движок, который два десятилетия был частью Internet Explorer. Он остается стабильной согласованной веб-платформой для работы в Internet Explorer 11. Trident получает и будет получать обновления безопасности и совместимости для всех поддерживаемых платформ Windows, включая Windows 10, однако в него не будут добавляться новые возможности или поддержка дополнительных веб-стандартов; они будут делаться исключительно для нового движка и Microsoft Edge.



Примечание. Подробный список состояния поддержки веб-стандартов для обоих движков находится по адресу: <https://status.modern.ie>. Стандарты, которые реализованы только в EdgeHTML, в настоящее время обозначены как Preview Release. Кроме нескольких исключений, стандарты с указанием Under Consideration или In Development (например, Touch Events) будут доступны только в EdgeHTML.

Чтобы графически проиллюстрировать общую кодовую базу обоих браузеров, проверьте свойства каждого файла (находятся в C:\Windows\System32). Обратите внимание на совпадение Версии файла (Product Version), как показано на следующем рисунке.



Несмотря на высокую скорость разработки Windows 10, Microsoft Edge разрабатывается еще быстрее. Он является относительно поздним добавлением в Windows 10 Technical Preview и известен публике как Проект Спартанец (Project Spartan).

Первый официальный выпуск Microsoft Edge состоялся в июле 2015 совместно с выпуском Windows 10. В ноябре 2015 Microsoft выпустила главное обновление платформы для Microsoft Edge, версия браузера стала 25-й, а версия движка EdgeHTML – 13-й; этот выпуск также добавил главные усовершенствования в Chakra, движок JavaScript в браузере Microsoft Edge.

Информация о версии доступна в меню Параметры (Settings) в Microsoft Edge.

Те, кто хочет просмотреть возможности, которые все еще находятся в разработке и пока не включены в производственные выпуски, могут ввести в адресной строке `about:flags`. Будет отображен список дополнительных параметров и экспериментальных функций, как показано на рис. 6-1.

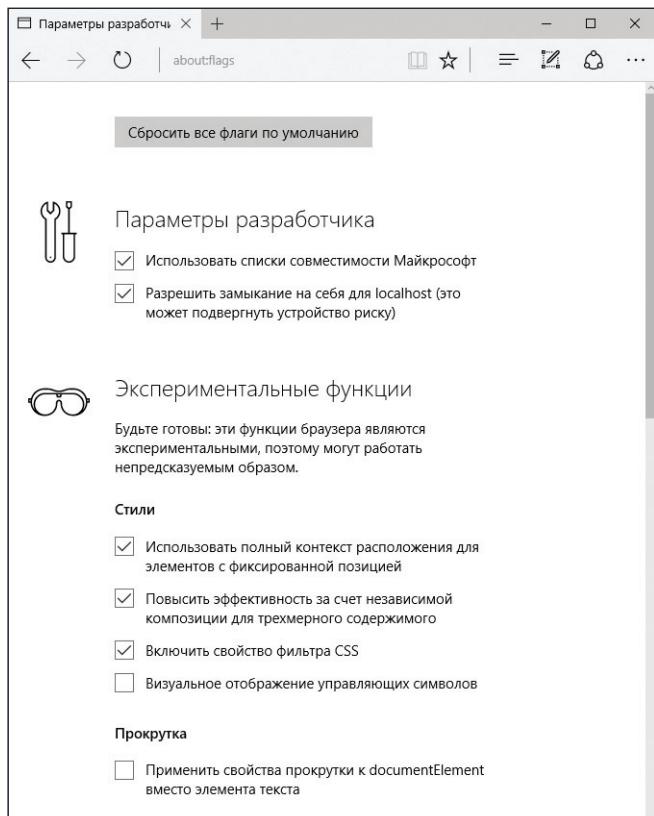


Рис. 6-1. Чтобы отобразить эти дополнительные параметры, введите `about:flags` в адресной строке Microsoft Edge

Одно из самых важных изменений Microsoft Edge – это строка агента пользователя (*user-agent string*), которая при некорректном отображении веб-страницы будет проверять ее кодировку под определенную версию браузера, а не ее особые возможности.

В Windows 10 версии 1511 Internet Explorer 11 обозначает себя с помощью следующей строки агента пользователя:

```
Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
```

А Microsoft Edge 25 возвращает эту строку агента пользователя с каждым запросом веб-страницы:

Это изменение в строке агента пользователя повышает вероятность того, что сайт обслужит ту же самую, совместимую со стандартами страницу, что и для других браузеров, и проигнорирует специфические возможности Internet Explorer.

Microsoft Edge

Как уже упоминалось ранее в этой главе, Microsoft Edge – это относительное недавнее нововведение в Windows 10, и он все еще быстро развивается. В текущем воплощении браузер имеет минималистский дизайн, представленный на рис. 6-2, который, скорее всего, и повлиял на кодовое имя Проект Спартанец.

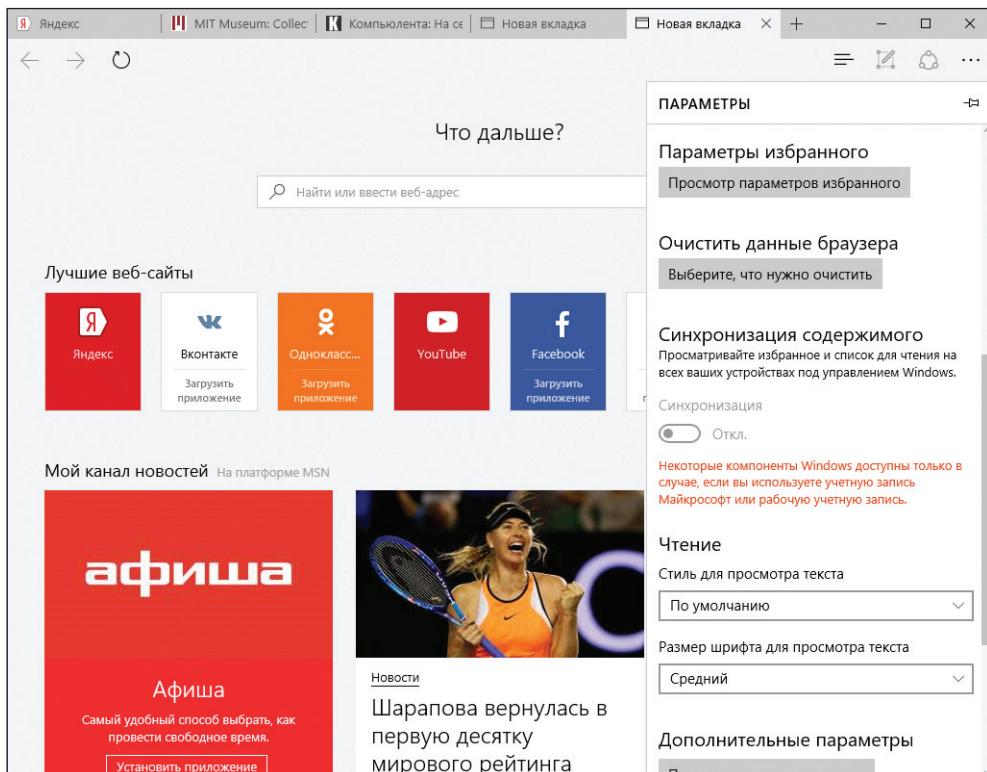


Рис. 6-2. Минималистский дизайн браузера Microsoft Edge включает возможность прикрепить панель к правому краю окна, здесь прикреплено меню Параметры (Settings)

В стандартном макете Microsoft Edge действительно «тощий». В нем нет строки заголовка, а есть только три кнопки и многоточие, которое открывает меню опций и параметров. На странице новой вкладки, представленной на рис. 6-2, даже не видна адресная строка, пока пользователь не загрузит страницу из поля поиска или не щелкнет на месте, где должна быть адресная строка.

Такая простота дизайна означает, что для настройки имеется гораздо меньше параметров, чем в Internet Explorer, а некоторые привычные возможности могут вообще отсутствовать.

Самая очевидная отсутствующая возможность в Microsoft Edge 25 – это поддержка любого вида расширений браузера. Internet Explorer 11 поддерживает Browser Helper Objects и панели инструментов, а также ряд других проприетарных расширений. По соображениям безопасности эти типы дополнений не разрешены в Microsoft Edge.

В Windows 10 версии 1511 единственным доступным дополнением для Microsoft Edge является Adobe Flash Player, который встроен в браузер (и автоматически обновляется) так же, как и в Internet Explorer 11. (Возможности Flash можно отключить в настройках, но само дополнение удалить нельзя.) Microsoft Edge также включает средства чтения PDF-документов, которые позволяют открывать PDF-документы с веб-сайтов, вложений электронной почты и локальной файловой системы, не требуя стороннего ПО.

Компания Microsoft планирует разрешить сторонним разработчикам писать дополнения для Microsoft Edge, используя HTML и JavaScript (такой же подход используется и в браузерах-конкурентах). Эта возможность сначала будет включена в предварительные выпуски и, скорее всего, попадет в Текущую ветвь в середине 2016 года для тех потребителей и малого бизнеса, которые принимают стандартное расписание обновлений. (Работа Текущей ветви рассматривалась в главе 1.)

Microsoft Edge включает ряд важных возможностей, которые входили еще в предварительные выпуски продукта. Одна из них – это Режим чтения (Reading View). Он должен быть знаком пользователям последней версии Internet Explorer в Windows 8 или Windows 8.1. При щелчке на кнопке Режим чтения (Reading View) в адресной строке убираются все объявления и лишние элементы, текст и графические элементы статьи переформатируются, облегчая чтение. Этот режим особенно полезен для маленьких экранов, например, планшетов с Windows 10, но может использоваться и на больших экранах, чтобы уменьшить напряжение глаз.

На рис. 6-3 представлена одна и та же страница в разных представлениях. Оригинальный макет находится слева, версия в Режиме чтения (Reading view) – справа.

Другим значимым аспектом Microsoft Edge является функция Веб-заметка (Web Note), которая позволяет добавить примечания на веб-страницу, а затем сохранить заметку или отправить другу или коллеге.

Инструменты управления заметками находятся на панели инструментов, которая скрыта, пока пользователь не активирует ее, щелкнув или прикоснувшись к кнопке Создать веб-заметку (Make A Web Note) на панели инструментов Microsoft Edge. На рис. 6-4 показана эта панель инструментов в действии, с выбором маркера или пера различных цветов и размеров, а также инструментами, позволяющими добавлять заметки и вырезать части экрана.

Abraham Lincoln Papers

EMANCIPATION PROCLAMATION

Introduction | Time Line | Gallery

Almost from the beginning of his administration, Lincoln was pressured by abolitionists and radical Republicans to issue an Emancipation Proclamation. In principle, Lincoln approved, but he postponed action against slavery until he believed he had wider support from the American public. The passage of the Second Confiscation Act by Congress on July 17, 1862, which freed the slaves of everyone in rebellion against the government, provided the desired signal. Not only had Congress relieved the administration of considerable strain with its limited initiative on emancipation, it demonstrated an increasing public abhorrence toward slavery.

Lincoln had already drafted what he termed his "Preliminary Proclamation." He read his initial draft of the Emancipation Proclamation to Secretaries William H. Seward and Gideon Welles on July 13, 1862. For a moment, both Secretaries were speechless. Quickly collecting his thoughts, Seward said something about anarchy in the South and possible foreign intervention, but with Welles apparently too confused to respond, Lincoln let the matter drop.

Nine days later, on July 22, Lincoln raised the issue in a regularly-scheduled cabinet meeting. The reaction was mixed. Secretary of War Edwin M. Stanton, correctly interpreting the Proclamation as a military measure designed both to deprive the Confederacy of slave labor and bring additional men into the Union Army, advocated its immediate release. Treasury Secretary Salmon P. Chase was equally supportive, but Montgomery Blair, the Postmaster General, foresaw defeat in the fall elections. Attorney General Edward Bates, a conservative, opposed civil and political equality for blacks but gave his qualified support. Fortunately, President Lincoln only wanted the advice of his Cabinet on the style of the Proclamation, not its substance. The course was set.

The Cabinet meeting of September 22, 1862, resulted in the political and literary refinement of the July draft, and on January 1, 1863, Lincoln composed the final Emancipation Proclamation. It was the crowning achievement of his

Brett (A.) & Co. Abraham Lincoln

Abraham Lincoln Papers

Almost from the beginning of his administration, Lincoln was pressured by abolitionists and radical Republicans to issue an Emancipation Proclamation. In principle, Lincoln approved, but he postponed action against slavery until he believed he had wider support from the American public. The passage of the Second Confiscation Act by Congress on July 17, 1862, which freed the slaves of everyone in rebellion against the government, provided the desired signal. Not only had Congress relieved the administration of considerable strain with its limited initiative on emancipation, it demonstrated an increasing public abhorrence toward slavery.

Lincoln had already drafted what he termed his "Preliminary Proclamation." He read his initial draft of the Emancipation Proclamation to Secretaries William H. Seward and Gideon Welles on July 13, 1862. For a moment, both Secretaries were speechless. Quickly collecting his thoughts, Seward said something about anarchy in the South and possible foreign intervention, but with Welles apparently too confused to respond, Lincoln let the matter drop.

Nine days later, on July 22, Lincoln raised the issue in a regularly-scheduled cabinet meeting. The reaction was mixed. Secretary of War Edwin M. Stanton, correctly interpreting the Proclamation as a military measure designed both to deprive the Confederacy of slave labor and bring additional men into the Union Army, advocated its immediate release. Treasury Secretary Salmon P. Chase was

Рис. 6-3. Включение режима чтения позволяет убрать лишние элементы из оригинальной страницы (слева) и переформатировать текст для облегчения чтения (справа)

Цвет

Размер

Линейка

Выход

principle, Lincoln approved, but he postponed action against slavery until he believed he had wider support from the American public. The passage of the Second Confiscation Act by Congress on July 17, 1862, which freed the slaves of everyone in rebellion against the government, provided the desired signal. Not only had Congress relieved the administration of considerable strain with its limited initiative on emancipation, it demonstrated an increasing public abhorrence toward slavery.

Lincoln had already drafted what he termed his "Preliminary Proclamation." He read his initial draft of the Emancipation Proclamation to Secretaries William H. Seward and Gideon Welles on July 13, 1862. For a moment, both Secretaries were speechless. Quickly collecting his thoughts, Seward said something about anarchy in the South and possible foreign intervention, but with Welles apparently too confused to respond, Lincoln let the matter drop.

Nine days later, on July 22, Lincoln raised the issue in a regularly-scheduled cabinet meeting. The reaction was mixed. Secretary of War Edwin M. Stanton, correctly interpreting the Proclamation as a military measure designed both to deprive the Confederacy of slave labor and bring additional men into the Union Army, advocated its immediate release. Treasury Secretary Salmon P. Chase was

1 Текст заметки

Рис. 6-4. Добавив примечания и сделав отметки на странице, вы можете сохранить их или отправить по электронной почте с помощью двух кнопок с правого края панели инструментов веб-заметки

Как и во всех современных браузерах, Microsoft Edge позволяет сохранять текущую страницу в Избранном и просматривать историю просмотра, список активных и прошлых загрузок. К этим стандартным возможностям добавилась функция Список чтения (Reading List). При щелчке на звездочке в конце адресной строки отображается диалоговое окно, в котором можно сохранить текущую страницу в избранном или добавить ее в список чтения.

По задумке, объекты в списке чтения являются временными – это страницы, которые пользователь хочет прочитать позднее. А список Избранное (Favorites) предназначен (по крайней мере, в теории) для сайтов, которые пользователь посещает регулярно.

Сохраненные объекты в списке для чтения отображаются в панели с миниатюрами, как показано на рис. 6-5.

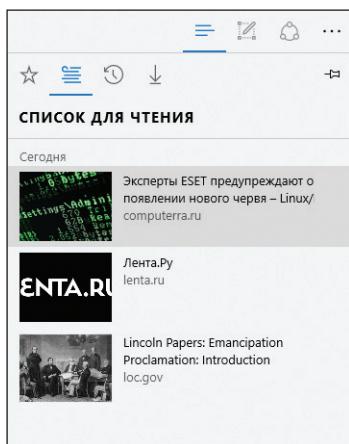


Рис. 6-5. Список для чтения – альтернатива списку Избранное. Элементы в нем сортируются и группируются по дате сохранения



Примечание. Стоит отметить, что Windows 8.1 включает приложение Список чтения (Reading List) со сходными функциями, используя чудо-кнопку Экспорт (Share) с современной версией Internet Explorer для сохранения ссылок. Это приложение все еще существует в Windows 10, но только для обратной совместимости с устройствами, работающими под управлением Windows 8.1. Его содержимое не связано с одноименной функцией в Microsoft Edge.

Microsoft Edge включает прямые обработчики Кортаны. При переходе на страницу, которую распознает Кортана, пользователю предлагается получить дополнительную информацию. Например, если посетить домашнюю страницу популярного ресторана, Кортана предложит часы работы, меню, отзывы и т.д. Если выбран просмотр дополнительной информации, то она отображается в панели справа, как показано на рис. 6-6.

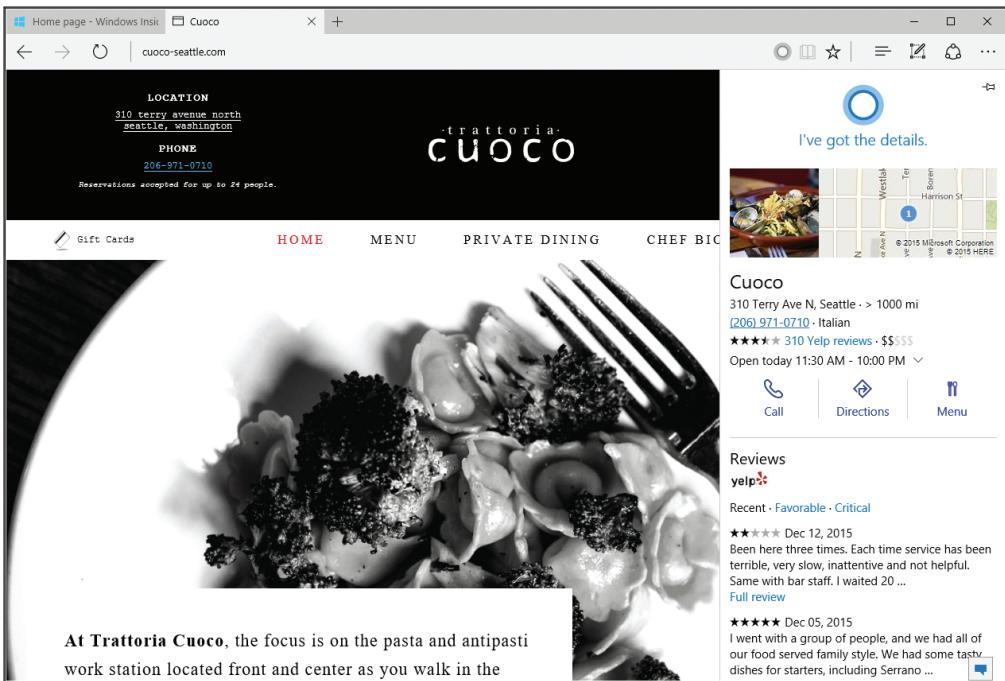


Рис. 6-6. Кортана интегрирована в Microsoft Edge и предлагает дополнительную информацию для некоторых веб-страниц

Кортана также доступна, если выделить слово или фразу на веб-странице, а затем щелкнуть правой кнопкой и выбрать команду Спросить Cortana (Ask Cortana) или начать переход к интересуемой странице. Например, если вы хотите отследить полет на завтра и начинаете вводить адрес авиалиний, Кортана немедленно скажет, если ли рейс завтра, – вам не нужно посещать веб-страницу, переходите на страницу состояния полета и вручную вводить информацию о полете.

В отличие от Internet Explorer, Microsoft Edge будет получать меньшие по размеру итеративные обновления на регулярной основе – аналогично тому, как это делается в других браузерах. Со временем к нему будут добавляться новые возможности. Обновление «Ноябрь 2015 Windows 10», например, включает возможность передачи мультимедиа на совместимое устройство, такое как Xbox One, остро необходимую возможность синхронизации Избранного и опцию предварительного просмотра вкладок, как показано на рис. 6-7.

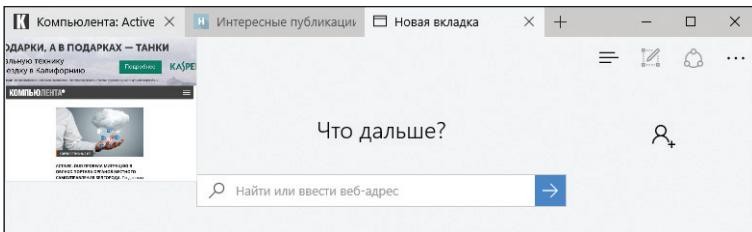


Рис. 6-7. Новая функция в Microsoft Edge версии 25 позволяет навести указатель мыши на вкладку, чтобы увидеть превью ее содержимого

Настройка режима предприятия в Windows 10

Используя движок Trident, Internet Explorer 11 в Windows 10 действует так же, как в Windows 7 или Windows 8.1. Это должно облегчить переход на Windows 10 и сократить проблемы совместимости для тех клиентов, которые уже обновились до Internet Explorer 11. В корпоративных развертываниях Microsoft рекомендует Internet Explorer 11 как стабильную и надежную веб-платформу для сложных бизнес-приложений, которые работают в веб-браузере.



Примечание. Microsoft Edge недоступен при развертывании Ветви долгосрочного обслуживания (Long Term Servicing Branch) Windows 10 Enterprise. Если не были изменены стандартные настройки, то в такой конфигурации доступен только Internet Explorer 11.

Microsoft Edge отображает все веб-страницы с помощью нового движка EdgeHTML, отвечающего современным стандартам. Можно переключиться к Internet Explorer 11 для сайтов в интрасети, сайтов, включенных в управляемый список сайтов или в список публичных веб-сайтов режима совместимости, управляемый Microsoft. Microsoft Edge также может выявлять сайты с устаревшей технологией, такой как элементы управления ActiveX, и предлагать вручную переключиться к Internet Explorer 11 для обратной совместимости.

Для внешних и внутренних сайтов, требующих другой режим документов для корректного отображения, особенно для сайтов, предназначенных для более старых версий Internet Explorer, можно включить режим предприятия (Enterprise Mode) и создать список сайтов с собственными настройками для каждого из них. После завершения конфигурирования сайтов Internet Explorer будет сам переключать режимы для отображения сайта или веб-приложения в корректном виде, не требуя вмешательства пользователей.

Режим предприятия доступен для всех редакций Internet Explorer, но по умолчанию он выключен. Его нельзя использовать, пока он не будет включен через объект групповой политики или через задание ключа в реестре.

Режим предприятия работает путем проверки адресов в списке веб-сайтов. Internet Explorer 11 использует заданный режим, если адрес сайта присутствует в списке. В Windows 10 Microsoft Edge автоматически переключается к Internet Explorer 11 для сайтов из списка сайтов режима предприятия.

Чтобы включить режим предприятия, нужно изменить настройку групповой политики с помощью настроек домена или, для одного устройства с Windows 10, с помощью редактора локальной групповой политики (gpedit.msc). Перейдите в раздел Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Internet Explorer (Computer Configuration > Administrative Templates > Windows Components > Internet Explorer) и включите политику Использовать список веб-сайтов IE в режиме предприятия (Use The Enterprise Mode IE Website List), как показано на рис. 6-8.

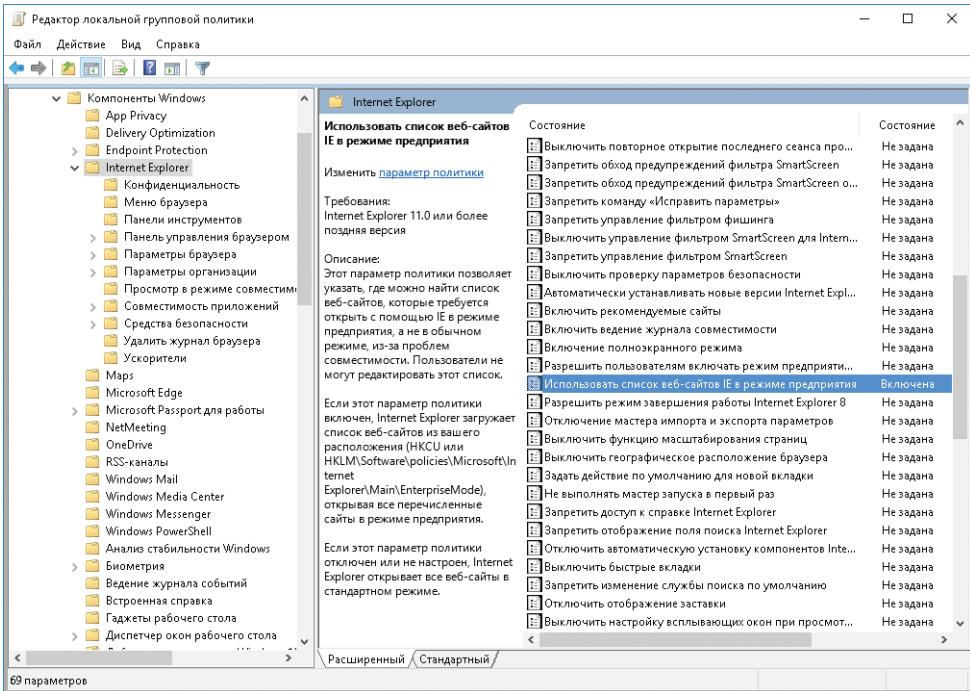


Рис. 6–8. Измените эту настройку групповой политики, чтобы включить режим предприятия

Включить режим предприятия можно также в редакторе реестра (Regedit.exe). Чтобы включить режим предприятия только для пользователя, который в данный момент находится в системе, отредактируйте значение SiteList (с типом REG_SZ) в разделе HKCU\Software\Policies\Microsoft\Internet Explorer\Main\EnterpriseMode. (Может потребоваться создать этот ключ и связанное с ним значение, если они еще не существуют.)

Чтобы включить режим предприятия для всех пользователей на ПК, отредактируйте значение SiteList (с типом REG_SZ) в разделе HKLM\ Software\ Policies\ Microsoft\ Internet Explorer\ Main\ EnterpriseMode. (Обратите внимание, что здесь используется узел HKLM, а не HKCU.)

Простого включения этой настройки недостаточно. Нужно указать, где находится список сайтов режима предприятия. Чтобы ввести расположение списка сайтов режима предприятия в редакторе локальной групповой политики или Regedit, используйте следующий синтаксис (при необходимости заменяя сервер, пользователя и страницу):

- **HTTP-адрес:** http://localhost:8080/sites.xml;
- **Локальная сеть:** \\сеть\\папка\\сайты.xml;
- **Локальный файл:** file:///c:\\Users\\<пользователь>\\Documents\\testList.xml.

На рис. 6-9 представлен синтаксис для списка сайтов режима предприятия, сохраненного в общей папке в локальной сети.

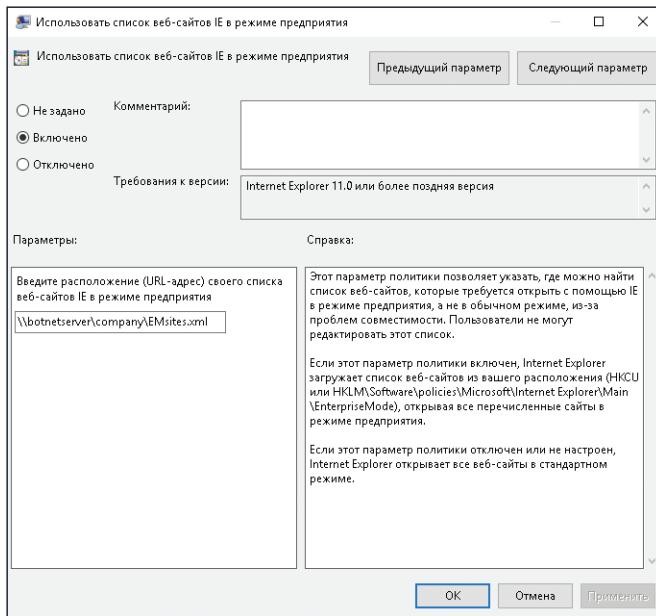


Рис. 6-9. Введите расположение файла для списка сайтов режима предприятия здесь или в соответствующем ключе в редакторе реестра

Чтобы добавлять и редактировать сайты в этом списке, установите утилиту Enterprise Mode Site List Manager, доступную в центре загрузок Microsoft: <http://www.microsoft.com/en-us/download/details.aspx?id=42501>.

Эта утилита позволяет добавлять сайты по одному или группой, указывать режим предприятия (по сути, эквивалентен настройкам режима совместимости из Internet Explorer 8) или вводить пользовательские режимы документа, как показано на рис. 6-10.

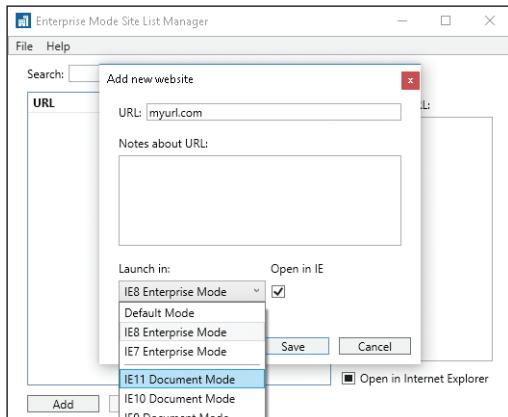


Рис. 6-10. Утилита Enterprise Mode Site List Manager позволяет редактировать содержимое локального или общего списка

Подробности о работе режиме предприятия приводятся на сайте TechNet по адресу <http://technet.microsoft.com/ie>. Дополнительная информация, включая советы по диагностике проблем, имеется в блоге Internet Explorer по адресу: <http://bit.ly/ie11-enterprise-mode>.

Сеть в Windows 10

Одна из ключевых задач современных версий Microsoft Windows – повысить продуктивность при работе на мобильных устройствах. Поэтому многие возможности, которые описываются в этой главе, будут особенно полезны на небольших планшетах, телефонах и других портативных устройствах.

Некоторые возможности, обсуждаемые в этой главе – это расширения функций, появившихся в Windows 8 и 8.1. Часть из них требует дополнительных функций на удаленном сервере. Другие зависят от аппаратного обеспечения, на устройствах, не обладающих соответствующим оборудованием, пользователь их попросту не увидит.

Усовершенствования беспроводной сети

Самое большое изменение «под капотом» – это новая модель драйверов Wireless Driver Interface (WDI). Она позволяет использовать универсальный пакет WLAN-драйвера, который поддерживает работу как в настольной, так и в мобильной версиях Windows 10.

Одно из преимуществ модели драйверов WDI – сотовые подключения и Wi-Fi подключения могут управляться одним сетевым стеком. Вы можете настроить лимитные подключения, чтобы избежать большие передачи данных, и отслеживать трафик по каждому сеансу подключения. Эта модель также обеспечивает большую надежность и быстрое восстановление, если устройство «зависает» по причинам, связанным с прошивкой. Новая модель драйверов также поддерживает рандомизацию MAC-адресов для повышения безопасности и конфиденциальности.

Bluetooth-устройства, как классические, так и энергосберегающие (low-energy, LE), также были усовершенствованы. Теперь они поддерживают широкополосную речь и аудио-кодек aptX, благодаря которому качество звука по Bluetooth-передаче сопоставимо с качеством при передаче по проводному подключению. На устройствах с повышенными требованиями к безопасности можно использовать ПО управления для принудительного применения Simple Secure Pairing (SSP). Эта возможность ограничивает класс подключаемых Bluetooth-устройств (например, только клавиатуры и мыши), уменьшая направления атак.

Три ключевых стандарта беспроводной связи поддерживают возможности, которые были введены в Windows 8.1 и усовершенствованы в Windows 10.

- **Радиочастотная связь ближнего действия** (Near-field communication, NFC). В Windows 8.1 была введена поддержка печати tap-to-pair (прикоснись для создания пары), которая позволяла ноутбукам и мобильным устройствам с поддержкой NFC связываться с корпоративным принтером с поддержкой NFC простым прикосновением. Добавить поддержку NFC к существующим принтерам позволяют NFC-метки. Windows 10 Mobile добавляет инфраструктуру,

которая позволяет превратить мобильное устройство в виртуальную кредитную карту, поддерживающую Host Card Emulation вместе с существующей поддержкой Universal Integrated Circuit Card (UICC) Secure Elements. Эта комбинация создает системы tap-to-pay (прикоснись, чтобы заплатить) на устройствах с Windows 10 Mobile. Она также позволяет приложениям tap-to-send (прикоснись, чтобы отправить) быстро обмениваться небольшими объемами данных, а также обмениваться данными с помощью NFC-меток.

- **Wi-Fi Direct.** Это относительно новый стандарт, который позволяет устройствам подключаться друг к другу по беспроводной сети в манере точка-к-точке (peer-to-peer), не требуя точки доступа. Поддержка нового API в Windows 10 означает, что приложения могут обнаруживать устройства, создавать пару и подключаться к устройствам автоматически, не требуя вмешательства пользователя. Та же технология может использоваться в корпоративных сетях для простых и защищенных подключений к принтерам без дополнительных драйверов или ПО.
- **Беспроводной дисплей Miracast.** Miracast – это еще один стандарт, использующий Wi-Fi Direct для потоковой передачи звука и видео с устройства на поддерживающий Miracast дисплей или проектор. Поддержка Miracast встроена во все устройства с Windows 10. Пользователи могут сопрягать планшет или ноутбук с Windows 10 с проектором конференц-зала с помощью Miracast и показывать презентацию без проводов или дополнительных адаптеров. Например, Wireless Display Adapter от компании Microsoft, представленный на рис. 7-1, подключается к HDMI-входу на большом телевизоре или другом дисплее, получает питание от близлежащего USB-порта и не требует никакой настройки.

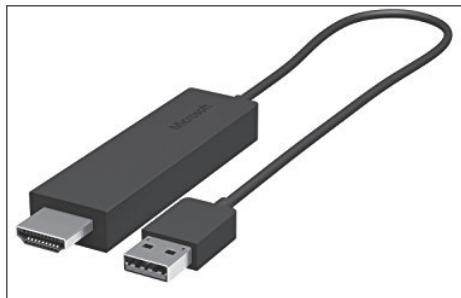


Рис. 7-1. Небольшой нетребовательный адаптер Microsoft Wireless Display Adapter подключается к любому дисплею с HDMI-входом и принимает удаленные подключения с любого устройства с Windows 10 с помощью Miracast

Многие из этих подключений можно выполнить, открыв Центра уведомлений (Action Center) и прикоснувшись к кнопке Подключиться (Connect) внизу панели под уведомлениями. На рис. 7-2 представлена Windows 10, готовая к подключению к Microsoft Wireless Display Adapter, ПК с Bluetooth и Bluetooth-гарнитуре.

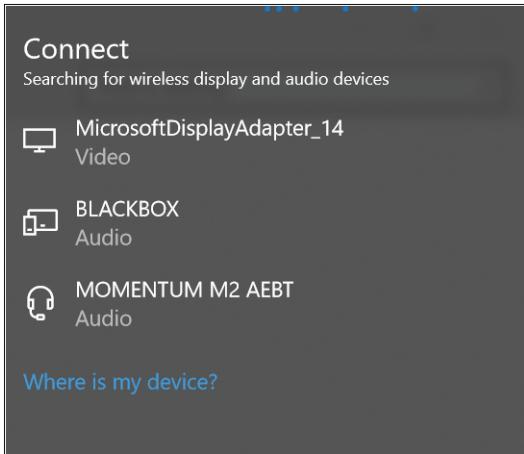


Рис. 7–2. При прикосновении к кнопке действия Подключиться (Connect) в Центре уведомлений (Action Center) перечисляются все доступные устройства с поддержкой Bluetooth, Wi-Fi Direct и Miracast, подключиться к которым можно прикосновением

Windows 10 включает новую возможность Wi-Fi Sense, которая позволяет автоматически подключаться к известным доверенным сетям. Введите «Wi-Fi» или «Беспроводная» в поле поиска приложения Параметры (Settings), чтобы открыть панель Wi-Fi, в которой перечисляются доступные подключения и присутствует переключатель для Wi-Fi подключения, как показано на рис. 7–3.

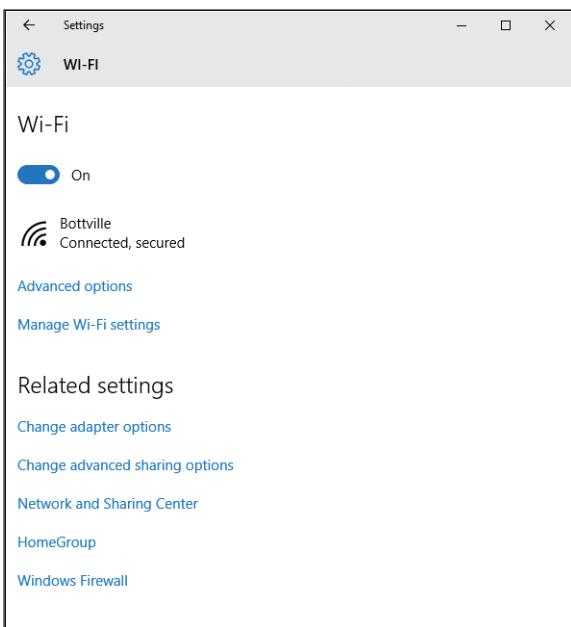


Рис. 7–3. Панель Wi-Fi предлагает простой переключатель, сведения о доступных подключениях и ссылки на несколько дополнительных опций

Щелкните или прикоснитесь к ссылке Управление параметрами сети Wi-Fi (Manage Wi-Fi Settings) внизу этой панели, чтобы отобразить настройки Контроль Wi-Fi (Wi-Fi Sense), представленные на рис. 7–4.

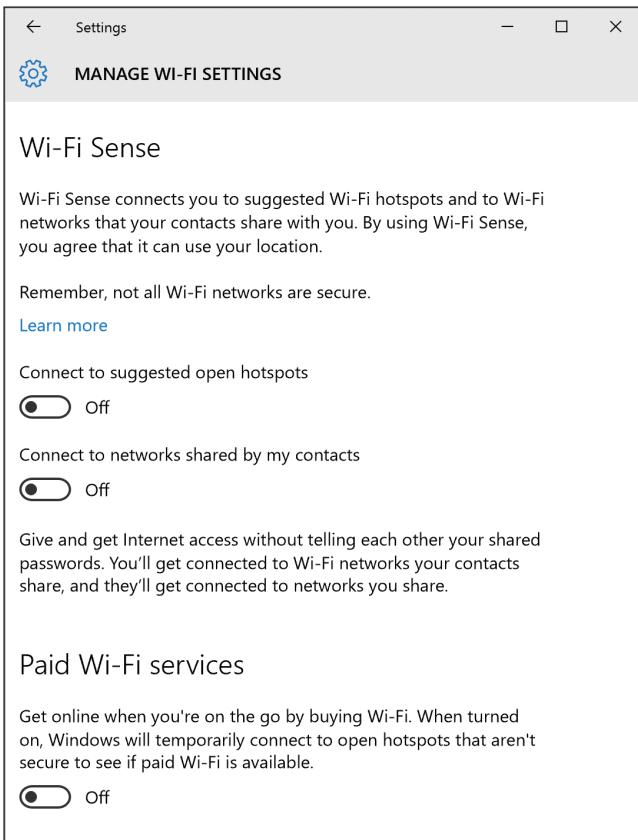


Рис. 7-4. Wi-Fi Sense позволяет автоматически подключаться к точкам доступа, которые были обозначены Microsoft как надежные или которыми с вами поделились ваши контакты

Эти функции подключаются в настройках групповой политики, которая была добавлена в Windows 10 версии 1511: Разрешить Windows автоматически подключаться к предложенным открытым хот-спотам, к сетям, доступ к которым предоставили контакты, и к хот-спотам, предлагающим платные услуги (Allow Windows To Automatically Connect To Suggested Open Hotspots, To Networks Shared By Contacts, And To Hotspots Offering Paid Services). Путь к настройке: Конфигурация компьютера > Административные шаблоны > Сеть > Служба WLAN > Параметры WLAN (Computer Configuration > Administrative Templates > Network > WLAN Service > WLAN Settings). Когда политика установлена в значение Отключено (Disabled), параметры Wi-Fi Sense отображаются в приложении Параметры (Settings), но установлены в значение Выключено (Off) и не могут изменяться пользователем.

Опытные пользователи Windows на Wi-Fi Sense резонно опасаются возможности автоматических подключений к опасным сетям и снижения безопасности домашней или рабочей сети. Не следует подключаться к тем открытым сетям, о которых вы ничего не знаете. Но если единственны сети, к которым выполняется автоматическое подключение, – это известные безопасные сети, то безопасность только улучшится.

Для Wi-Fi Sense поддерживается список открытых сетей, которые известны, безопасны и надежны, такие как официальные сети в аэропортах и отделениях почты, отелях и в постоянно уве-

личивающихся публичных местах в городах. Если вы или ваши пользователи посещаете новое место с устройством Windows 10 с включенным Wi-Fi Sense, то вы никогда не увидите сети, созданные преступниками; вы будете подключаться автоматически к известным сетям, которые заработали себе репутацию безопасных и надежных.

Опция Подключаться к сетям, доступ к которым предоставили мои контакты (Connect To Networks Shared By My Contacts) предназначена для потребительских точек доступа и роутеров Wi-Fi, использующих для аутентификации стандарт WPA2 с общим ключом, который пользователи должны вводить для доступа. При подключении к защищенной WPA2 домашней сети на устройстве с Windows 10 пользователю предлагается разделить подключение с контактами и друзьями.

Такое разделение подключения не позволяет приглашенному разделить его повторно со своими друзьями. Для этого им понадобится пароль.

На рабочих сетях, конечно же, не следует использовать безопасность на основе паролей. Вместо этого сеть должна быть защищена с помощью аутентификации 802.11X с сервером RADIUS, и каждый подключающийся должен выполнять вход с использованием учетных данных, которыми управляете вы. Относительно просто настроить это в большой корпоративной сети. Для малого бизнеса можно поискать что-то вроде JumpCloud (<http://jumpcloud.com>), который предоставляет сервис RADIUS по низкой стоимости. (На самом деле сервис особенно привлекателен для очень малого бизнеса, поскольку для организации до 10 пользователей он бесплатен.)

Опция Платные услуги сети Wi-Fi (Paid Wi-Fi Services) – это компаньон для нового приложения из Windows Store от Microsoft, которое называется, естественно, Microsoft Wi-Fi. Оно использует промышленный механизм аутентификации для обеспечения защищенного доступа к сетям на базе оплаты при подключении. Эта программа все еще находится в процессе развертывания, поэтому может пройти некоторое время, прежде чем ее можно будет использовать в регулярно посещаемых местах.

Защищенное подключение к корпоративным сетям

Удаленные сети по определению не являются доверенными. Работник, который подключается к бесплатной Wi-Fi сети в аэропорту или использует гостевую сеть в отеле, рискует, что его подключение может быть перехвачено злоумышленником с угрозой для данных в корпоративной сети.

Традиционно используется виртуальная защищенная сеть (virtual private network, VPN), которая шифрует подключение между корпоративной сетью и удаленным ПК, чтобы пакеты, путешествующие по недоверенной сети, не могли быть прочитаны атакующим.

Windows 8 включает базовый VPN-клиент. В Windows 8.1 была добавлена поддержка ограниченного числа VPN-поставщиков, включая Check Point, F5, Juniper Networks и SonicWall, помимо клиента Microsoft. В Windows 10 эта функциональность расширена: допускается использование любого поставщика VPN-решения, которое распространяется через Store.

В Windows 10 усовершенствована возможность автоматически запускать VPN-подключения при выборе приложения или ресурса, требующего VPN. При доступе к интрасети компании из удаленной сети пользователь сможет войти с помощью одного щелчка. Она также включает возможность создания постоянных (always-on) VPN-сессий, превращая удаленное устройство в постоянного члена корпоративной сети.

Поддержка VPN по приложениям работает в обратном направлении: администраторы могут создать список приложений, которым можно обращаться к корпоративным ресурсам через VPN, все остальные приложения будут блокироваться. На рис. 7-5 показано, как работает эта возможность.

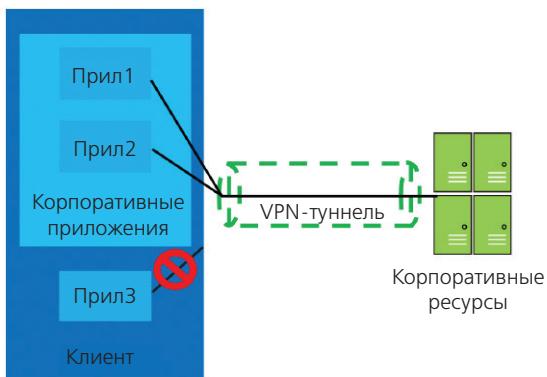


Рис. 7-5. Администраторы могут создавать списки приложений, которым разрешается обращаться к корпоративным серверам из удаленной сети, все остальные приложения будут блокироваться

Удаленное подключение к корпоративным сетевым ресурсам через VPN не свободно от некоторых сложностей, начиная с вопросов конфигурации и заканчивая потенциальными проблемами с безопасностью, если пользователи будут переподключаться к сети недостаточно часто, чтобы получать обновления безопасности и групповой политики. Лучшее решение – возможность DirectAccess, доступная в редакциях Enterprise Windows 10 и требующая подключения к Windows Server 2012 или более поздней версии.

DirectAccess позволяет удаленным пользователям безопасно обращаться к общим ресурсам, веб-сайтам и приложениям, когда их мобильное устройство с поддержкой DirectAccess подключено к Интернету. DirectAccess не требует частых входов или поддержки доступа и даже позволяет администраторам управлять удаленным компьютером без установки VPN-подключения. Эта возможность постоянного подключения упрощает работу и повышает эффективность при выполнении повседневных задач за пределами офиса.

На рис. 7-6 показаны простые настройки для правильно сконфигурированного подключения DirectAccess.

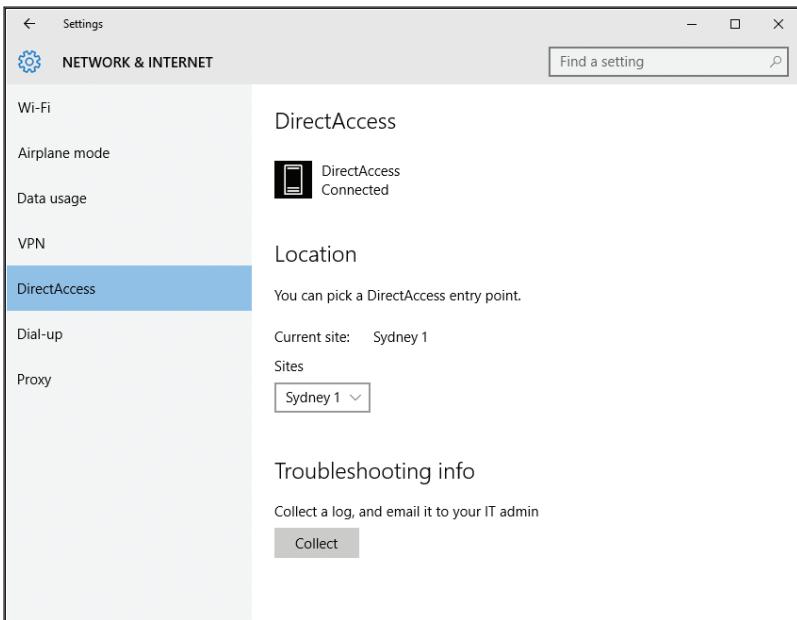


Рис. 7–6. Подключения DirectAccess обеспечивают безопасность VPN без забот по настройке и постоянному переподключению

Управление сетевыми подключениями

При переходе к новой версии Windows обиднее всего обнаружить, что важные возможности перемещены или удалены. Это особенно справедливо для первых выпусков Windows 10, в которых настройки переносятся из классической панели управления в новое приложение Параметры (Settings).

Доступные для пользователей кнопки и переключатели для настройки сетевых подключений перенесены не полностью, то есть большая часть функциональности все еще находится в старом Центре управления сетями и общим доступом (Network And Sharing Center), но некоторые функции уже перенесены на вкладку Сеть и интернет (Networking) приложения Параметры (Settings). Иногда можно поиском найти знакомые инструменты управления. Некоторые опции из более старых версий Windows, такие как просмотр карты сети или ручное переименование сети, временно недоступны.

В этом разделе приводится обзор самых необходимых инструментов.

На рис. 7-7 представлен прежний Центр управления сетями и общим доступом (Network And Sharing Center), который позволяет включать или отключать отдельные сетевые адаптеры и анализировать или изменять свойства существующих подключений.

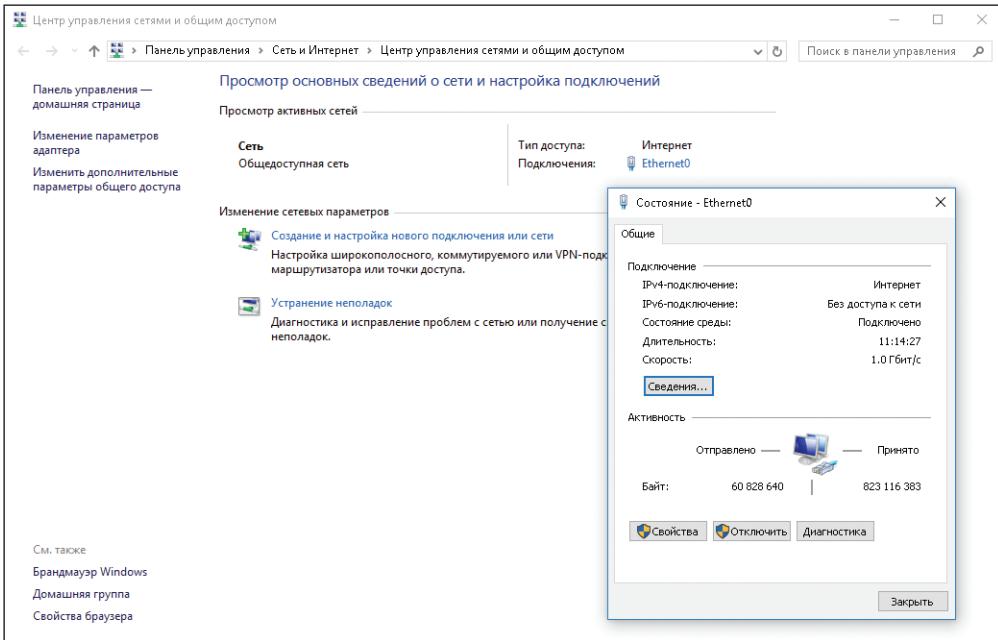


Рис. 7–7. Отправной точкой для большинства задач по администрированию сети все еще остается Центр управления сетями и общим доступом (Network And Sharing Center)

Страница Сеть и Интернет (Network & Internet) в новом приложении Параметры (Settings) содержит гораздо меньше опций, каждая панель включает несколько ссылок, которые возвращают к Центру управления сетями и общим доступом. Упомянем список сохраненных Wi-Fi сетей, который находится внизу панели Управление параметрами сети Wi-Fi (Manage Wi-Fi Settings). Как показано на рис. 7–8, здесь есть возможность «забыть» сохраненную сеть.

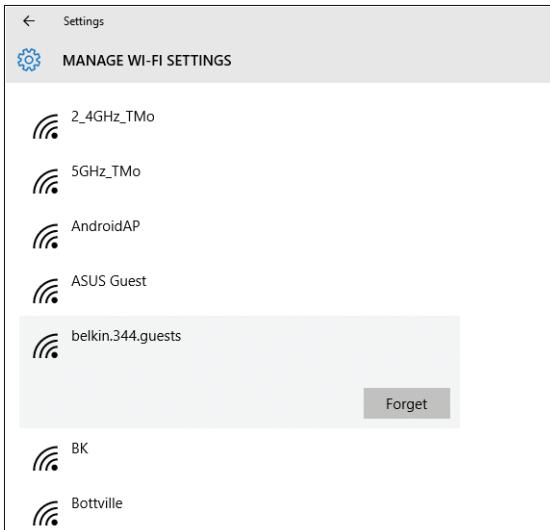
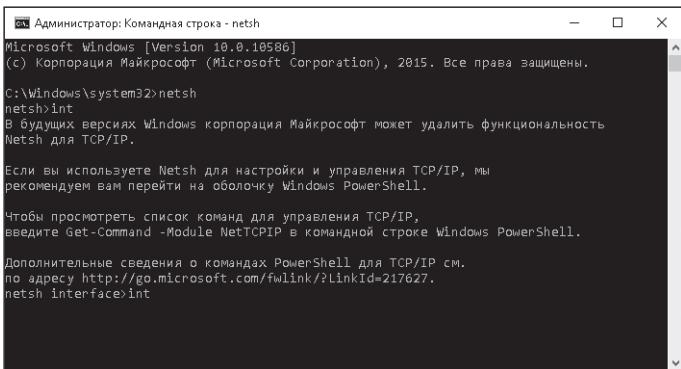


Рис. 7–8. Список сетей Wi-Fi, которые сохраняются для автоматического подключения впоследствии – одна из ключевых возможностей в новом приложении Параметры (Settings)

Управлять большинством опций можно из командной строки. Это хороший повод освежить навыки Windows PowerShell, с особым упором на командлеты управления сетью. Если вы раньше работали с утилитой командной строки Netsh, то сейчас самое время переключиться к PowerShell. Более старая функциональность Netsh в Windows 10 удалена как устаревшая, как показано на рис. 7-9.



```
Administrator: Командная строка - netsh
Microsoft Windows [Version 10.0.10586]
(c) Корпорация Майкрософт (Microsoft Corporation), 2015. Все права защищены.

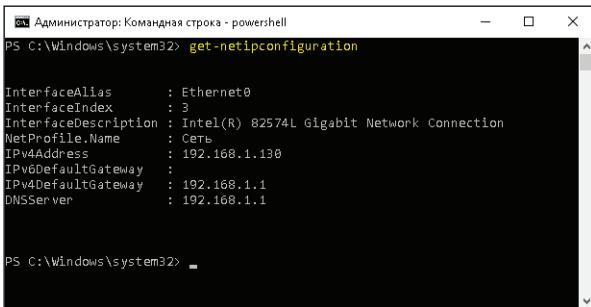
C:\Windows\system32>netsh
netsh!nt
В будущих версиях Windows корпорация Майкрософ트 может удалить функциональность
Netsh для TCP/IP.

Если вы используете Netsh для настройки и управления TCP/IP, мы
рекомендуем вам перейти на оболочку Windows PowerShell.

Чтобы просмотреть список команд для управления TCP/IP,
введите Get-Command -Module NetTCPiP в командной строке Windows PowerShell.

Дополнительные сведения о командах PowerShell для TCP/IP см.
по адресу http://go.microsoft.com/fwlink/?LinkId=217627.
netsh interface>int
```

К счастью, все, что умеет Netsh, можно сделать с помощью PowerShell, которая позволяет делать гораздо больше. В категории Net-TCP/IP имеются десятки командлетов, включая Get-NetIPConfiguration, который возвращает полный список деталей для текущей сети, как показано на рис. 7-10.



```
Administrator: Командная строка - powershell
PS C:\Windows\system32> get-netipconfiguration

InterfaceAlias      : Ethernet0
InterfaceIndex      : 3
InterfaceDescription: Intel(R) 82574L Gigabit Network Connection
NetProfile.Name     : Серь
IPv4Address         : 192.168.1.130
IPv6DefaultGateway : 192.168.1.1
DNSServer          : 192.168.1.1

PS C:\Windows\system32>
```

Рис. 7-9. Утилита командной строки Netsh все еще доступна в Windows 10, но теперь предпочтение следует отдавать командлетам PowerShell

Можно использовать другие командлеты, такие как New-NetIPAddress и Set-DnsClientServer-Address, для изменения настроек сети – в данном случае локального IP-адреса и адреса DNS-сервера для сетевого адаптера.

 **Примечание.** Полный список связанных с сетью команд PowerShell находится по адресу: <http://bit.ly/powershell-net-tcp>.

Поддержка IPv6

Переход от IPv4 к IPv6 идет ударными темпами, но путь еще длинный. Windows 10 полностью поддерживает сети IPv4, но выдача IPv4 адресов официально прекращена. Использование трансляции сетевых адресов (network address translation, NAT) позволяет домашним пользователям и малому бизнесу использовать один IPv4-адрес, но повсеместное использование NAT снижает эффективность служб геолокации и мешает работе многих приложений, которые полагаются на прямую коммуникацию. По ходу развития интернета вещей (Internet of Things), когда каждое устройство имеет собственное прямое подключение к нескольким сетям, проблемы будут становиться остree.

Чтобы избавиться от этих проблем, был создан IPv6 с невообразимой масштабируемостью, который предлагает $3,4 \times 10^{38}$ доступных IP-адресов (этого достаточно, чтобы каждый человек на земле имел миллиарды личных уникальных IPv6-адресов.) Помимо безмерного диапазона адресов, IPv6 также предлагает новые возможности безопасности, такие как IPsec, который обеспечивает безопасность на уровне пакетов. При переходе от IPv4 к IPv6 все еще реализуются двухстековые топологии. Это позволяет настраивать устройства с обоими адресами – IPv6 и IPv4.

Современные версии Windows (начиная с Windows 8) автоматически дают IPv6-адресу приоритет над IPv4-адресом. Поскольку некоторые приложения не поддерживают IPv6, Windows автоматически выбирает корректное подключение для приложений, используя метод сортировки адресов (address sorting).

Windows Server 2012 R2 расширяет поддержку IPv6 в групповой политике и позволяет использовать новые настройки с устройствами с Windows 8.1 и более новыми. При расширенной поддержке:

- принтеры TCP/IP могут настраиваться на использование адресов IPv6;
- в любой настройке групповой политики нацеливание на уровне элементов (item-level targeting) может использоваться для задания IPv6-адреса вместо диапазона IP-адресов;
- для VPN-подключений доступен флагок Использовать IPv6 (Use IPv6).

Дополнительные детали об этих настройках вы найдете по адресу: <http://technet.microsoft.com/en-us/library/dn265973.aspx>.

ГЛАВА 8

Hyper-V и варианты виртуализации рабочих столов

Обычно Microsoft Windows 10 устанавливается на физическое устройство. При этом операционная система, приложения и данные работают напрямую из локального накопителя. Такой подход обладает неоспоримыми преимуществами в плане производительности, но не в плане управления. Например, если локальный накопитель на физическом устройстве выйдет из строя, то данные пропадут, а при переключении к другому устройству пользователь не получит доступ к своей знакомой среде.

Решение подобных проблем – это виртуализация, которая принимает несколько форм. Windows 10 Pro и Enterprise включают возможность создания виртуальных машин (ВМ), в которых могут выполняться другие копии Windows, даже других редакций, на таком же профессиональном гипервизоре, который используется в продуктах Windows Server. В корпоративных средах администраторы могут применять серверные инструменты виртуализации для предоставления пользователям доступа к приложениям или полноценным средам рабочего стола.

В этой главе объясняется, как каждый из этих вариантов работает в Windows 10.



Дополнительная информация. Тема виртуализации заслуживает целой книги. За подробным обсуждением и руководствами по всем типам решений виртуализации обратитесь к веб-сайту Microsoft Desktop Virtualization по адресу: <http://www.microsoft.com/dv/>.

Глава начинается с самого простого решения, требующего минимум настроек.

Клиентский Hyper-V

Windows 8 была первой настольной версией Windows со встроенным гипервизором, позволяющим разработчикам и IT-профессионалам создавать виртуальные машины (ВМ), работающие под управлением Windows или альтернативных операционных систем, главным образом для тестирования и ознакомления. Клиентский Hyper-V – это полезный инструмент обеспечения совместимости, поскольку позволяет выполнять программы, требующими ранних версий Windows, не отказываясь от преимуществ самой последней версии Windows.

Клиентский Hyper-V использует ту же технологию и форматы виртуальных машин, что и текущие версии Windows Server. Это позволяет перемещать виртуальные машины между серверами и клиентскими компьютерами и запускать их без каких бы то ни было изменений. Клиентс-

кий Hyper-V работает на 64-разрядных версиях Windows 10 Pro и Enterprise. Он поддерживает 32-разрядные и 64-разрядные гостевые операционные системы, которые могут создаваться «на лету» из физического установочного носителя или при подключении ISO-файла. Можно также создать виртуальный жесткий диск (virtual hard disk, VHD) с физического диска, даже с работающей операционной системой, с помощью инструмента Disk2vhd, доступного по адресу: <http://technet.microsoft.com/en-US/sysinternals/ee656415>.



Дополнительная информация. В корпоративных средах для конвертации физических компьютеров в виртуальные машины может использоваться диспетчер виртуальных машин (Virtual Machine Manager) в System Center. Обзор процесса приводится в статье «How to Deploy a Virtual Machine by Converting a Physical Computer (P2V)» по адресу: <http://technet.microsoft.com/en-us/library/hh368990.aspx>.

Инструменты управления Hyper-V в Windows 10 будут знакомы тем, кто использовал эту возможность в Windows 8.1 или Windows Server 2012 R2. Windows 10 содержит несколько важных возможностей, которые по достоинству будут оценены IT-профессионалами.

- **Рабочие контрольные точки** (Production checkpoints). Эта опция, которая включена по умолчанию в новых ВМ, создаваемых с помощью Windows 10, позволяет задавать контрольную точку, использующую службу Volume Snapshot Service для создания резервных копий типа «точка во времени», которые можно легко восстанавливать. Эта возможность особенно полезна для сценариев тестирования и более надежна, чем старая технология контрольных точек, которая сохраняла текущее состояние ВМ и всех выполняющихся приложений и служб. На рис. 8-1 представлена эта возможность в настройках конфигурации виртуальной машины.

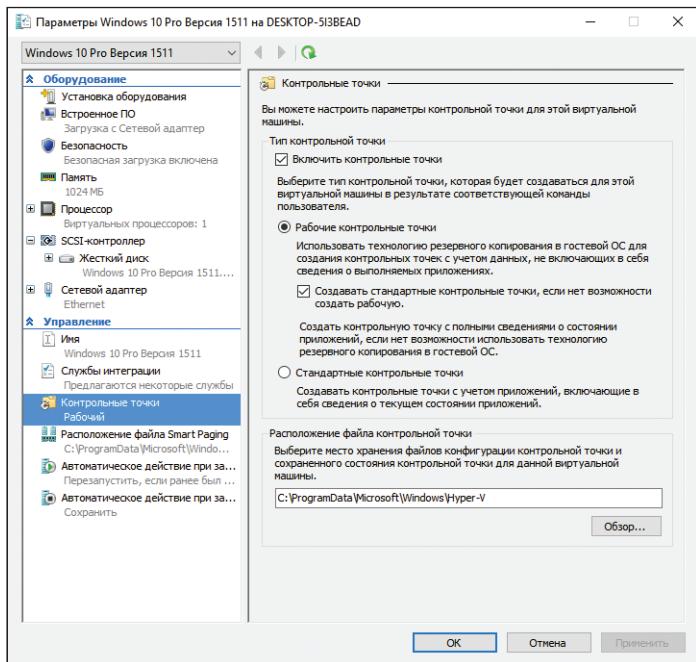


Рис. 8-1. Рабочие контрольные точки, которые создают полную резервную копию с помощью технологии Volume Snapshot – новинка в Windows 10

- **Новый формат файла конфигурации.** Виртуальные машины, созданные в Windows 10, используют версию конфигурации 6.2 (в выпуске Июль 2015) или версию 7.0 (в Windows 10 версии 1511) и сохраняют информацию о конфигурации в новом двоичном формате файла, который более надежен, чем старый формат на основе XML. Новые конфигурационные файлы используют расширение .VMCX для данных конфигурации виртуальной машины и расширение .VMRS для данных состояния времени выполнения.
- **Новые опции безопасности.** Виртуальные машины, созданные с использованием формата поколения 2, поддерживают Безопасную загрузку (Secure Boot). Начиная с версии 1511, машины Hyper-V поддерживают виртуальный Trusted Platform Module (TPM), который позволяет использовать полное шифрование диска на виртуальных машинах. (Для работы этой опции необходимо включить Режим изолированного пользователя [Isolated User Mode].)
- **«Горячее» добавление памяти и сетевых адаптеров.** Можно изменять объем памяти, назначеннной виртуальной машине, даже когда она работает и динамическая память не включена. Эта опция работает для виртуальных машин обоих поколений – 1 и 2. На виртуальных машинах поколения 2 можно добавлять или удалять сетевой адаптер, когда виртуальная машина работает.
- **Совместимость с режимом ожидания с подключением.** Когда роль Hyper-V включена на компьютере, который использует план питания Always On/Always Connected (AOAC) (например, Microsoft Surface Pro 3 или 4 или Surface Book), режим питания Ожидание с подключением (Connected Standby) доступен и работает как положено. В Windows 8.1 такая конфигурация приводила к проблемам с питанием.
- **Усовершенствованный диспетчер Hyper-V.** Консоль управления Hyper-V в Windows 10 поддерживает больше сценариев удаленного управления (включая управление гипервизорами на предыдущих версиях Windows настольных и серверных выпусков). Она также позволяет использовать альтернативные учетные данные для управления Hyper-V на удаленном компьютере или сервере.

Клиентский Hyper-V не включен в стандартную установку Windows 10. Перед его использованием на отдельном ПК или как часть стандартного образа нужно убедиться, что работает 64-разрядная операционная система, что машина-хост поддерживает инструкции Second Level Address Translation (SLAT) и что эта возможность включена. Большинство современных ПК для корпоративного использования включают эту возможность.

Чтобы включить клиентский Hyper-V, на ПК с 64-разрядной Windows 10 Pro, Enterprise или Education нужно выполнить следующие действия.

1. В настольной панели управления щелкните на Программы (Programs), а затем выберите Программы и компоненты (Programs And Features).
2. Выберите Включение или отключение компонентов Windows (Turn Windows Features On Or Off).
3. Выберите опцию Hyper-V и убедитесь, что под ней также выбраны дополнительные элементы, как показано на рис. 8-2. Щелкните на кнопке OK и перезагрузите ПК, чтобы включить эти возможности.

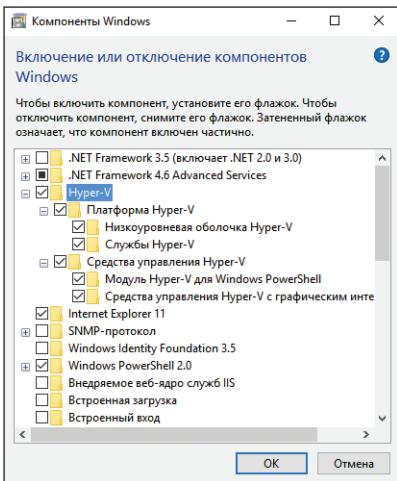


Рис. 8-2. Возможности клиентского Hyper-V в Windows 10 Pro, Enterprise или Education должны быть включены в этом диалоговом окне

Чтобы включить клиентский Hyper-V с помощью Windows PowerShell, воспользуйтесь следующим командлетом:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V
```

Чтобы использовать виртуальный TPM, понадобится включить Режим изолированного пользователя (Isolated User Mode). Это может быть сделано в диалоговом окне Включение или отключение компонентов Windows (Turn Windows Features On Or Off) или с помощью последовательности команд PowerShell:

```
Install-WindowsFeature Isolated-Usermode  
New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard -Force  
New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard  
-Name  
EnableVirtualizationBasedSecurity -Value 1 -PropertyType DWord -Force
```



Примечание. Подробное обсуждение усовершенствований безопасности в самом последнем выпуске Hyper-V и переноса защищенных виртуальных машин между компьютерами см. в статье TechNet «Virtual machine security settings in Hyper-V Manager» по адресу: <https://technet.microsoft.com/library/mt403347.aspx>.

Если Hyper-V включен, нужно полностью выключить и перезагрузить компьютер для завершения установки. После перезагрузки можно создавать виртуальные машины и управлять ими с помощью мастера в диспетчере Hyper-V или с помощью модуля Hyper-V для Windows PowerShell. На рис. 8-3 показан мастер для интерактивного создания новой виртуальной машины.

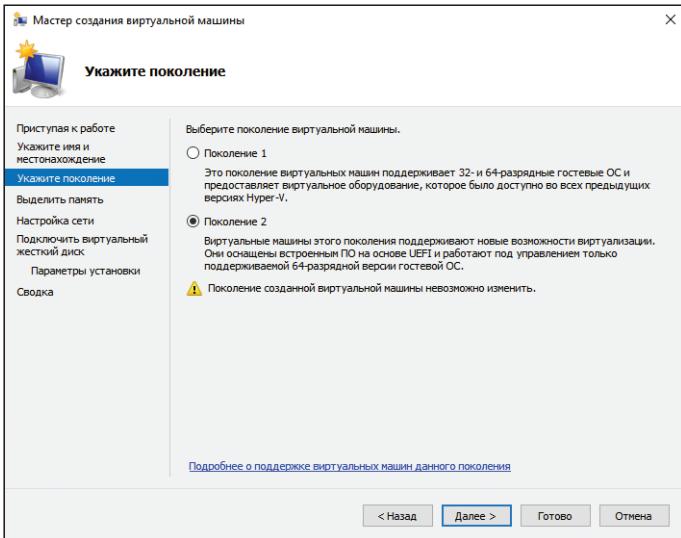


Рис. 8-3. Клиентский Hyper-V в Windows 10 поддерживает виртуальные машины Поколения 2, которые базируются на UEFI и требуют установки 64-разрядной гостевой операционной системы

Программа Virtual Machine Connection позволяет работать с виртуальными машинами или обращаться к ним в расширенном сеансе, используя вариант технологии удаленного рабочего стола. Стоит отметить, что машина Hyper-V может поддерживать до 12 мониторов с поддержкой беспроводных сетей и режимов сна и гибернации на машине-хосте. Машины Hyper-V не поддерживают аудио или USB-устройства, хотя в расширенном сеансе могут быть включены аудио подключения и подключения к некоторым типам USB-устройств.

Поддержка нескольких точек касания недоступна с ВМ Hyper-V, хотя одна точка касания доступна при совместимости оборудования.

Варианты виртуализации рабочих столов

В современном мире пользователи часто переключаются между разными устройствами, среди которых есть и автономные, поэтому важно предоставить этим пользователям безопасный доступ к знакомой рабочей среде. Microsoft предоставляет ряд решений уровня предприятия, которые позволяют запускать управляемые рабочие столы в центре данных. Пользователи получают доступ к рабочим столам на общем ресурсе, при этом их персональная среда остается нетронутой.

Windows 10 предлагает такие решения виртуализации, которые для пользователя практически идентичны физическому рабочему столу. Дополнительные серверные решения позволяют виртуализировать отдельные приложения. В центре данных администраторы могут эффективно управлять приложениями и данными и быть уверенными в правильном применении политик безопасности и соответствия.

Спустя несколько недель после выпуска Windows 10 появился Microsoft Desktop Optimization Pack (MDOP) 2015, который доступен клиентам Volume License с соглашениями Software Assurance, а также доступен для тестирования и оценки в составе подписок MSDN. MDOP позволяет исполь-

зователь три технологии виртуализации: Microsoft Application Virtualization (App-V), Microsoft User Experience Virtualization (UE-V) и Microsoft Enterprise Desktop Virtualization (MED-V).

Microsoft Azure предлагает похожие возможности виртуализации с помощью Azure RemoteApp, которая доставляет приложения Windows из облака на широкий диапазон клиентских устройств, включая работающие под управлением Windows 10.

Движок виртуальных рабочих столов – это службы Remote Desktop Services (RDS), они появились в Windows Server 2012 и доступны в Windows Server 2016, который основывается на той же кодовой базе, что и Windows 10, и пока находится в состоянии технического предварительного выпуска. RDS предоставляет единую платформу для доставки любого типа размещаемого рабочего стола, а RemoteFX обеспечивает согласованное полнофункциональное взаимодействие с пользователем.

- **Полноценное взаимодействие с пользователем.** RemoteFX использует встроенный программный GPU или аппаратный GPU на сервере для обеспечения 3D-графики и полнофункциональных мультимедиа-возможностей. RemoteFX также предлагает перенаправление USB-устройств и поддержку несколько точек касания, что актуально для планшетов. Производительность остается на высоком уровне даже при передаче через сети с большой задержкой и небольшой полосой пропускания, в том числе глобальные сети.
- **Низкая стоимость.** FairShare гарантирует высокую производительность системы путем динамического распределения системных ресурсов. Диски профилей пользователей обеспечивают гибкость для развертывания рабочих столов на основе пулов и сеансов, предоставляя пользователям возможность персонализировать свою рабочую среду. Также поддерживается мало затратное дисковое хранилище Direct Attached Storage.
- **Простое управление.** Простой мастер облегчает настройку виртуализации рабочих столов с помощью автоматической конфигурации виртуальных машин. Консоль управления на сервере предоставляет средства для администрирования пользователей, виртуальных машин и сеансов. В каких-то дополнительных инструментах нет необходимости.



Дополнительная информация. Дополнительная информация о службах Remote Desktop Services, включая ряд полезных руководств по подготовке тестовой среды, приводится в статье: <http://technet.microsoft.com/en-us/library/hh831447.aspx>.

С помощью RDS виртуальные рабочие столы могут доставляться одним из следующих методов.

- **Персональные виртуальные машины.** Персональные ВМ дают пользователям доступ к выделенному высокопроизводительному рабочему столу, над которым они имеют полный контроль.
- **ВМ в составе пула.** ВМ в составе пула дают пользователям доступ к высокопроизводительным рабочим столам с подключенными устройствами. RDS назначают пользователям ВМ по запросу из существующего пула. Когда пользователь выходит из ВМ, RDS возвращает ВМ в пул для другого пользователя.

- **Рабочие столы на основе сеансов.** Рабочие столы на основе сеансов предоставляют доступ к приложениям, данным и общим рабочим столам, которые централизованно размещены в центре данных. Это вариант традиционных терминальных служб для виртуализации рабочих столов.



Примечание. Пользуясь виртуальными машинами из состава пула и рабочими столами на основе сеансов, пользователи могут настроить свои рабочие столы, хотя и не могут устанавливать приложения. Перемещаемые профили пользователей и перенаправление папок обеспечивают персонализированные рабочие среды, а RDS добавляет поддержку дисков профилей пользователей. Когда диски профилей пользователей включены, RDS подключает виртуальный жесткий диск, содержащий настройки и данные пользователя, к папке профиля пользователя, и сохраняет эти данные между сеансами.

Выбор предпочтительного метода зависит от сочетания разных факторов. Здесь они рассматриваются подробно, а сведены в табл. 8-1.

- **Персонализация.** Нужно ли пользователям настраивать свои рабочие столы? Если да, то какой уровень настройки необходим? Для рабочих столов на основе сеансов и виртуальных машин из состава пула возможности персонализации с дисками профиля пользователя ограничены (т.е. данные между разными входами в систему могут не сохраняться). Установленные пользователями приложения не сохраняются между сеансами. На персональных ВП с административным доступом пользователи могут изменять любые возможности своего рабочего стола, включая установку приложений, которые будут сохраняться между сеансами работы.
- **Совместимость приложений.** Рабочие столы на основе сеансов делят общую серверную операционную систему; следовательно, любые устанавливаемые приложения должны быть совместимы с Windows Server 2012 или позднее. В сценариях ВМ, однако, Windows 10 выполняется в ВМ, что позволяет устанавливать приложения, совместимые с этой клиентской операционной системой. Администраторы управляют приложениями, устанавливаемыми на ВМ из состава пула.
- **Плотность пользователей.** Рабочие столы на основе сеансов делят одну операционную систему сервера, поэтому один сервер всегда будет обслуживать больше пользователей, чем в любом другом сценарии виртуальных машин. У ВМ из состава пула размеры обычно меньше, чем у персональных ВМ, поскольку данные пользователей не хранятся локально (но могут храниться в отдельном диске профиля пользователя). В результате ВМ из состава пула имеют немногим более высокую плотность. Можно повысить плотность ВМ из пула и персональных ВМ с помощью технологий виртуализации состояния пользователя и виртуализации приложений на ВМ, но они всегда будут иметь меньшую плотность по сравнению с рабочими столами на основе сеансов.
- **Число образов.** Лучший способ использовать один образ – это рабочие столы на основе сеансов или развертывание ВМ из пула. В рабочем столе на основе сеансов все пользователи делят один образ сервера. В случае с ВМ из пула все пользователи используют клонированную копию одного образа. Конфигурациями с одним образом легче управлять, и они обходятся дешевле, чем персональные ВМ, в которых каждый пользователь использует отдельный образ.

- Затраты.** Поскольку виртуализация на основе сеансов предлагает наивысшую плотность и один образ, то она обычно управляется легче всего и с минимальными затратами. ВМ из пула имеют один образ и преимущества управления виртуализации на основе сеансов, но большие затраты на развертывание из-за меньшей плотности и более сложного управления. Персональные ВМ имеют наименьшую плотность и наивысшую сложность в управлении, что делает их самым дорогим методом развертывания. Организации могут снизить общие затраты, используя преимущества дешевого хранилища, виртуализации приложений, динамической памяти и дисков профилей пользователей.

Табл. 8-1. Выбор оптимального варианта виртуализации рабочего стола

	Рабочий стол на основе сеансов	ВМ в составе пула	Персональные виртуальные машины
Персонализация	**	**	***
Совместимость приложений	**	***	***
Легкость в управлении	***	**	*
Эффективность затрат	***	**	*

* = Хорошо; ** = Лучше; *** = Наилучший.

Виртуализация приложений

Microsoft предлагает два решения для виртуализации приложений, оба доступны в Windows Server 2012 и Windows Server 2012 R2 (и продолжают совершенствоваться в Windows Server 2016).

Первое – RemoteApp, которое основывается на сеансовой виртуализации. Это решение представляет приложения удаленно через RDS. Приложения работают в центре данных на оборудовании, управляемом IT-службой. Перенося их из организации в центр данных, вы улучшаете управление безопасностью и целостность конфиденциальных данных.

Пользователи могут легко обращаться к своим удаленным приложениям с разнообразных клиентов – через веб-страницу или RDS-клиент. Кроме того, удаленные приложения работают рядом с локальными. Например, они работают в своих собственных окнах изменяемого размера, их можно перетаскивать между несколькими мониторами, у них есть свои собственные значки на экране Пуск (Start) или панели задач.

Второе решение – это App-V, которое является частью MDOP. Оно упаковывает приложения, которые могут передаваться потоком с сервера и выполняться без установки приложения. Пользователи могут обращаться к своим приложениям динамически практически с любого места на любом уполномоченном ПК, щелкнув на пакете для запуска приложения. В результате работа с приложением ведется так, как если бы оно выполнялось локально.

Виртуальные приложения работают в своих собственных неавтономных виртуальных средах на пользовательских ПК. Это устраняет конфликты приложений – на самом деле можно запустить несколько версий одной и той же программы на одном ПК даже таких программ, которые не позво-

ляют устанавливать на одном ПК несколько своих копий. Виртуальные приложения и настройки пользователя сохраняются независимо от того, подключен ли пользователь к сети. Вместе с виртуализацией состояния пользователя App-V обеспечивает согласованную работу с пользователем и надежный доступ к приложениям и бизнес-данным независимо от расположений пользователей или ПК.

На рис. 8-4 представлена общая схема работы этого типа виртуализации на предприятии.

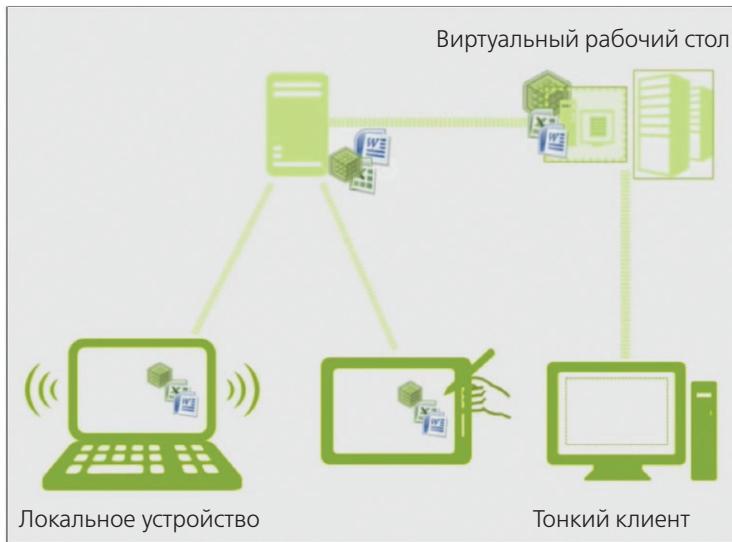


Рис. 8-4. Виртуализуемые приложения могут доставляться на локальные устройства с помощью App-V или развертываться как часть виртуального рабочего стола с помощью RemoteApp, не требуя локальных установок

Администратор App-V использует секвенсор для создания пакета приложения, который сохраняется с расширением имени файла .appv. Секвенсор выполняет мониторинг процесса установки.

Развертывание пакетов виртуальных приложений выполняется с помощью серверов App-V, которые по запросу передают потоком виртуальные приложения на пользовательские ПК и локально кэшируют их для работы с ними офлайн. Другой вариант – использовать диспетчер конфигурации (Configuration Manager) для развертывания, обновления и отслеживания работы физических и виртуальных приложений. Так можно использовать существующие процессы, рабочие процедуры и инфраструктуру для доставки виртуальных приложений пользователям.

App-V 5.0, который был выпущен одновременно с Windows 8, предлагает основанный на вебе интерфейс управления и поддержку Windows PowerShell для создания сценариев сложных или повторяющихся задач. Его возможности динамической конфигурации позволяют доставлять один пакет с разными настройками для разных групп пользователей. Приложения и их зависимости могут упаковываться отдельно, чтобы облегчить процесс обновления.

App-V 5.1 – это текущий выпуск, включенный в состав MDOP 2015 и требуемый для Windows 10. (App-V 5.0 и предыдущие версии несовместимы с Windows 10, хотя пакеты App-V, созданные с помощью App-V 5.0, совместимы и не требуют преобразования.) Эта версия поставляется в настольной и RDS версиях, она удобнее и производительнее, позволяет устанавливать приложения, использующие расширения оболочки, и включать зависимости времени выполнения, такие как MSXML и библиотеки Microsoft Visual C++.



Примечание. За дополнительной информацией о App-V 5.1 обратитесь по адресу: <http://bit.ly/app-v-51>.

Виртуализация User Experience

Виртуализация User Experience (UE-V) дебютировала в MDOP вместе с Windows 8. Эта корпоративная возможность позволяет администраторам концентрировать приложения и настройки Windows в центре, позволяя пользователям обращаться к своим настольным приложениям практически из любого места и на любом из своих устройств.

Самый последний выпуск, UE-V 2.1 SP1, добавляет поддержку Windows 10. Он поддерживает приложения Windows Store, включая приложения, приобретенные через Store и бизнес-приложения (line-of-business, LOB), разворачиваемые внутренне. По умолчанию синхронизируется множество настроек Windows (например, фон рабочего стола и настройки панели задач); приложения Microsoft Office 2010 и Microsoft Office 2013; Internet Explorer 11; все предустановленные приложения Windows; ряд настольных приложений Windows. В SP1 была добавлена поддержка перемещаемых сетевых принтеров.

Центр настроек компании (Company Settings Center) позволяет пользователям управлять синхронизацией настроек на устройствах, диагностировать проблемы с этими устройствами и синхронизировать настройки вручную, не дожидаясь автоматической синхронизации.



Дополнительная информация. Дополнительную информацию о UE-V вы найдете по адресу: <https://technet.microsoft.com/en-us/library/dn458926.aspx>.

Перенаправление папок (Folder Redirection) дополняет UE-V, собирая папки с данными пользователя (Документы, Изображения, Видео и т. д.) в центре данных и делая их доступными пользователям с любого ПК, когда они входят в систему со своими учетными данными домена. Пользователи с любого ПК имеют полный доступ к своим документам, изображениям, видео и другим файлам.

Новая возможность под названием Рабочие папки (Work Folders), представленная в Windows 8.1, предлагает существенные усовершенствования в сравнении с перенаправлением папок и автономными файлами. (Наиболее заметное – это возможность синхронизации файлов на устройствах, которые не подключены к домену.) Рабочие папки подробно рассматриваются в главе 13.

Инструменты восстановления и устранения неполадок

Для большинства проблем с Microsoft Windows IT-профессионалы применяли метод «очисти и загрузи». Сейчас Microsoft и сторонние разработчики ПО предоставили массу инструментов для создания корпоративных образов. Восстановите этот образ, и пользователь может продолжать работу.

Эта стратегия прекрасно работает с устройствами, которыми владеет организация, особенно с теми, которые выполняют конкретные задачи и подключаются к корпоративной сети. Если настольный ПК испытывает проблемы, причины которых не удается быстро диагностировать, можно воспользоваться средой развертывания и восстановить стандартный образ, а затем восстановить среду пользователя из сети.

Но в современных компаниях идет постоянный рост автономных устройств у мобильных сотрудников. Принести в IT-отдел устройство, состоящее на балансе организации, – не вариант для путешествующего сотрудника. Автономные устройства приводят к дополнительным проблемам в организациях, которые поощряют сотрудников работать на собственных устройствах. Для таких ситуаций Windows 10 включает набор инструментов восстановления, которыми пользователь (возможно, с помощью службы поддержки) может выполнить типичные действия по устранению неполадок, вплоть до полного восстановления стандартной операционной системы.

В Windows 10 появились важные изменения в работе процесса «сброс по нажатию кнопки». Решена раздражающая проблема длительного времени восстановления образа (больше не нужно ждать несколько часов для применения обновлений), и значительно снижен объем места, необходимого для стандартной установки.

В этой главе рассматриваются доступные инструменты устранения неполадок для Windows, в том числе входящие в состав операционной системы, и некоторые полезные внешние инструменты. Для организаций с соглашением Volume License с Software Assurance доступен дополнительный чрезвычайно полезный ресурс Microsoft Diagnostics and Recovery Toolset (DaRT).

В этой главе обсуждаются варианты восстановления и устранения неполадок.

Использование среды восстановления Windows

Что происходит, когда Windows 10 не запускается правильно при включении ПК или мобильного устройства? Отправной точкой для всех инициируемых пользователем операций исправления и восстановления является среда восстановления Windows (Windows Recovery Environment,

Windows RE). Эта среда появилась в Windows 8 и включает подборку ключевых инструментов для диагностики проблем и исправления проблем с запуском. На ПК с поддержкой EUFI образ Winre.wim копируется в раздел Windows RE Tools на заключительном этапе установки. На ПК с BIOS образ копируется в раздел System. Такая схема позволяет запустить Windows RE даже в случае проблем с разделом Windows.

Windows RE запускается автоматически в определенных сценариях, в том числе после двух последовательных неудачных попыток запуска Windows, двух последовательных завершений в течение двух минут по окончании загрузки, ошибки защищенной загрузки (Secure Boot), ошибки BitLocker на сенсорном устройстве.

Запустить Windows RE можно и вручную: с установочного носителя Windows 10, с диска восстановления или с раздела восстановления на устройстве, если этот вариант доступен. Пользователь может также запустить Windows RE вручную из Windows 10, воспользовавшись опцией Особые варианты загрузки (Advanced Startup) в Параметры (Settings), Обновление и безопасность (Update & Security); выбрав команду Перезагрузка (Restart) из меню Пуск (Start), удерживая нажатой клавишу **Shift** или введя команду **Shutdown /r /o**.

В начальном меню Выбор действия (Choose An Option) пользователю предоставляется возможность щелкнуть на Продолжить (Continue), чтобы попытаться запустить операционную систему, не предпринимая каких-либо действий. (Это правильный вариант, если система загрузилась в Windows RE из-за временной проблемы, которая не требует исправления.)

Если на компьютере установлено несколько операционных систем, то меню Выбор действия (Choose An Option) может отобразить команду Использовать другую операционную систему (Use Another Operating System), которая позволяет выбрать альтернативную операционную систему для загрузки. Опция Использовать устройство (Use a Device) позволяет загрузиться с USB-накопителя флэш-памяти, DVD или сервера сетевой загрузки.

При выборе опции Поиск и устранение неисправностей (Troubleshoot) открывается экран Диагностика (Troublesheet) с опциями, похожими на представленные на рис. 9-1. На OEM-компьютерах может также присутствовать опция Восстановить заводской образ (Factory Image Restore). Организации, разворачивающие собственные образы, могут добавлять опции в это меню.

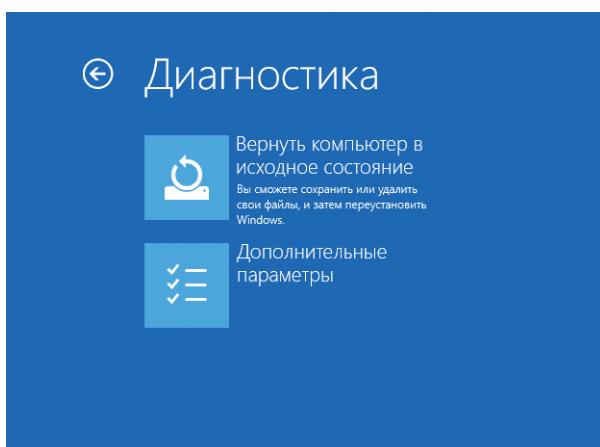


Рис. 9-1. При запуске устройства с Windows 10 с носителя среды восстановления выберите Поиск и устранение неисправностей (Troubleshoot), чтобы отобразить опции среды восстановления Windows

В Windows 8.1 и в ранних предварительных выпусках Windows 10 меню Диагностика (Troubleshoot) включало две опции Refresh и Reset. Сейчас они консолидированы в одну опцию Вернуть компьютер в исходное состояние (Reset This PC), которая активирует функцию сброса по кнопке. Она также доступна на странице Обновление и безопасность (Update & Security) в приложении Параметры (Settings) для работы с системами, которым удается правильно загрузиться. Мы рассмотрим ее далее в этой главе.

При выборе Дополнительные параметры (Advanced Options) будет открыто меню, похожее на представленное на рис. 9-2.

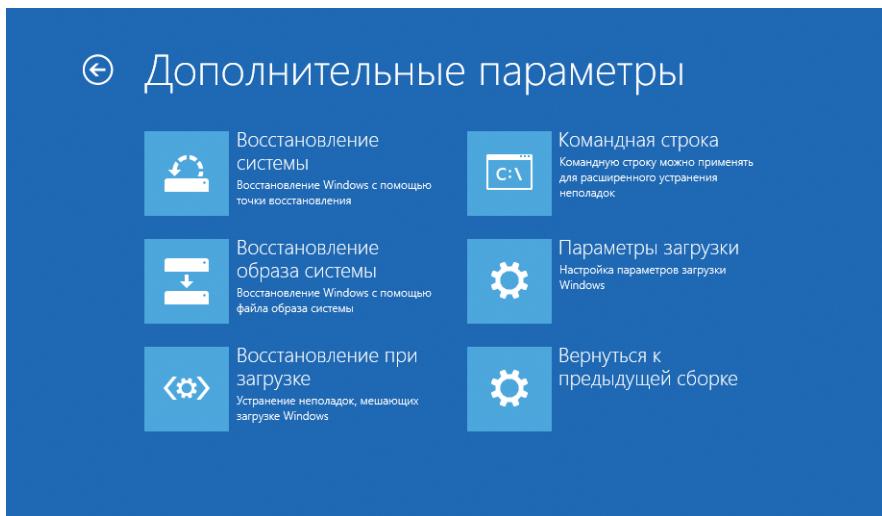


Рис. 9-2. Это меню Windows RE предоставляет доступ к ключевым инструментам устранения неполадок и восстановления

В табл. 9-1 перечисляются ключевые функции, доступные из меню Дополнительные параметры (Advanced Options). Многие из них являются наследниками инструментов восстановления из предыдущих версий Windows. На некоторых устройствах могут присутствовать дополнительные опции, например возможность доступа к настройкам прошивки UEFI, откат к предыдущей версии Windows или предварительной сборки.

Табл. 9-1. Дополнительные опции для восстановления

Опция	Описание
Восстановление системы (System Restore)	Эта опция позволяет выбрать точку восстановления, созданную ранее, и восстановить конфигурацию системы
Восстановление образа системы (System Image Recovery)	Эта опция позволяет заменить все на компьютере, используя образ системы, включая образы Windows 7 или позднее, созданные с помощью утилиты Архивация Windows (Windows Backup). (В Windows 10 эта утилита доступна в настольной Панели управления. В Система и безопасность [System & Security] нужно выбрать История файлов [File History] и щелкнуть на ссылке Резервная копия образа системы [System Image Backup] в нижнем левом углу.)

Опция	Описание
Восстановление при загрузке (Startup Repair)	При выборе этой опции Windows пытается диагностировать и автоматически исправлять типичные проблемы с загрузкой
Командная строка (Command Prompt)	Эта опция открывает командную строку администратора, в которой можно использовать такие инструменты командной строки, как Bootrec и Bcdedit



Дополнительная информация. Чтобы открыть опцию Параметры прошивки UEFI (UEFI Firmware Settings) через Windows RE на планшете с UEFI, выключите питание устройства, нажмите и удерживайте нажатой аппаратную кнопку уменьшения громкости и нажмите кнопку питания. Это единственный способ включить или отключить, например, защищенную загрузку.

Выберите Восстановление при загрузке (Startup Repair), чтобы вручную попробовать тот же набор исправлений, который Windows использует, когда обнаруживает сбой и автоматически запускает Windows RE. (Эта возможность ранее называлась Автоматическим восстановлением [Automatic Repair].) Функции Восстановление образа системы (System Image Recovery) требуется заранее сохраненный на внешнем устройстве хранения образ системы.



Дополнительная информация. За дополнительной информацией о восстановлении загрузки и восстановлении образа системы обратитесь к статье по адресу: <http://technet.microsoft.com/en-us/library/hh824837>. Она написана для Windows 8.1, но ее инструкции применимы и для Windows 10.

Среду восстановления Windows можно настраивать как часть стандартного образа. Например, можно добавить предпочтительный инструмент диагностики в меню Windows RE или назначить аппаратную кнопку для вызова Windows RE. Эти и другие практические пособия вы найдете в техническом справочнике Windows Recovery по адресу: <http://brt.ly/win-re-reference>.

Windows 10 и варианты сброса по нажатию кнопки

Революционное изменение, представленное в Windows 8, – это метод, который позволяет конечным пользователям восстановить чистую копию Windows без необходимости отдельного установочного носителя.

Когда компьютер постоянно испытывает проблемы, и стандартная диагностика не позволяет выявить причину, большинство IT-профессионалов стараются очистить компьютер и восстановить его из стандартного образа. Описываемые в этом разделе варианты сброса по нажатию кнопки позволяют достичь того же результата быстрее и без очистки потенциально важных данных. Windows 10 предлагает упрощенный вариант сброса, значительно усовершенствованный по сравнению с предшественниками.

На ПК с Windows 8 или более поздней версией, которые были собраны для розничных продаж и для каналов распространения, образ для восстановления по нажатию кнопки обычно содержиться в выделенном разделе в конце жесткого диска. Этот образ для восстановления может состоять из одного файла образа или из набора файлов образов, со сжатием или без. На ПК с Windows 8.1 можно освободить место, занимаемое этим разделом восстановления, но тогда пропадет возможность обновить или сбросить операционную систему.

В Windows 10 OEM-производители все еще могут предоставлять этот образ восстановления и связанный с ним раздел, чтобы компьютер можно было откатить к заводскому состоянию. Однако это больше не требуется. Вместо этого Windows 10 может выполнить полное восстановление путем пересборки операционной системы к чистому состоянию, используя существующие системные файлы из Windows Component Store (`C:\Windows\WinSxS`).



Дополнительная информация. На OEM-компьютере, который поставлялся с Windows 8 или Windows 8.1, при обновлении до Windows 10, существующий раздел восстановления остается не тронутым. (Это не относится к ПК с Windows 8.1, установленными с помощью WIMBoot.) Этот вариант может использоваться для восстановления изначально установленной операционной системы. Если пользователь считает, что старый раздел восстановления не нужен, то его можно удалить с помощью встроенных в Windows 10 инструментов, таких как консоль Управление дисками (Disk Management), утилита командной строки DiskPart и команды PowerShell.

Этот подход имеет несколько преимуществ.

- Значительно снижается объем дискового пространства, необходимого для чистой установки. Это особенно важно для планшетов и других устройств с небольшим объемом встроенного хранилища (32 ГБ или меньше).
- Сброс по нажатию кнопки доступен на всех ПК с Windows 10, а не только на OEM-компьютерах или корпоративных компьютерах с настроенным образом восстановления.
- Операционная система и драйверы восстанавливаются до самого последнего сводного состояния, со всеми обновлениями, кроме установленных в последние 28 дней. (Это современный эквивалент «последней удачной конфигурации», который позволяет восстановить последнюю рабочую конфигурацию, если источником проблем является недавно установленное обновление.) Напомним, что в Windows 8 и Windows 8.1 образ восстановления восстанавливает заводское состояние ПК. Такой откат потребует от пользователя загрузки всех обновлений, вышедших со времени заводской сборки компьютера.

Для OEM-компьютеров все измененные настройки и настольные программы, установленные производителем, восстанавливаются со сбросом Windows 10. Эти изменения сохраняются в отдельном контейнере, который создается в процессе OEM-установки. Все языковые пакеты, установленные в системе, восстанавливаются в момент инициации сброса по нажатию кнопки.

Настольные программы не восстанавливаются, их потребуется переустановить вручную. Все приложения Windows, включенные по умолчанию в Windows 10 (например, Погода, Музыка и Почта Outlook и Календарь), восстанавливаются вместе с приложениями, которые были добавлены в систему OEM-производителем или как часть корпоративного развертывания.

Обновления приложений после восстановления автоматически загружаются и переустанавливаются через Store. Все установленные пользователем приложения отклонаются, и их необходимо переустановить из Store.

Как упоминалось ранее, инициировать обновление или сброс можно из Windows RE или из приложения Параметры (Settings), как показано на рис. 9-3.

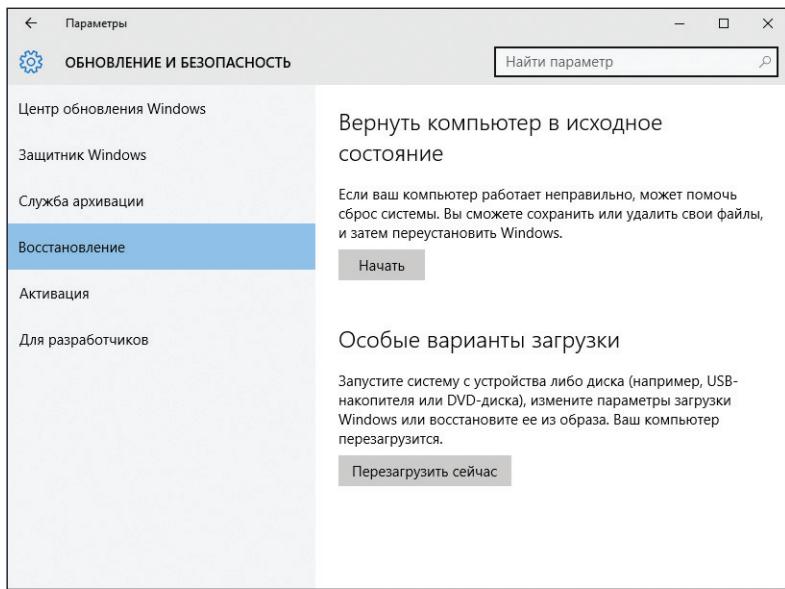


Рис. 9-3. Опции в этом меню варьируются. Например, на ПК, который был недавно обновлен с предыдущей версии, здесь находится опция отката к предыдущей версии

При выборе опции Вернуть компьютер в исходное состояние (Reset This PC) предлагаются две возможности, как показано на рис. 9-4.

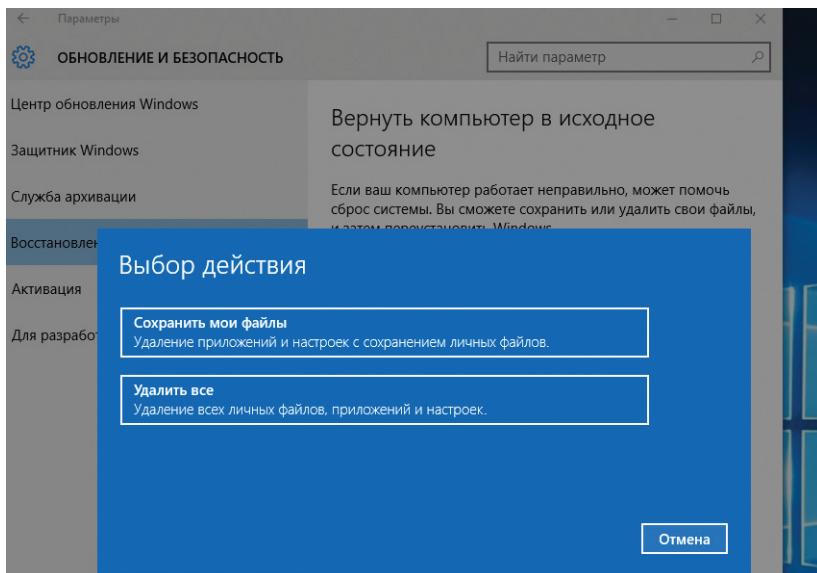


Рис. 9-4. Опция Вернуть компьютер в исходное состояние (Reset This PC) предлагает возможность сохранить файлы данных (и некоторые настройки) или начать все заново, удалив все файлы, приложения и настройки, т.е., по сути, выполнив чистую установку

Оба варианта эквиваленты переустановке Windows 10 с нуля, но с возможностью сохранить файлы и некоторые настройки или выполнить чистую установку.

Опция Сохранить мои файлы (Keep My Files)

Эта опция эквивалентна возможности Refresh Your PC из Windows 8.1, с тем важным исключением, что она не сохраняет приложения, приобретенные пользователем из Windows Store. (Их нужно переустановить после сброса.) При выборе опции Сохранить мои файлы (Keep My Files) сохраняются все файлы данных плюс следующие настройки персонализации.

- Учетные записи пользователей (локальные, домена и Microsoft) и членство в группах.
- Настройки домена.
- Настройки Windows Update.
- Настройки библиотеки.
- Фон экрана блокировки.
- Темы рабочего стола.
- Настройки интернационализации.
- Профили беспроводных сетей.
- Настройки окна входа в систему.

Файлы в профиле пользователя (за исключением тех, что находятся в папке AppData) сохраняются, как и любые папки, созданные в корне системного диска и на других разделах, а также данные истории файлов (File History). Все установленные пользователем настольные программы и приложения из Windows Store удаляются, а список удаленных программ сохраняется на рабочем столе.

Эта функция выполняет загрузку в Windows RE и собирает учетные записи пользователей, настройки, данные и приложения Windows Store. Затем она использует самую последнюю сводку системы, которая старше 28 дней, для создания новой чистой установки следующих папок со всеми подпапками:

- \Windows;
- \ProgramData;
- \Program Files;
- \Program Files (x86);
- %UserProfile%\AppData.

Операция сброса сохраняет драйверы устройств, следуя тем же правилам, что и для системных файлов.

Драйверы восстанавливаются к последней версии, которая старше 28 дней. Апплеты устройств, которые устанавливаются отдельно от пакета драйвера, не восстанавливаются в процессе сброса.

Предустановленные приложения Windows восстанавливаются к своим фабричным версиям и состоянию и будут обновлены по окончании сброса автоматически. Любые приложения и настройки, созданные как часть оригинального OEM-образа, восстанавливаются из контейнера настроек для этих изменений.

После перезагрузки сохраненные настройки, файлы данных и приложения применяются к новой операционной системе. Этот процесс может занять несколько минут.

Для использования опции Сохранить мои файлы (Keep My Files) требуется значительный объем свободного дискового пространства – как минимум 4 ГБ плюс двукратный объем места, занимаемого пакетами подготовки, расположеннымными в папке C:\Recovery\Customizations.

Опция Удалить все (Remove Everything)

Эта опция (ранее она называлась Reset Your PC в Windows 8.1) удаляет все приложения и пользовательские данные, включая учетные записи пользователей и настройки персонализации. Она полезна перед продажей или передачей компьютера новому сотруднику или за пределы организации.

Поскольку этот процесс приводит к потере данных, отображается несколько предупреждений с описанием того, что произойдет. Процесс сброса также включает опцию очистки данных с диска, чтобы затруднить их восстановление с помощью дисковых утилит. Как показано на рис. 9-5, работа опции Удаление файлов и очистка диска (Remove Files And Clean The Drive) может занять несколько часов. Эта опция обеспечивает хорошую защиту, но не сертифицирована для соответствия какому-либо стандарту правительства или индустрии для удаления данных.

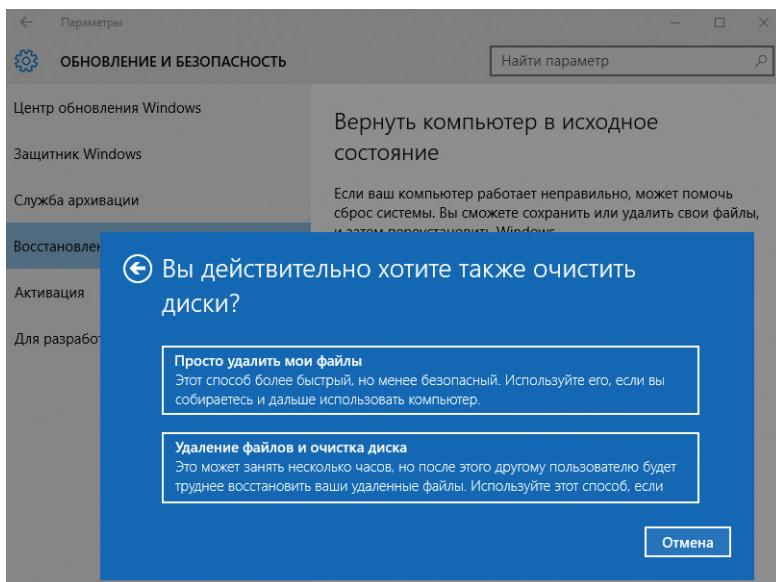


Рис. 9-5. Процедура Вернуть компьютер в исходное состояние (Reset This PC) включает опцию по очистке диска, чтобы затруднить восстановление файлов данных из предыдущей установки

В ходе сброса ПК загружается в Windows RE. Если система содержит несколько разделов, которые доступны пользователю (например, выделенный том с данными), то пользователю предоставляется возможность отформатировать весь диск или только раздел с Windows. Удаляются все учетные записи пользователей, файлы данных, настройки, приложения и любые изменения на разделе с Windows. Образ восстановления применяется к вновь отформатированному разделу с Windows, и на системном разделе создается новое хранилище Boot Configuration Data.

Когда система перезагружается, пользователь проходит через стандартные процедуры подготовки ПК и создания новой учетной записи пользователя. Этот процесс формально известен как «запуск при первом включении компьютера» (out-of-box experience, OOBE).

Опция восстановления не отменяет необходимость в носителе для восстановления, который понадобится в следующих сценариях.

- Если файлы операционной системы были значительно повреждены или заражены вредоносным ПО, процесс сброса, скорее всего, не сработает.
- Если имеется серьезная проблема в кумулятивном обновлении, которое старше 28 дней, сброс не позволит избежать этой проблемы.
- Если пользователь выбирает неправильный язык в ходе этапа OOBE на редакции с одним языком, может потребоваться полная переустановка.

Инструменты диагностики

Подобно предшественникам, Windows 10 включает широкий ассортимент инструментов диагностики и устранения неполадок для отслеживания причин, вызывающих проблемы с производительностью, сбоев и других нежелательных событий, особенно в ходе пилотного тестирования новой операционной системы.

Три утилиты в этом списке должны быть знакомы каждому IT-профессионалу.

- **Диспетчер задач** (Task Manager). Эта почтенная утилита Windows получала важные обновления, начиная с Windows 8, постепенно становясь все более функциональной. Она доступна из меню быстрых ссылок (щелкните правой кнопкой мыши на кнопке Пуск [Start] или воспользуйтесь комбинацией клавиш **[Windows] + [X]**) или комбинацией клавиш **[Ctrl] + [Shift] + [Esc]**. Вкладка Автозагрузка (Startup) предлагает информацию о программах, автоматически запускаемых с Windows. Вкладка Производительность (Performance), представленная на рис. 9-6, предлагает подробные сведения по нескольким подсистемам Windows. Обычно этой информации достаточно, чтобы понять причину медленной работы.
- **Монитор ресурсов** (Resource Monitor). Если деталей в диспетчере задач недостаточно, откройте эту утилиту, которая дает подробное представление об активности файловой системы и диска, использования процессора и сети.

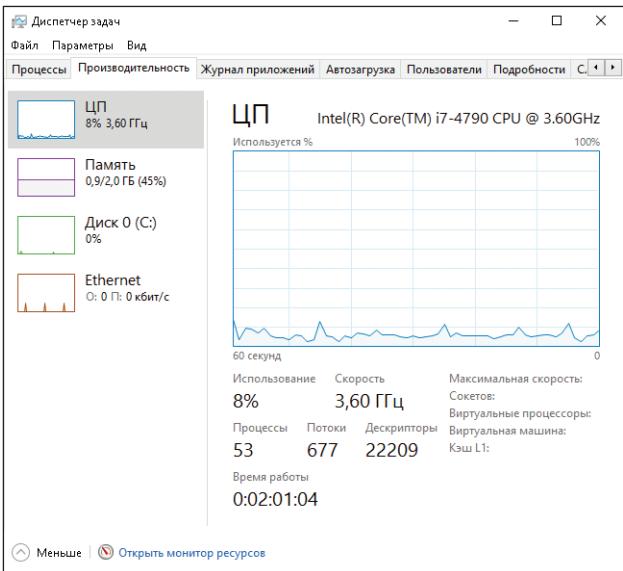


Рис. 9–6. Вкладка Производительность (Performance) в Диспетчере задач показывает массу информации по использованию ЦП, памяти, диска и сети. Обратите внимание на ссылку внизу, которая позволяет открыть Монитор ресурсов (Resource Monitor)

- **Просмотр событий** (Event Viewer). Практически все связанные с системой задачи, которые выполняет Windows в фоне, не в фоне или в ответ на действия пользователя, записываются в журнал событий доступны для анализа с помощью утилиты Просмотр событий (Event Viewer, Eventvwr.msc). Эта утилита практически не изменилась за последние десять лет.

Инструменты Sysinternals

Windows Sysinternals – один из самых постоянных и полезных источников продвинутых системных утилит для любого IT-профессионала. Сайт, доступный по адресу: <http://sysinternals.com>, был создан в 1996 году Марком Руссиновичем (Mark Russinovich), который присоединился к Microsoft в 2006 и сегодня является техническим директором Microsoft Azure.

Один только список утилит Sysinternals занял бы несколько страниц. Мы рассмотрим ключевые утилиты при диагностике проблем в незнакомой среде. Process Explorer предлагает доскональное представление текущих активных процессов, а AutoRuns дает контроль над программами, которые запускаются автоматически.

Примечательно, что эти инструменты регулярно обновляются, в основных выпусках добавляются новые возможности. Приятно, что они бесплатны.

В составе пакета Sysinternals Suite доступно почти 70 отдельных утилит диагностики Sysinternals. Можно загрузить и запустить отдельные инструменты с веб-сайта: <https://live.sysinternals.com/>.

Пакет Microsoft Diagnostics and Recovery Toolset

Пакет Diagnostics and Recovery Toolset (DaRT) является частью пакета Microsoft Desktop Optimization Pack (MDOP), который доступен по подписке для корпоративных клиентов с соглашением Software Assurance.

Он также доступен под другими лицензионными соглашениями через подписки Microsoft MSDN.

Каждая версия DaRT предназначена для конкретной версии Windows. Для Windows 10 это DaRT 10, которая включена в пакет MDOP 2015.

Dart предоставляет дополнительные опции восстановления и исправления, которых нет в Windows RE. DaRT поддерживает загрузку UEFI и может создавать образы Windows Imaging (.wim) или ISO-образы, которые могут развертываться с помощью USB-носителя. Используя DaRT, специалисты поддержки организации также могут удаленно подключаться к компьютеру для восстановления, без необходимости физически присутствовать за компьютером.

Стандартная установка Dart добавляет мастер Recovery Image Wizard, который позволяет создать образ для IT-профессионалов. С ним локальные пользователи могут выполнить ряд задач по восстановлению. Текущая версия пакета Dart включает Disk Commander для восстановления поврежденных разделов и томов дисков; Crash Analyzer анализирует файлы дампов; инструмент Hotfix Uninstall приходит на помощь, если установленное исправление вызывает проблемы на компьютере.

Некоторые организации могут развертывать DaRT как раздел восстановления по умолчанию в стандартных образах. В этом случае инструменты восстановления будут доступны все время, и съемный загрузочный носитель будет не нужен.

Интеграция с Azure Active Directory

Каждый сетевой администратор знает основы Active Directory, службы, которая работает на серверных редакциях Microsoft Windows и управляет бесконечным числом сетей на основе доменов по всему миру. Редакции Pro, Enterprise и Education Windows 10, конечно же, предлагают полную поддержку традиционных развертываний Active Directory, но Windows 10 также поддерживает новую облачную альтернативу, которая называется Azure Active Directory, или кратко Azure AD.

Подобно своему аналогу, Azure AD предоставляет службы идентификации и доступа для организаций. Используя рабочую или учебную учетную запись Azure AD, пользователи могут входить в любое облачное или локальное веб-приложение, используя широкий перечень клиентских устройств.

Azure AD предоставляет ключевые возможности идентификации и управления каталогами, стоящими за несколькими облачными бизнес-службами компании Microsoft, включая Microsoft Office 365 (естественно) Microsoft Azure. Службы Azure AD можно интегрировать с локальным развертыванием Active Directory или обойтись без интеграции. В любом случае имеется возможность сконфигурировать мультифакторную аутентификацию для защиты локального и удаленного доступа, а также использовать преимущества встроенных возможностей генерации отчетов и аналитики, которые масштабируются даже на очень большие организации.

В этой главе приводится обзор Azure AD и инструкции о том, как заставить Azure AD работать с устройствами с Windows 10 всех форм и размеров.

Знакомство с Azure AD

Читатель, возможно, уже использует Azure AD, даже не зная об этом. Если вы или ваша организация подписаны на облачную бизнес-службу Microsoft – такую, как Azure, Office 365, Microsoft Intune или Microsoft Dynamics Online, то эта подписка включает каталог Azure AD. По умолчанию этот каталог включает поддомен в домене onmicrosoft.com, но большинство организаций присваивают каталогу собственное доменное имя. Например, компания Contoso Corporation может начать с поддомена contoso.onmicrosoft.com, но добавить в качестве собственного домена contoso.com. Такая конфигурация позволяет пользователям входить в систему и обращаться к локальным или облачным ресурсам с помощью знакомого адреса электронной почты.

Каждый выделенный экземпляр Azure Active Directory (Azure AD) называется клиентом (tenant). Хотя компания Microsoft размещает службу в своей большой глобальной инфраструктуре Azure, каждый каталог Azure AD полностью изолирован от других каталогов, как показано на рис. 10-1.



Рис. 10-1. Все клиенты Azure Active Directory делят одну и ту же глобальную инфраструктуру, но каждый каталог полностью изолирован от других по соображениям безопасности.

Для удобства можно консолидировать несколько каталогов Azure AD на одной административной панели. Каталоги будут полностью разделены и защищены от неавторизованного доступа (случайного или злоумышленного).

Имеется возможность связать каталог Azure AD для существующей облачной службы Microsoft, такой как Office 365, с бесплатной подпиской Microsoft Azure, что позволит управлять этим каталогом на портале управления Azure (Azure Management Portal) (<https://manage.windowsazure.com>). На рис. 10-2 показана конфигурация каталога.

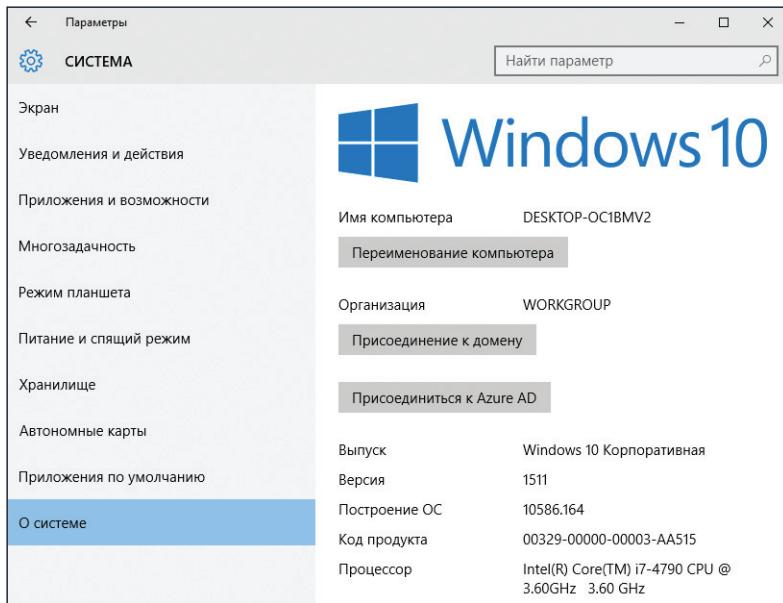


Рис. 10-2. Для конфигурации и расширения каталога Azure AD используйте этот портал управления

Подписки Azure AD доступны на трех уровнях. Подписка Office 365 или Azure включает каталог Azure AD на уровне Бесплатный (Free). Можно обновиться до редакций Базовый (Basic) и Премиум (Premium) через соглашение Microsoft Enterprise Agreement, через программу лицензирования Open Volume или через программу Cloud Solution Providers. Подписчики Azure и Office 365 могут также приобрести премиум-лицензии Active Directory онлайн.

Дополнительную информацию об уровнях подписки Azure AD вы найдете по адресу: <https://azure.microsoft.com/en-us/pricing/details/active-directory/>. Отличия перечислены ниже.

- **Бесплатный** (Free). Этот уровень позволяет использовать до 500 000 объектов каталога, поддерживает инструменты управления пользователями и группами и регистрации устройств, позволяет самостоятельно изменять пароли для облачных пользователей. Она также позволяет подключать до 10 приложений на пользователя в рамках единого входа (single sign-on, SSO) и поддерживает Active Directory Connect, механизм синхронизации для расширения локальных каталогов до Azure AD.
- **Базовый** (Basic). Помимо всех возможностей уровня Free, этот уровень убирает ограничение на число объектов в каталоге, позволяет сбрасывать пароли, добавляет управление доступом на уровне групп и включает соглашение об уровне обслуживания.
- **Премиум** (Premium). На этом уровне подписчики Azure AD имеют все преимущества уровня Базовый (Basic) плюс неограниченное число SSO-приложений, возможность использовать мультифакторную аутентификацию и улучшенные возможности управления паролями. Функция Cloud App Discovery позволяет сетевым администраторам определять, какие облачные службы (уполномоченные и неуполномоченные) используются в организации и, опционально, интегрировать их с Azure AD, чтобы уменьшить риски утечки данных.

Azure AD Premium также доступна как часть пакета Enterprise Mobility Suite, который включает Microsoft Intune и Azure Rights Management.

Azure Active Directory Join доступен только на устройствах Windows 10. На всех уровнях подписки, включая Free, можно подключить ПК с Windows 10 к Azure AD, использовать SSO-функции и восстанавливать ключи BitLocker с помощью администратора. На уровне Premium доступно самостоятельное восстановление ключа BitLocker, а дополнительные локальные учетные записи администраторов могут присоединять устройство Windows 10, используя Azure AD Join.

Возможность интеграции сторонних SaaS-приложений (software-as-a-service) с Azure AD – это ключевое преимущество. Сотни приложений доступны в Azure AD через Application Gallery и могут настраиваться одним щелчком кнопкой мыши. На рис. 10-3 показаны службы Amazon Web Services, интегрированные с Azure AD.

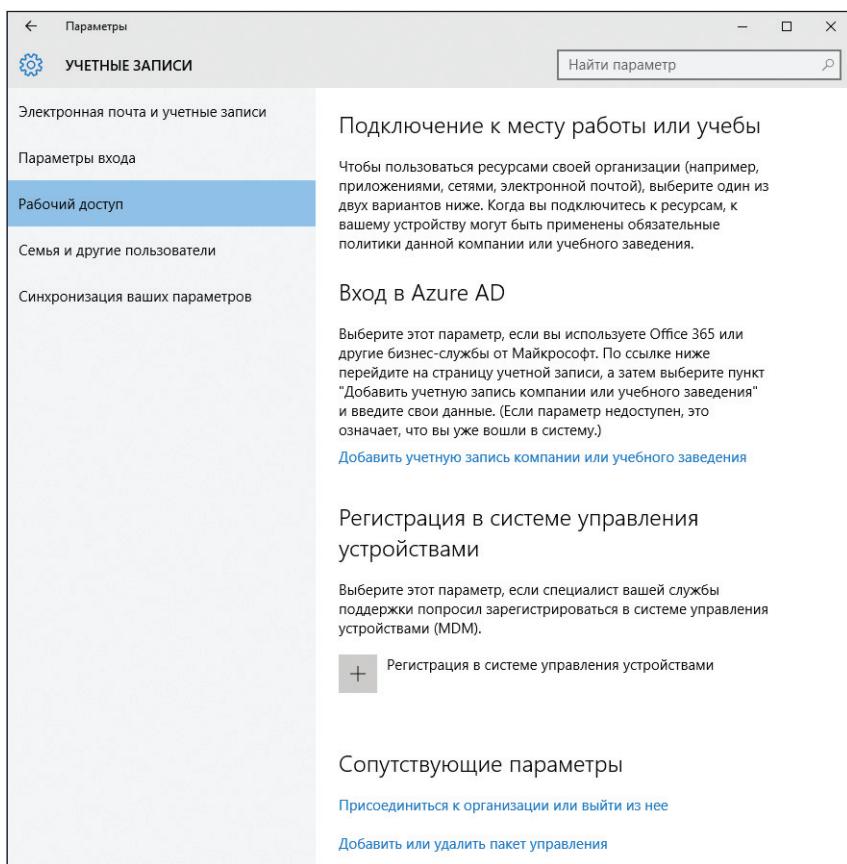


Рис. 10-3. Портал управления Azure позволяет интегрировать сторонние веб-приложения и онлайн-службы, а затем назначать их пользователям

Конфигурирование единого входа – весьма простая административная задача. Можно установить федерацию между двумя службами, если эта опция поддерживается, или хранить внешние

учетные данные для каждого пользователя прямо в Azure AD. Также можно подключаться к стороннему SSO-поставщику. На рис. 10-4 показаны эти опции на портале управления Azure.

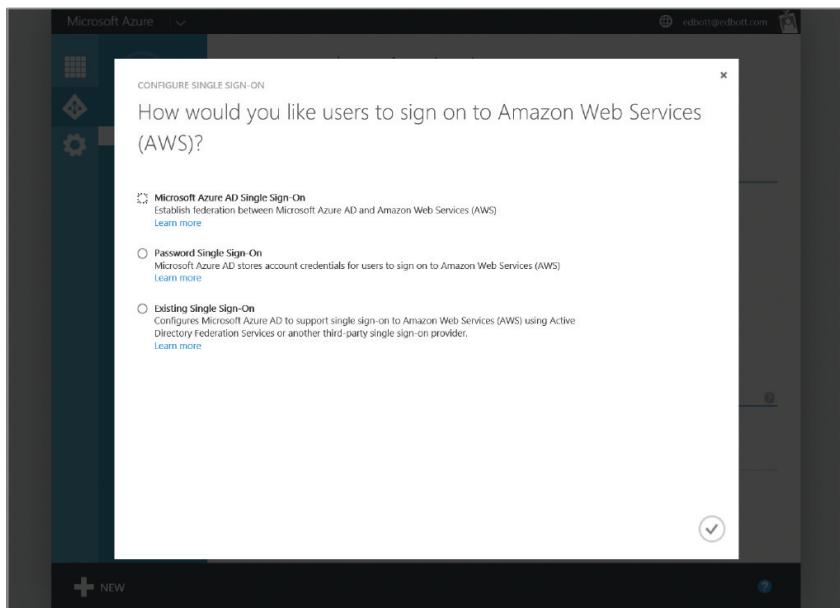


Рис. 10-4. Конфигурирование настроек единого входа выполняется для каждого приложения и доступно даже со службами-конкурентами других облачных продуктов Microsoft

Если нужно хранить данные учетных записей для пользователей как часть конфигурации SSO, то данные вводятся на портале управления Azure, как показано на рис. 10-5.

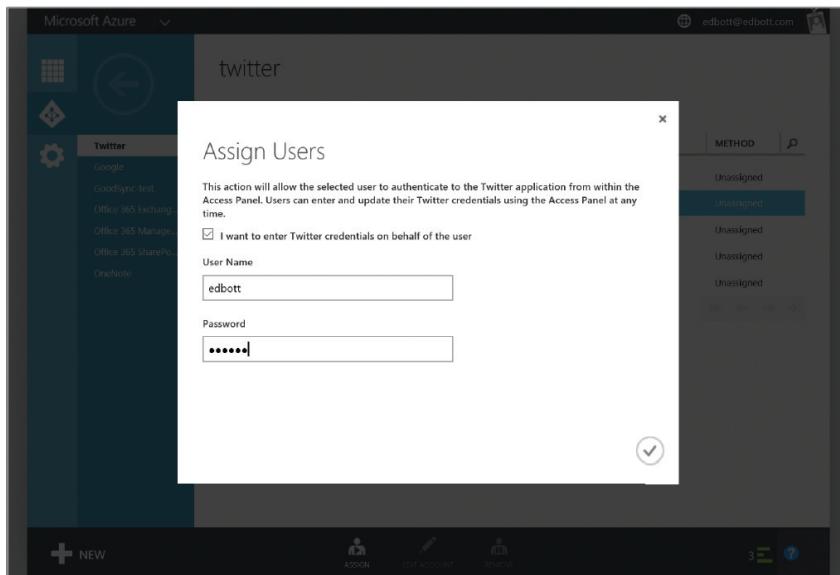


Рис. 10-5. После интеграции в Azure AD онлайн-службы, такой как Twitter, можно сохранять учетные данные для индивидуальных учетных записей пользователей. Эти пользователи затем смогут входить в Twitter прямо с панели доступа Azure AD

Даже на уровнях Free и Basic можно конфигурировать SSO и предоставлять пользователям доступ к неограниченному числу SaaS-приложений. Пользователи, однако, будут видеть в своей панели доступа только 10 приложений.

Подключение ПК с Windows 10 к Azure AD

Подключение устройства с Windows 10 к Azure AD выполняется аналогично подключению ПК с Windows 10 Pro или Enterprise к домену Active Directory. Этот вариант наиболее типичен в таких сценариях, когда устройство должно обращаться к локальным ресурсам и облачным службам, но подключать его к полноценному домену не хочется.

Лучше всего подключать ПК к Azure AD в ходе первоначальной настройки устройства с Windows 10. На рис. 10-6 показана страница, где пользователь начинает процесс и указывает, что настраивается ПК организации.

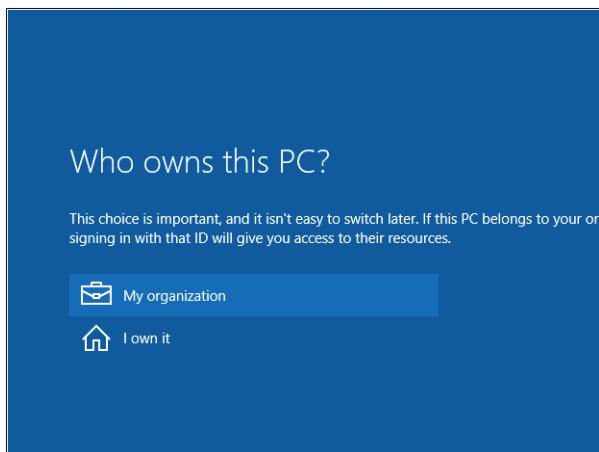


Рис. 10-6. Этот шаг выполняется на заключительных этапах настройки нового ПК с Windows 10 Pro

При выборе этого варианта отображается страница, представленная на рис. 10-7, где возможность подключения к Azure AD уже доступна. (Если выбрать опцию подключения к домену, то будет создана локальная учетная запись, которую затем понадобится подключить к домену.)

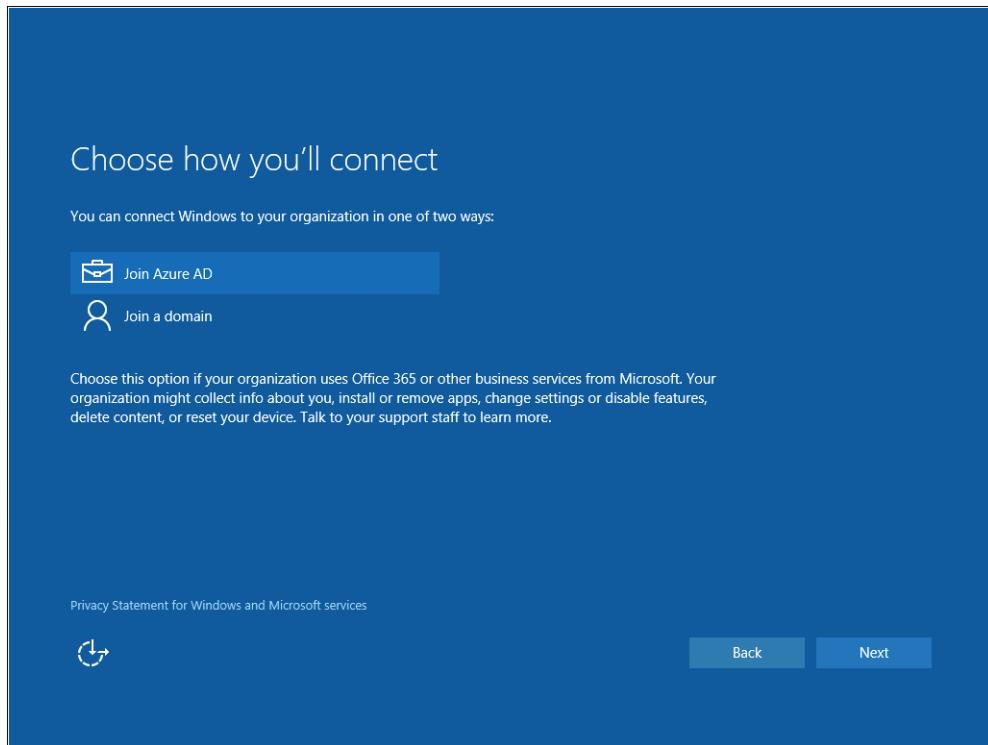


Рис. 10-7. При подготовке ПК для корпоративной сети можно использовать учетные данные Azure AD или подключиться к традиционному домену

После выбора этого варианта и ввода учетных данных Azure AD процесс варьируется в зависимости от настроек, заданных администратором Azure AD. Может потребоваться подтвердить свою личность, используя мультифакторную аутентификацию для регистрации устройства и задания PIN-кода для доступа. Также пользователям объясняется, что к этому устройству будут применяться политики компании.

На рис. 10-8 показана финальная часть процесса настройки, когда пользователь должен принять политики сервера.

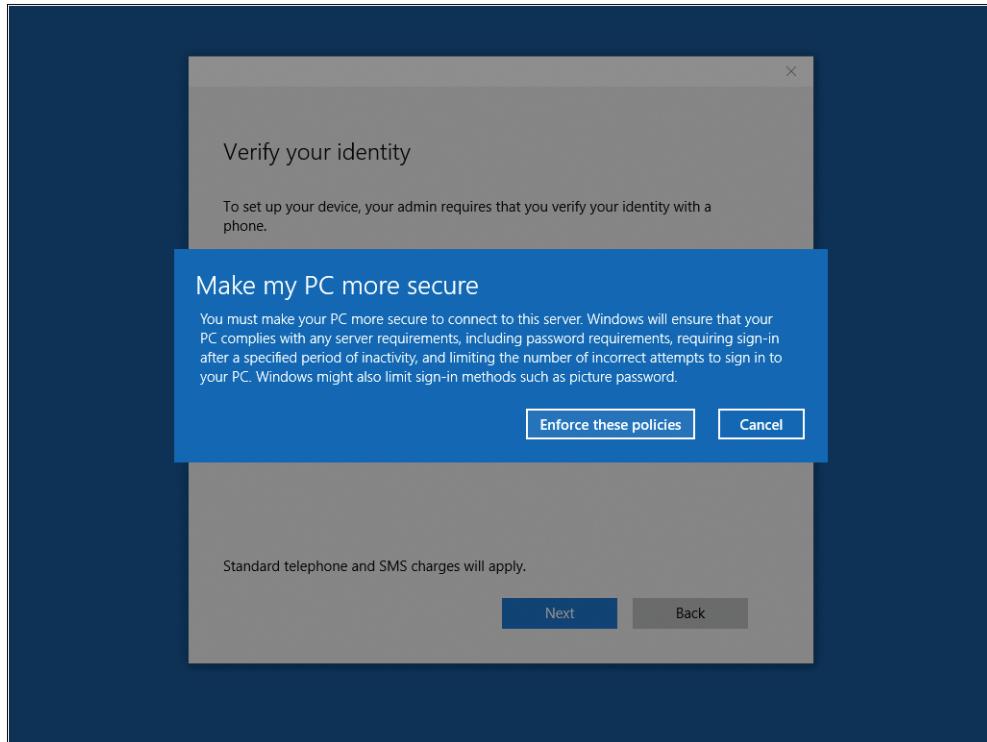


Рис. 10-8. Подключение ПК с Windows 10 к Azure AD означает, что политики компании смогут перекрывать некоторые стандартные настройки в Windows

После завершения процесса можно просмотреть текущую регистрацию на странице О системе (About) в приложении Параметры (Settings). Название организации определяется настройками организации в Azure AD, на странице также имеется кнопка для отключения от организации (которая также отключит доступ к облачным службам и ресурсам организации, связанными с этим ИД).

Эта же страница является отправной точкой, если нужно подключить к Azure AD ПК, на котором Windows уже настроена. На рис. 10-9 показано, где читатель найдет кнопку Присоединиться к Azure AD.

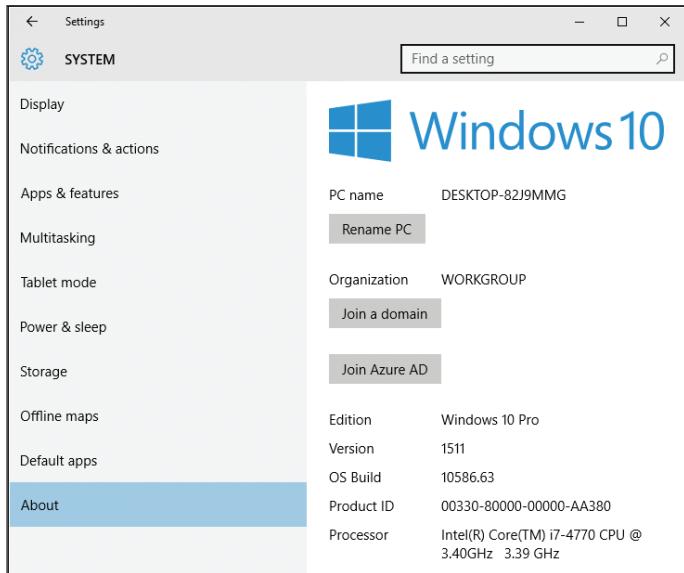


Рис. 10-9. Страница Система > О системе (System > About) в приложении Параметры (Settings) позволяет подключиться к Azure AD на системе, которая уже настроена с Windows 10

В любой момент пользователи могут обратиться к своим учетным записям Azure AD для изменения пароля или для SSO-доступа к приложениям. Чтобы найти эту ссылку, нужно выбрать учетную запись Azure AD внизу страницы Учетные записи (Accounts) в параметрах или открыть страницу управления учетными записями в веб-браузере по адресу: <https://account.activedirectory.windowsazure.com>. Эта страница показана на рис. 10-10. Все приложения, сконфигурированные для SSO, отображаются на странице Applications.

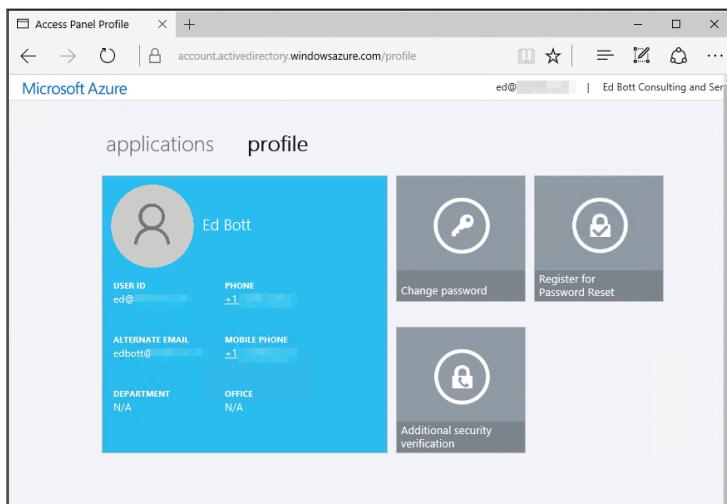


Рис. 10-10. Панель доступа Azure AD позволяет пользователям управлять информацией, изменять или сбрасывать пароли, а также обращаться к предварительно сконфигурированным приложениям

Добавление рабочих учетных записей в Windows 10

На персональных устройствах с Windows 10 подключение к Azure AD не всегда приемлемо, но можно получить некоторые преимущества Azure AD, добавив рабочую или учебную учетную запись с учетными данными Azure AD. Этот шаг позволит входить в Office 365 автоматически и использовать панель доступа Azure AD.

Процесс прост. Нужно начать со страницы Учетные записи (Accounts) в приложении Параметры (Settings), а затем открыть Рабочий доступ (Work Access), чтобы отобразить опции, представленные на рис. 10-11.

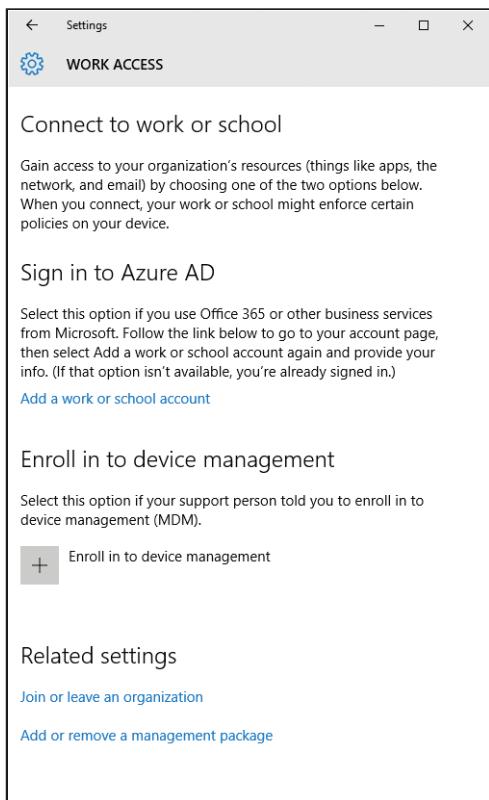


Рис. 10-11. Добавление рабочей или учебной учетной записи позволяет подключаться к Office 365 и другим службам на не полностью управляемом устройстве

Универсальные приложения и новый Windows Store

Фундаментальная разделительная линия между Microsoft Windows 7 и последующими версиями – это возможность более новых выпусков Windows выполнять новый класс приложений, неформально известных как современные (modern) приложения, а формально – доверенные приложения Windows Store (Trusted Windows Store). Конечно, Windows 10 все еще может выполнять практически все классические настольные программы Windows; новые приложения добавляют другой набор опций. Поскольку они оптимизированы для сенсорного и мобильного использования, их легче использовать на планшетах и гибридных мобильных устройствах. И, поскольку они распространяются через Windows Store, они безопаснее и легче в развертывании.

В этой главе предлагается обзор доверенных приложений и нового Store, универсального для всех редакций Windows 10, и нового набора возможностей Windows Store для бизнеса (Windows Store for Business).

Универсальная платформа Windows

Приложения, разработанные для Windows 8 и 8.1, выполняются только в полноэкранном режиме или будучи прикрепленными к краю экрана. В Windows 10 каждое современное приложение, включая встроенные приложения Параметры (Settings) и Microsoft Edge, могут выполняться в своем собственном окне или прикрепляться к панели задач. Такое изменение в поведении – одно из преимуществ новых приложений в сравнении с их классическими настольными аналогами.

Первое поколение современных приложений, создаваемых для Windows 8, использовало архитектуру приложений Windows Runtime (WinRT). С выпуском Windows 8.1 эта платформа была расширена до Windows Phone 8.1, что позволило разработчикам создавать универсальные приложения Windows 8, которые хоть и были раздельными, но имели большую часть общего кода.

С Windows 10 Microsoft представила универсальную платформу Windows (Universal Windows Platform, UWP), значительно усовершенствованного потомка WinRT, который предоставляет универсальную платформу приложений для каждого устройства Windows 10. Приложения, создаваемые с помощью UWP, не просто делят общий код; они выполняют

один и тот же код на разных семействах устройств. Имеется несколько универсальных прикладных интерфейсов программирования (API), доступных на всех семействах устройств. Дочерние семейства устройств имеют свои собственные API-интерфейсы в добавление к универсальным API-интерфейсам устройств. Руководство по UWP-приложениям, опубликованное в центре разработчиков Windows (<http://bit.ly/uwpg-guide>), предназначено в первую очередь для разработчиков Windows 10, но может служить замечательным обзором и для IT-профессионалов.

Как отмечают авторы этого руководства, добавление UWP в унифицированное ядро Windows 10 стало ключевым преимуществом современных приложений.

Будучи частью ядра, UWP теперь обеспечивает универсальную прикладную платформу, доступную на каждом устройстве с Windows 10. Благодаря такой эволюции UWP-приложения могут вызывать не только WinRTAPI, типичное для всех устройств, но и другие API-интерфейсы (включая Win32 и .NETAPI), специфичные для того семейства устройств, на котором работает приложение. UWP обеспечивает гарантированный API-слой ядра на всех устройствах. Это означает, что разработчики могут создать единый пакет приложения для установки на широком классе устройств.

Используя UWP, разработчики могут создавать гораздо более мощные приложения, чем раньше. Эти приложения могут быть ориентированы на конкретное устройство или на все семейство устройств, от телефонов и маленьких планшетов до ПК и игровых консолей Xbox One, а также других нетрадиционных устройств, которые обычно называют Интернетом вещей (Internet of Things, IoT), на которых работают редакции Windows 10 IoT.



Примечание. За дополнительными деталями о семействе Windows 10 IoT обратитесь по адресу: <https://www.microsoft.com/en-us/WindowsForBusiness/windows-iot>.

Что еще важнее, Windows 10 позволяет доставлять приложения на все устройства через единый магазин. IT-профессионалам, внимание которых сфокусировано главным образом на развертывании, управлении и защите корпоративных приложений, безусловно будет интересен Windows Store for Business, новое дополнение в Windows 10 версии 1511, которое может быть расширено для доставки универсальных приложений Windows и традиционных настольных приложений в управляемой среде через защищенные бизнес-порталы.

Знакомство с новым Windows Store

Внешне Store в Windows 10 и Store в Windows 8.1 похожи, но если приглядеться, то можно выявить большие изменения.

Новый Store (который сам по себе является UWP-приложением) предлагает не только приложения, – здесь доступны также игры, фильмы, ТВ-передачи и музыка, которые можно приобрести или взять в аренду. Единое поле поиска позволяет искать объекты в одной категории или по всему магазину, как показано на рис. 11-1 (имеется возможность уточнить критерии поиска).

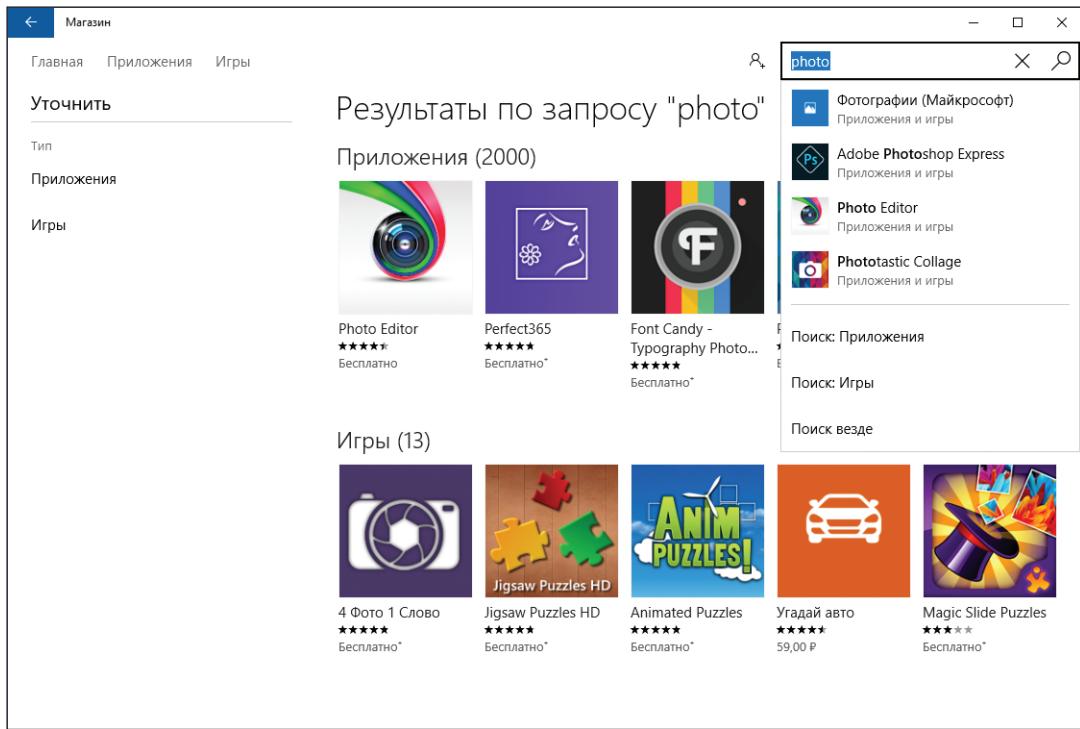


Рис. 11-1. Store в Windows 10 предлагает замечательные возможности поиска и доступ не только к приложениям

Новый Store также включает подробную сводку ранее установленных приложений с возможностью их автоматического обновления в фоне. Если выполнен вход в Store, то пользователь может проверить текущий статус загрузок и установок приложений, приостановить, возобновить или отменить загрузки. На рис. 11-2 показано, как работает эта возможность.

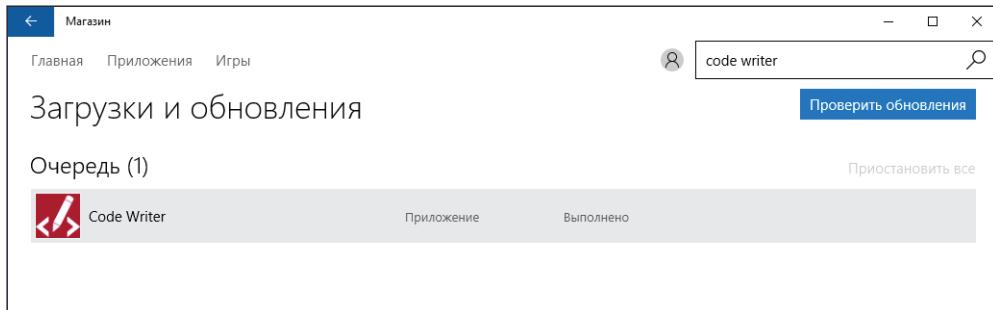


Рис. 11-2. Щелчок на изображении пользователя (слева от поля поиска) открывает меню с командами для доступа к настройкам и опциям учетной записи. Эта страница позволяет управлять текущими загрузками и обновлениями приложений

Для управления устройствами, связанными с учетной записью Microsoft, войдите в <https://account.microsoft.com> и откройте вкладку Устройства (Devices). Можно просмотреть все устрой-

ства, с которых был выполнен вход в текущую учетную запись Microsoft, можно просмотреть детали об устройстве и его операционной системе, как показано на рис. 11-3.

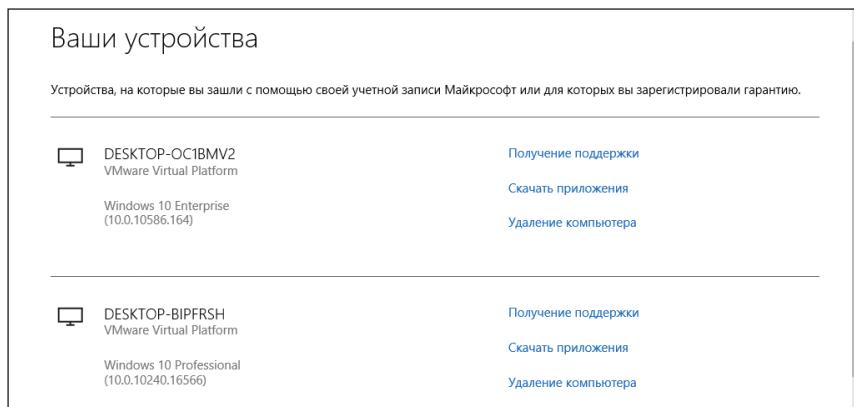


Рис. 11-3. На вкладке Устройства (Devices) страницы управления учетной записью Microsoft перечислены все устройства, связанные с конкретным ID. Поддерживаются ПК, ноутбуки, планшеты и телефоны

Для планшетов Surface в этом списке показываются статус гарантии и ссылки для поддержки.

Приложения, приобретенные в Windows 10 Store (бесплатные и платные), могут устанавливаться на 10 устройствах.

Отдельный список устройств, связанных с учетной записью Store, также доступен со страницы учетной записи Microsoft. Здесь можно удалить приложение, если его нужно освободить для последующей установки на новом устройстве. На рис. 11-4 показано, как работает эта возможность.

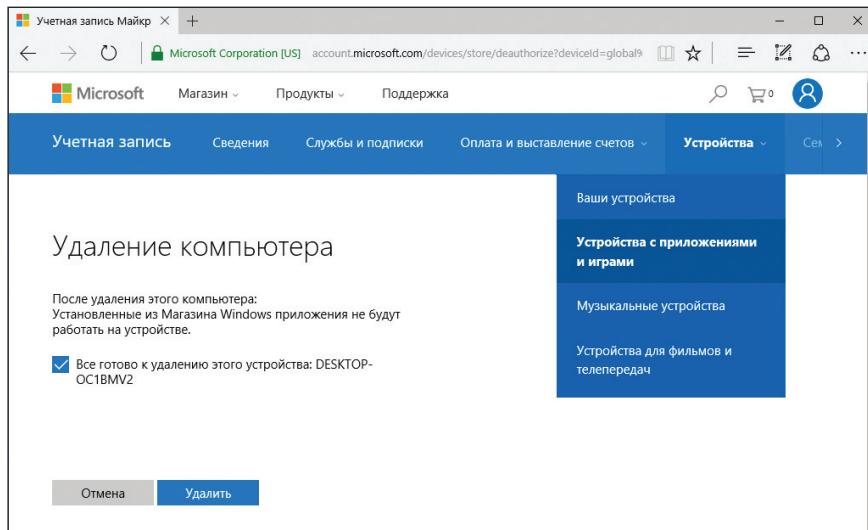


Рис. 11-4. В Windows 10 приложения могут устанавливаться максимум на 10 устройствах. Эта страница позволяет удалить устройство из списка авторизованных для установки приложений из связанной учетной записи Microsoft

Для простых потребителей и пользователей Windows 10 из малого бизнеса публичный Windows Store - это главное место приобретения приложений через учетную запись Microsoft. Имеются разные варианты оплаты. С новым Store в Windows 10 корпоративные возможности гораздо шире.

Однако, прежде чем переходить к этой теме, посмотрим на новые UWP-приложения в действии.

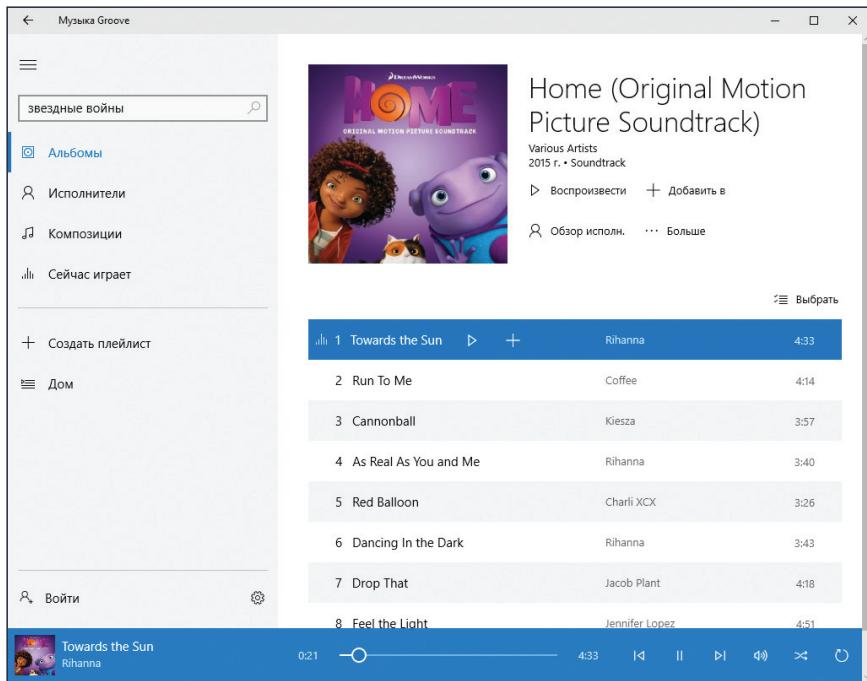
Как работают UWP-приложения

Следующие характеристики UWP-приложений в Windows 10 совпадают с характеристиками первого поколения современных приложений, написанных для Windows 8 и Windows 8.1.

- Приложения устанавливаются для каждого пользователя отдельно. Простой механизм установки не требует прав локального администратора.
- Сторонние приложения легко удалять, за исключением ряда предустановленных приложений (они также называются подготовленными [provisioned] приложениями), которые удаляются только командами Windows PowerShell.
- Каждое приложение имеет свою плитку, которая может быть запрограммирована на динамическое обновление, что делает ее «живой». Приложения могут вызывать уведомления, используя стандартные API-интерфейсы. Каждый пользователь управляет отображением информации в живых плитках и может отключать оповещения и уведомления глобально или для конкретного приложения.
- Приложения должны соответствовать строгому набору API-интерфейсов, которые не дают напрямую обращаться к системным ресурсам. Это ограничивает возможность приложений выполнять многие функции, которые типичны для настольных приложений. Эти ограничения повышают безопасность и надежность, поскольку блокируют наиболее распространенные векторы атак.

Поскольку UWP-приложения могут выполняться на разных размерах и ориентациях экрана, при взаимодействии с пользователем они адаптируются к масшабируемым макетам экрана и элементам управления. Это преимущество наиболее очевидно на телефонах и маленьких планшетах, но изменение можно увидеть и на традиционном ПК с Windows 10, если изменить размер окна.

Посмотрите на работу приложения Музыка Groove (Groove Music), которое включено во все редакции Windows 10, за исключением Ветви долгосрочного обслуживания (Long-Term Servicing Branch). На рис. 11-5 окно достаточно широкое, чтобы отобразить область навигации слева и полную информацию по текущему альбому справа.



При уменьшении ширины окна область навигации сначала уменьшается до столбца со значками, а затем полностью исчезает, чтобы оставить больше места под полезную информацию, как показано на рис. 11-6.

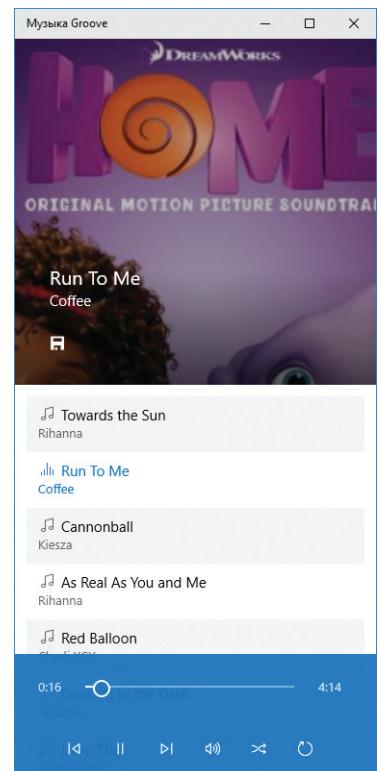


Рис. 11-6. UWP-приложения, такие как Groove Music, адаптируются под меньший размер окна или экрана, скрывая элементы управления навигацией

Рис. 11-5. Адаптивное взаимодействие с пользователем в Windows 10 позволяет UWP-приложению Музыка Groove (Groove Music) показывать больше информации, если экран позволяет

Все редакции Windows 10 включают подборку универсальных приложений компании Microsoft, которые следуют этим принципам: Калькулятор (Calculator), Будильники и часы (Alarms & Clock), Новости (News), Спорт (Sports), Деньги (Money) и Погода (Weather).

При развертывании Windows 10 вам может потребоваться удалить одно или несколько из этих подготовленных приложений либо вручную, либо в ходе подготовки образа системы для развертывания. Один из методов – использовать команды PowerShell (командлеты Get-AppxPackage и Remove-AppxPackage) с инструментами развертывания. Бэн Хантер (Ben Hunter) из компании Microsoft задокументировал этот процесс в статье, которую он написал для Windows 8.1, но она подходит и для Windows 10: <http://bit.ly/remove-built-in-Windows-apps>. Обновленная версия сценария автора Майкла Ниехауса (Michael Niehaus) может динамически определять список приложений, которые можно удалить. Эта статья доступна по адресу: <http://bit.ly/remove-windows-10-apps>.

Новая возможность, которая появилась в Windows 10 версии 1511, автоматически устанавливает некоторые игры и приложения из Windows Store для вошедшего в систему пользователя. Эти приложения варьируются в зависимости от региона и нацелены, главным образом, на простых потребителей. Чтобы запретить их установку, нужно включить настройку групповой политики Выключить возможности потребителя Microsoft (Turn Off Microsoft Consumer Experience), расположенную по пути Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Содержимое облака (Computer Configuration > Administrative Templates > Windows Component > Cloud Content), как показано на рис. 11-7.

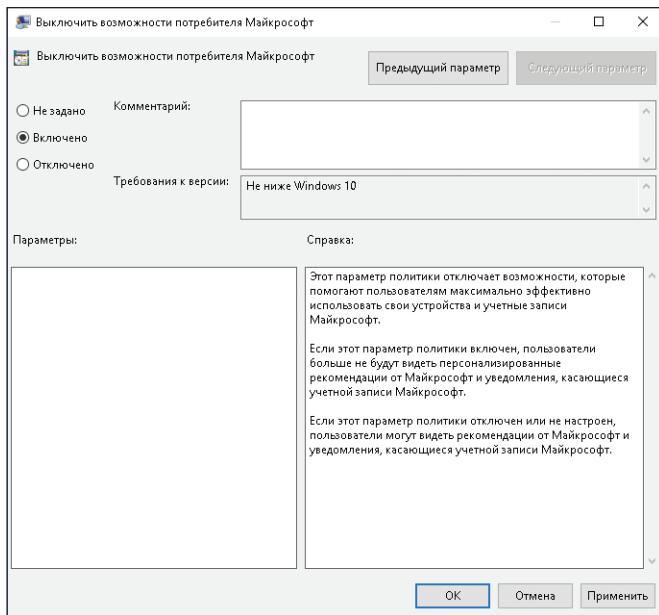


Рис. 11-7. Включите эту настройку в групповой политике, чтобы запретить установку игр на компьютерах пользователей

Универсальные приложения используют общую группу пользовательских элементов управления, которые также адаптивны и предлагают большие или меньшие области для сенсорного взаимодействия в зависимости от доступного размера.

Ради экономии электроэнергии (ключевой фактор на мобильных устройствах) большинство приложений Windows Store приостанавливаются в течение нескольких секунд после того, как пользователь переключается к другому приложению. Некоторые приложения (например, музыкальные проигрыватели и приложения, которым нужно загружать файлы в фоне) могут настраиваться на работу в фоне.

Универсальные приложения Windows 10 включают поддержку естественного ввода пользователя: речь, рукописный ввод, жесты и даже взгляд.

По умолчанию приложения в Windows 10 обновляются автоматически, не требуя взаимодействия с пользователем. Опция автоматического обновления может быть отключена в настройках обновления страницы Параметры (Settings) в Store. В управляемых средах для отключения доступа к приложению Store может использоваться групповая политика.

Использование Windows Store для бизнеса

Организации, использующие Windows 10, могут разрабатывать универсальные бизнес-приложения и предоставлять их пользователям внутри организации. Они также могут приобретать лицензии для приложений Windows 10 и позволять сотрудникам устанавливать эти приложения без запроса учетной записи Microsoft. Эти приложения могут развертываться через приватный магазин, при этом они управляются и развертываются через Windows Store, или через процесс загрузки неопубликованных приложений (sideloading).

Windows Store для бизнеса дебютировал в Windows 10 версии 1511. Организации с инфраструктурой Azure Active Directory могут использовать эту возможность, чтобы разрешить пользователям входить со своими учетными записями Azure AD и просматривать, загружать и устанавливать приложения. Управлением и отслеживанием лицензий занимается Windows Store для бизнеса.

Чтобы начать создание собственного Windows Store для бизнеса, войдите в <http://businessstore.microsoft.com> с учетными данными администратора Azure AD. На рис. 11-8 представлена страница управления для магазина с набором приложений, доступных для организации.

The screenshot shows the Windows Store for Business interface. At the top, there's a navigation bar with links for 'Windows Store for Business', 'Shop', 'Manage', 'Settings', and 'Support'. A search bar and a user account dropdown are also present. The main area is titled 'Inventory' and contains a table of application details. The columns are 'Product', 'Actions', and 'Last modified'. The table lists five applications: PowerPoint Mobile, Onefootball, OneNote, Word Mobile, and another instance of PowerPoint Mobile. To the right of the table is a sidebar titled 'Refined by: Offline' with a 'Clear' button. It includes checkboxes for 'License type' (Offline), 'Source' (Store), 'Private store', 'In private store', 'Not in private store', 'Add in progress', and 'Remove in progress'. A note at the bottom right of the sidebar says 'Not applicable'.

Рис. 11-8. Windows Store для бизнеса выглядит и ведет себя аналогично публичному Store, но ограничен только членами вашей организации, которые выполнили вход с учетной записью Azure AD

Администраторы могут добавлять приложения в закрытый магазин. Эти приложения отображаются как вкладка в Windows Store для бизнеса для членов организации Azure AD. В закрытый магазин добавляются только приложения с онлайн-лицензиями либо в момент их приобретения администратором, либо позднее из хранилища. Когда приложение добавлено в закрытый магазин, сотрудники могут затребовать и установить его.

На рис. 11-9 представлено добавление приложения в хранилище в закрытом магазине.

The screenshot shows the 'App details' page for the 'Translator' app. The app has a rating of 4 stars and 1170 reviews. It is categorized as 'Travel' and is available for PC and mobile devices. The 'Distribute' dialog box is open, asking if the app should be added to the private store or assigned to people. The 'Add to your private store where all people in your organization can find and install it' option is selected. Buttons for 'Confirm' and 'Cancel' are visible. Below the dialog, the app's details are listed: Category (Travel), Approximate size (13.59 MB - 72.71 MB), Age rating (For ages 12 and up), Supported processors (x64, x86, arm, neutral), and Supported languages (English (United States), Portuguese (Brazil), Italiano (Italy), Deutsch (Deutschland), Français (France)).

Рис. 11-9. Администратор Windows Store для бизнеса может выбирать приложения из публичного Store и делать их доступными для членов организации

Обновления доставляются через обычные каналы – Windows Update или Windows Server Update Services (WSUS).

Бизнес-приложения могут распространяться в организации с помощью ПО управления мобильными устройствами (MDM) или инструментов развертывания, таких как диспетчер System Center Configuration Manager или Microsoft Deployment Toolkit, без подключения к Windows Store. Этот процесс, называемый загрузкой неопубликованных приложений (*sideloading*), не требует от приложений подписи корпорации Microsoft и учетных записей Azure AD. Однако приложения должны быть подписаны с помощью сертификата, выданного одним из доверенных корневых центров сертификации на этой системе.

В таком сценарии установочные файлы загружаются и развертываются с помощью собственной инфраструктуры организации. Приложения могут устанавливаться как часть собственного установочного образа или индивидуально с помощью инструментов развертывания или MDM.

Эта новая возможность сейчас активно развивается. Дополнительную информацию об одном из сценариев вы найдете в статье по адресу: <http://bit.ly/Windows-Store-for-Business-with-MDT2013>.

Хранилище

Что остается неизменным в каждой версии Microsoft Windows, начиная с самых первых?

Встроенное хранилище для хранения операционной системы, настроек, приложений, файлов данных и цифровых мультимедиа-данных. Но детали подсистем хранения за эти годы разительно изменились.

Всего несколько лет назад, например, твердотельные накопители (solid-state drive, SSD) были роскошью, доступной только самым дорогим системам. Сегодня цены на SSD снизились, флэш-накопители стали принадлежностью дешевых устройств, а традиционные жесткие диски зачастую используются как вспомогательный накопитель для хранения больших объемом данных или ускоряются с помощью SSD-кэша.

В то же время переход на твердотельные накопители на портативных устройствах приводит к значительному уменьшению среднего размера диска. Производители некоторых портативных ПК в начале 2016 года предлагают на выбор SSD (обычно размером в 128 ГБ) или гораздо больший по размеру традиционный жесткий диск. Перед покупателями стоит выбор между быстрым, но ограниченным хранилищем, и большими по размеру, но более медленными и менее надежными дисками.

Годами производители ПК стабильно увеличивали размер основного системного диска. Но с началом эры SSD тренд повернулся в обратном направлении. Для планшетов и недорогих портативных компьютеров основной системный диск стал крошечным. Здесь приходится использовать режим Compact OS, позволяющий Windows 10 работать с основными устройствами хранения, размер которых слишком мал для того, чтобы предыдущие версии Windows могли комфортно работать на них.

DVD-приводы постепенно вымирают. Теперь, благодаря стандарту USB, чаще встречаются съемные приводы самых разных форм и размеров.

В этой главе приводится общий обзор вариантов хранения, доступных для устройств с Windows 10, начиная с инструментов для управления встроенными и съемными накопителями.

Инструменты управления хранилищем

В распоряжении IT-профессионала, оценивающего Windows 10, имеется ряд инструментов для анализа, конфигурирования, управления и диагностики устройств хранения. Некоторые из них знакомы даже самим древним пользователям Windows. Другие появились

только в Windows 10, подтверждая медленный, но постоянный перевод ключевых функций на современный пользовательский интерфейс Windows 10.

Управление дисками

Самый важный инструмент управления дисками, – это консоль Управление дисками (Disk Management), Diskmgmt.msc, представленная на рис. 12-1. Самый быстрый способ открыть эту консоль – щелкнуть правой кнопкой мыши на кнопке Пуск (Start) или нажать комбинацию клавиш [Windows] + [X], чтобы открыть меню быстрых ссылок, а затем выбрать команду Управление дисками (Disk Management).

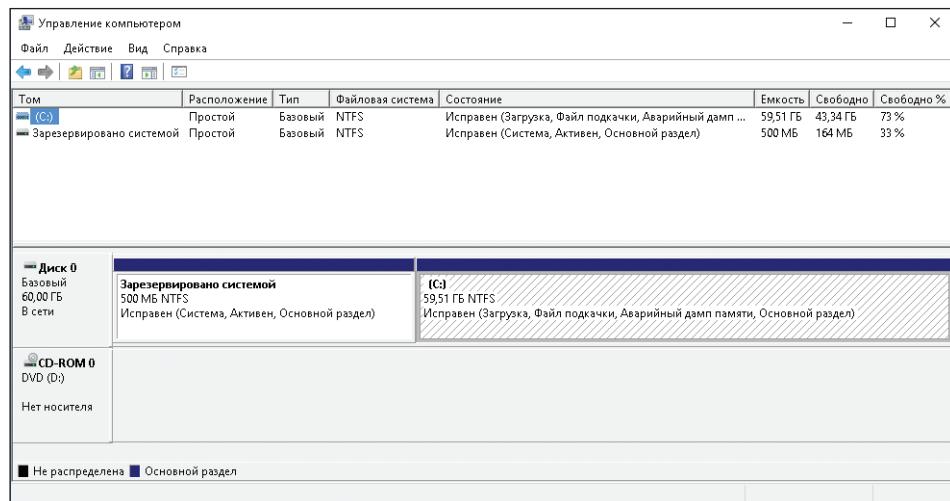


Рис. 12-1. Консоль Управление дисками (Disk Management) знакома даже седьмым IT-профессионалам

DiskPart

Более продвинутая утилита управления дисками – DiskPart. Как показано на рис. 12-2, она запускается в окне командной строки с повышенными привилегиями, в своей собственной управляемой командной строке, и позволяет перечислять, выбирать и управлять дисками, томами и другими объектами хранилища.

```
Administrator: Командная строка - diskpart
Microsoft Windows [Version 10.0.10586]
(c) Корпорация Майкрософт (Microsoft Corporation), 2015. Все права защищены.

C:\Windows\system32>diskpart

Microsoft DiskPart версии 10.0.10586

(С) Корпорация Майкрософт (Microsoft Corporation), 1999-2013.
На компьютере: DESKTOP-OC1BMV2

DISKPART> list disk

Диск ### Состояние Размер Свободно Дин ГРТ
----- -----
Диск 0 В сети 60 Гбайт 0 байт

DISKPART> sel disk 0

Выбран диск 0.

DISKPART> detail

Microsoft DiskPart версии 10.0.10586

DISK      - Отображение свойств выбранного диска.
PARTITION - Отображение свойств выбранного раздела.
VOLUME   - Отображение свойств выбранного тома.
VDISK    - Отображение свойств выбранного виртуального диска.

DISKPART>
```

Рис. 12-2. Чтобы просмотреть полный список команд DiskPart, введите Help. Введите любую команду без аргументов, чтобы увидеть синтаксис этой команды

Одна из самых полезных команд DiskPart – это Clean, которая немедленно убирает все форматирование разделов или томов с выбранного в данный момент диска. Эта команда записывает ноль в каждый байт и каждый сектор диска, что полностью удаляет все данные на диске и очищает все форматирование диска. (Технически, используя специальные технологии, можно восстановить данные с диска, который был очищен таким образом, но это потребует огромных усилий.)

Storage Sense

Экран Storage Sense – новинка Windows 10 (выберите Параметры [Settings], а затем Хранилище [Storage] в категории Система [System]). Как показано на рис. 12-3, сначала перечисляются доступные фиксированные накопители с графическим отображением используемого и свободного пространства, затем – используемые по умолчанию места для стандартных папок с данными.

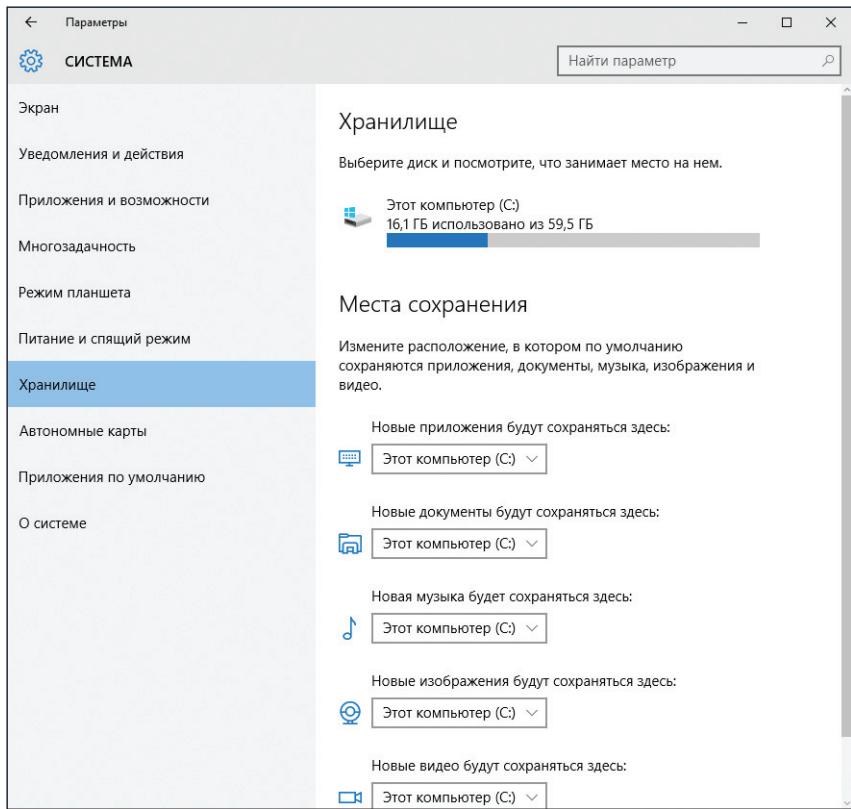


Рис. 12-3. Интерфейс Хранилище (Storage) предлагает обзор доступных накопителей и позволяет изменить расположение стандартных папок с данными

Если щелкнуть на элементе диска в панели Хранилище (Storage), будет отображен список используемого места по категориям файлов, как показано на рис. 12-4.

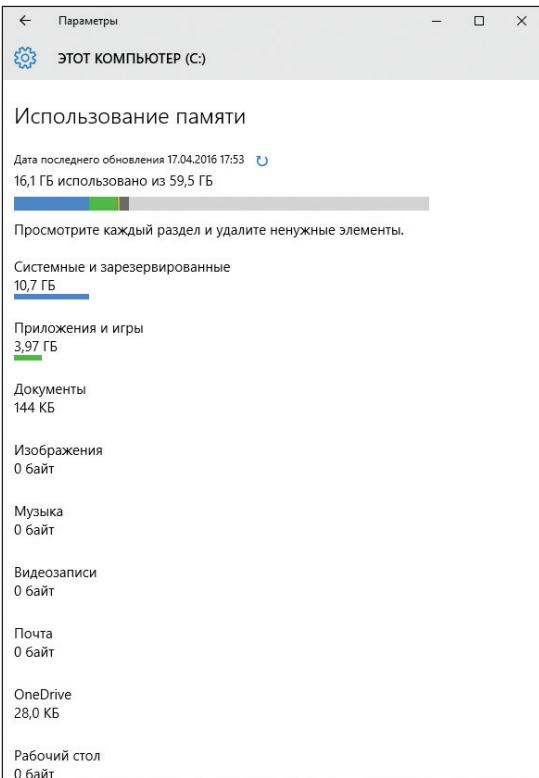


Рис. 12-4. При щелчке на диске в панели Хранилище (Storage) открывается подробный список используемого места, разбитый по категориям файлов

История файлов

Возможность История файлов (File History) была введена в Windows 8, последней в длинной линейке решений для резервного копирования для отдельных Windows ПК. Эта функция в Windows 10 претерпела лишь незначительные модификации.

История файлов (File History) (прямой потомок возможности Предыдущие версии [Previous Versions] из более старых версий Windows) требует либо внешнего диска, либо совместимого сетевого хранилища в качестве диска резервного копирования.

После выбора диска для истории файлов и включения этой функции Windows начинает сохранять копии всех файлов через регулярные промежутки времени, предоставляя пользователю хранилище резервных копий, которое позволяет восстанавливать более старые версии отдельных файлов или же целых папок или дисков. Вместе с возможностью восстановить сохраненные настройки и приложения Windows Store с помощью учетной записи Microsoft эта функция позволяет быстро перейти от одного основного вычислительного устройства к другому.

Как и для других подобных возможностей, конфигурирование функции История файлов (File History) выполняется в одной из двух точек входа. Первая находится в приложении Параметры (Settings) в Windows 10, где поиск по словам История файлов (File History) вернет простую страницу с переключателем и ссылкой Другие параметры (More Options), которая открывает панель параметров, представленную на рис. 12-5.

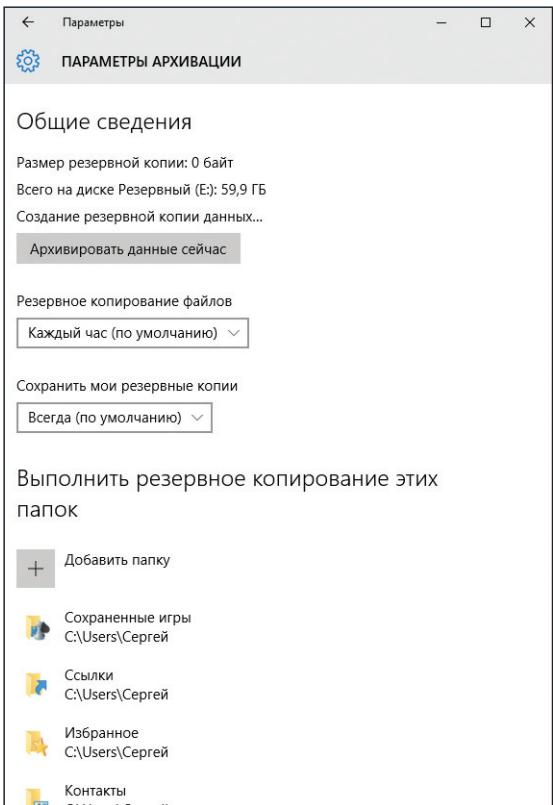


Рис. 12–5. Список папок, резервные копии которых будут создаваться функцией История файлов (File History)

Вторая точка входа, включающая многие дублирующие элементы управления и несколько уникальных опций, – классическая Панель управления (Control Panel), как показано на рис. 12–6.

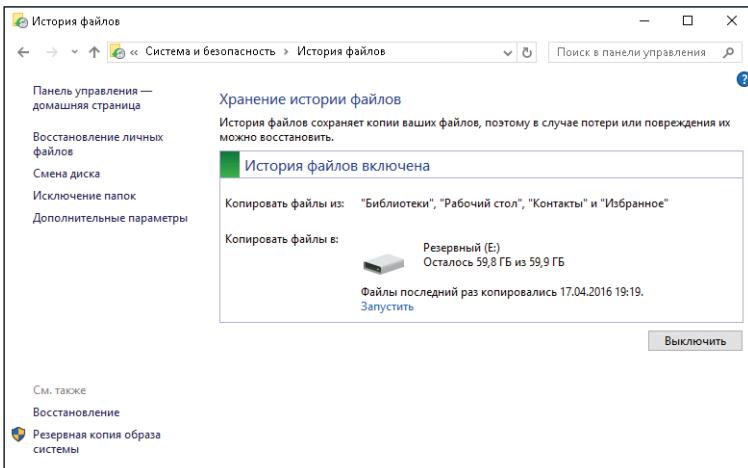


Рис. 12–6. Представление истории файлов в классической панели управления содержит возможность восстановить резервные копии файлов с резервного диска. Обратите внимание, что в данном случае в качестве цели для резервного копирования выбран второй жесткий диск

Со временем большинство этих функций должно быть перенесено в новое приложение Параметры (Settings).

Дополнительные варианты хранилища

Большинство рассмотренных выше возможностей касались стандартных настольных ПК и ноутбуков с единственным системным диском и, возможно, несколькими внешними хранилищами данных. В этом разделе описываются две экзотические возможности, которые все же заслуживают исследования, особенно для тех, кто переходит с Windows 7.

Функция Дисковые пространства (Storage Spaces) предлагает программный способ объединить несколько физических накопителей в одно виртуальное устройство, не используя аппаратные возможности, такие как RAID.

Консоль Дисковые пространства (Storage Spaces) используется для превращения двух или более накопителей в одно виртуальное устройство, которое называется Storage Space, имеющее свою собственную букву диска и действующее так, как если бы это был физический накопитель. На рис. 12-7 диски объемами 60 ГБ и 30 ГБ объединены в один виртуальный диск, который в Проводнике обозначен буквой F.

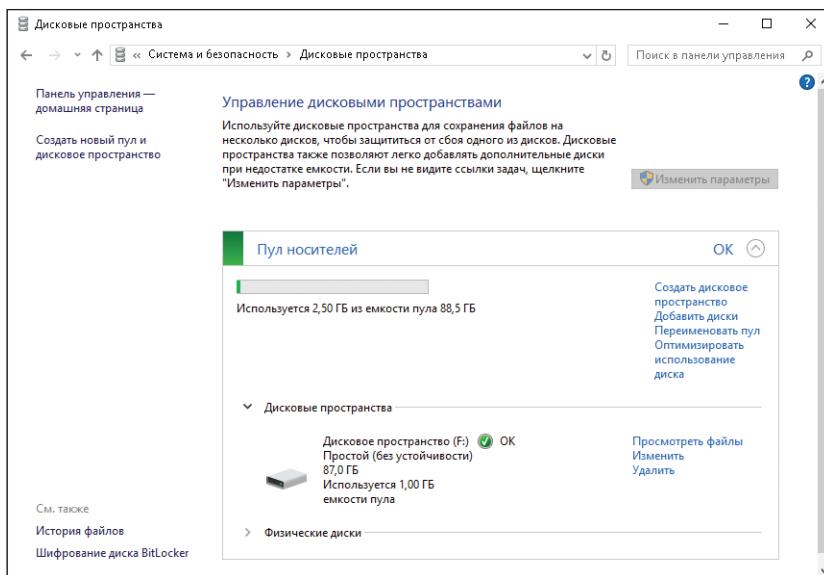


Рис. 12-7. Дисковые пространства (Storage Spaces) позволяют объединить несколько физических дисков в один виртуальный диск. В этом примере пространство объединено в один пул

При создании дисковых пространств возможны четыре типа использования пространства. Пространство, созданное с использованием опции Простой (Simple), объединяет несколько емкостей, создавая виртуальный диск с размером, равным сумме размеров всех его частей. Наличие определенного числа физических устройств позволяет выбрать более надежные варианты для защиты данных в случае сбоя физического устройства. На рис. 12-8 представлены опции, доступные в списке Тип устойчивости (Resiliency) при создании нового дискового пространства.

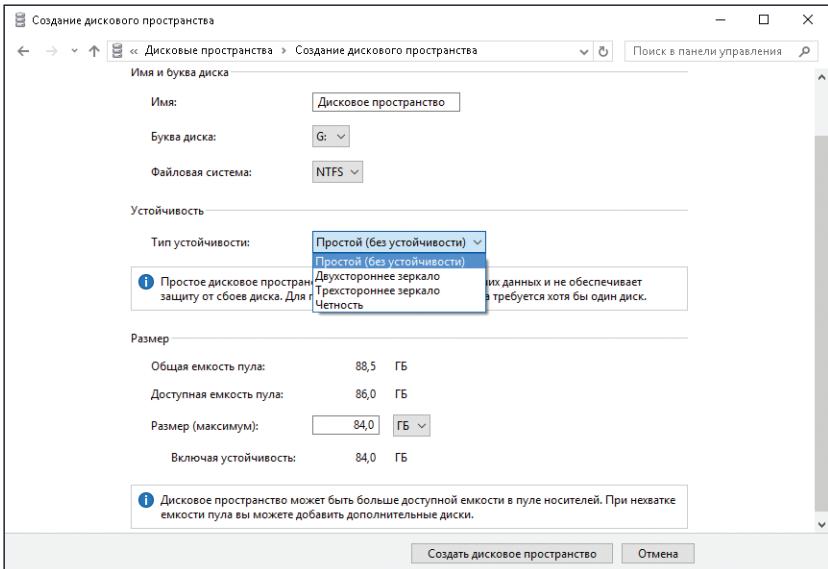


Рис. 12-8. При достаточном количестве физических дисков можно создавать устойчивые дисковые пространства, позволяющие восстановить данные при сбое физического диска

Еще одна дополнительная возможность, о которой должен знать каждый IT-профессионал, – создание и подключение файла виртуального жесткого диска (Virtual Hard Drive, VHD) так, как если бы это был физический диск. Преимущество VHD-файлов состоит в том, что их легко переносить между компьютерами и подключать двойным щелчком кнопкой мыши в Windows 10.

(Возможность подключения VHD-файлов появилась в Windows 8; на ПК с Windows 7 вам понадобится стороннее ПО.)

В консоли Управление дисками (Disk Management) имеются две тщательно скрытые, но полезные опции. Первая – создание нового VHD, который будет действовать так, как если бы он был отдельным жестким диском. Вторая – подключение существующего VHD-файла с собственной буквой диска. Если вы регулярно сохраняете файлы программ и шаблоны в стандартном месте, то вариант с созданием нового VHD-файла позволит легче перенести данные на новый ПК – поскольку перенести один файл проще, чем папку с файлами. На рис. 12-9 представлена эта возможность после выбора команды Создать виртуальный жесткий диск (Create VHD) из меню Действие (Action) в консоли Управление дисками (Disk Management).

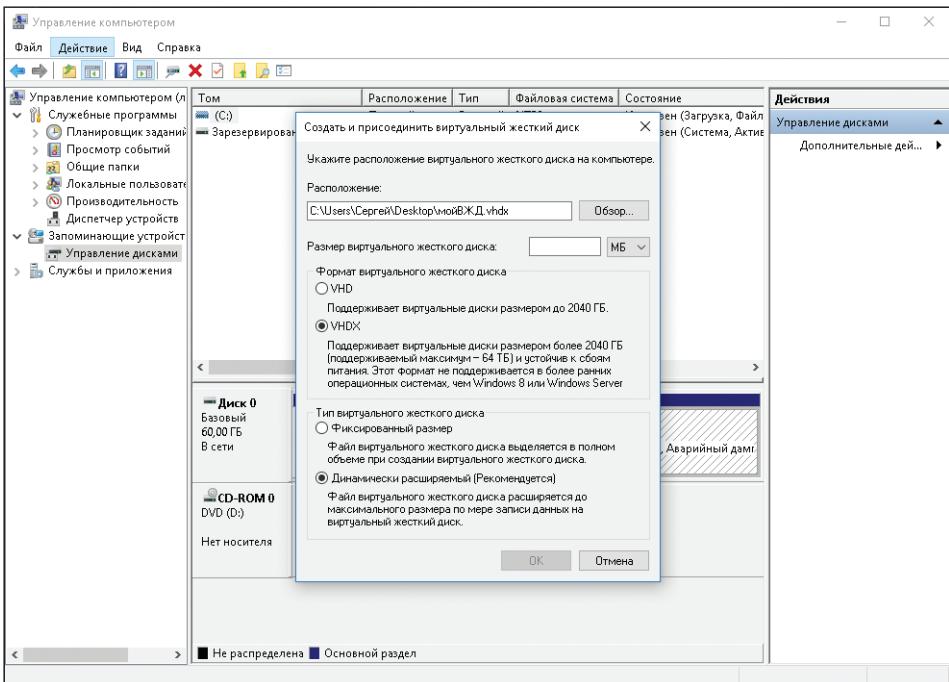


Рис. 12-9. Чтобы открыть это диалоговое окно, в меню Действие (Action) в консоли Управлении дисками (Disk Management) выберите команду Создать виртуальный жесткий диск (Create VHD). Выберите место и имя файла, чтобы создать виртуальный жесткий диск, который действует как отдельный физический диск

Наконец, для фиксированных и съемных накопителей редакции Windows 10 Pro, Enterprise и Education предлагают полный диапазон возможностей шифрования BitLocker и BitLocker To Go. Длинный список усовершенствований облегчает использование этих возможностей в сравнении с их предшественниками в Windows 7. На рис. 12-10 представлен портативный ПК с зашифрованным системным диском и съемной SD-картой с зашифрованным томом.

BitLocker Drive Encryption

Control Panel Home BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

OS (C): BitLocker on

Suspend protection
Back up your recovery key
Turn off BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

D: BitLocker on

Back up your recovery key
Change password
Remove password
Add smart card
Turn on auto-unlock
Turn off BitLocker

See also

TPM Administration
Disk Management
Privacy statement

Рис. 12-10. Возможностями BitLocker гораздо легче управлять в Windows 10, чем в предыдущих версиях

ГЛАВА 13

Управление мобильными устройствами и корпоративными данными

В прежние времена управление сетью выполнялось относительно легко. Сотрудники садились за стол, входили в ПК компании и подключаясь к ресурсам компании на серверах компании.

Сегодня все изменилось.

В мире «Принеси свое собственное устройство» (Bring Your Own Device, BYOD) сотрудники ожидают, что смогут выполнять свою работу с любого места, с любого устройства, имея полный доступ к своим рабочим ресурсам и данным. Такой подход делает многие традиционные методики управления непрактичными, а зачастую – технически невозможными. И особенно остро встает вопрос защиты конфиденциальных данных и соответствия законодательным актам, которые относятся к вашей индустрии.

К счастью, на помощь приходит новое поколение инструментов управления мобильными устройствами (mobile device management, MDM) от Microsoft и других компаний. Они соответствуют стандартам и обеспечивают доступ к корпоративным приложениям и информации с сохранением эффективного контроля над ресурсами.

Стратегии управления мобильными устройствами

Microsoft предлагает два основных инструмента управления широким диапазоном устройств в организации.

- System Center Configuration Manager предлагает полные возможности управления над традиционными устройствами, подключенными к домену Windows ПК, включая работающие под управлением Windows To Go и Windows Embedded. Он также работает с устройствами Apple под управлением OS X. Самый последний выпуск, System Center Configuration Manager (SCCM) и Endpoint Protection (версии 1511), позволяет управлять устройствами с Windows 10 напрямую через MDM.

- Microsoft Intune – это облачный сервис, который может управлять ПК с Windows 10, а также мобильными устройствами с Windows 10 Mobile, iOS и Android. Конечно, уровень контроля ниже, чем для полностью управляемых, подключенных к домену ПК, но управлять предсказуемыми сценариями вы сможете. Microsoft Intune также может интегрироваться в SCCM.

Ключ к успешной интеграции персональных компьютеров и планшетов сотрудников в стратегии MDM – это набор открытых стандартов, которые используют протоколы Open Mobile Alliance Device Management - точнее OMA-DM 1.2.1. Эти протоколы отвечают за защищенную коммуникацию с облачными службами управления, используя HTTPS.

Этот агент управления доступен на большинстве мобильных устройствах, и он включен по умолчанию со всеми редакциями Windows 10, дополнительное ПО не требуется. Для ПК, которыми владеет и управляет организация, можно развернуть полный клиент диспетчера конфигурации. Подключение к домену персональных устройств, которые сотрудники приносят в рамках стратегии BYOD, как полностью управляемых устройств либо непрактично, либо невозможно – персональные устройства с редакцией Core Windows 10 или Windows 10 Mobile не имеют возможности подключения к домену. В таком случае можно использовать Microsoft Intune для упрощенного управления.

Инструменты управления, поддерживающие OMA-DM, включая Microsoft Intune, MobileIron и AirWatch, могут выполнять следующие задачи:

- инвентаризация оборудования и ПО;
- конфигурация ключевых настроек;
- установка и конфигурация современных бизнес-приложений;
- предоставление и развертывание сертификатов;
- защита данных, включая возможность очистки утерянного или украденного устройства.

Две дополнительные возможности могут использоваться как часть стратегии BYOD. Azure Active Directory (Azure AD) позволяет провести аутентификацию персонального устройства и разрешить пользователю обращаться к корпоративным ресурсам и приложениям. (Эта возможность детально обсуждалась в главе 10.) Рабочие папки (Work Folders) – это упрощенная функция синхронизации файлов, введенная в Windows 8.1, которую могут использовать персональные устройства с Windows 10 для защищенного хранения и доступа к файлам из корпоративной сети.

В этой главе рассматриваются все вышеупомянутые стратегии.

System Center Configuration Manager

System Center Configuration Manager с Endpoint Protection – это самый последний выпуск универсального инструмента управления от Microsoft для Windows-систем (физических и виртуальных) и мобильных Windows-устройств. Вместе с Microsoft Intune он обеспечивает унифицированную среду управления, которая поддерживает и устройства компании, и персональные (BYOD) устройства.



Примечание. Если вы использовали предыдущие версии диспетчера System Center Configuration Manager, то не могли не заметить отсутствие года в имени текущего выпуска. Это решение отражает стратегию более частого выпуска обновлений. Как и в случае с Windows 10, версии Configuration Manager теперь идентифицируются строкой из четырех цифр в формате ггмм. На момент написания текущая версия – 1511 (у Technical Preview версия 1512). Обзор версии 1511 вы найдете по адресу: <http://bit.ly/system-center-1511>.

Configuration Manager – это ориентированный на пользователей инструмент работы с инфраструктурой Active Directory организации. Он связывает аппаратные ресурсы с конкретными пользователями, позволяя предоставлять им доступ к конкретным программам и возможностям. Configuration Manager также предоставляет IT-профессионалам всестороннюю платформу генерации отчетов и возможности развертывания.

Configuration Manager содержит следующие функции.

- **Развертывание/обновление операционной системы.** Самый последний выпуск Configuration Manager поддерживает широкий диапазон сценариев развертывания, включая обновления на месте для перевода систем прямо с Windows 7 и Windows 8.1 до Windows 10. (Эти сценарии подробнее рассматривались в главе 4.)
- **Управление приложениями.** Configuration Manager включает набор инструментов и ресурсов для упаковки, управления, развертывания и мониторинга приложений в организации.
- **Защита Endpoint Protection.** Включает возможности управления защитой, антивирусом и брандмауэром Windows.
- **Настройки соответствия.** Встроенные инструменты позволяют анализировать и настраивать конфигурацию клиентских устройств, чтобы они отвечали требованиям соответствия.
- **Доступ к ресурсам компании.** Предоставляйте удаленный доступ к ресурсам, настраивая профили Wi-Fi, профили виртуальных частных сетей (virtual private network, VPN) и профили сертификатов. Например, можно установить сертификаты доверенных корневых центров сертификации для организации, чтобы проверять подлинность устройств с Windows 10 на корпоративных Wi-Fi точках доступа и VPN.
- **Профили удаленных подключений.** Создавайте и развертывайте настройки удаленных подключений на устройствах, облегчая пользователям задачу подключения их компьютеров к корпоративной сети.
- **Инвентаризация.** Администратор может собирать подробную информацию об оборудовании, ПО, файлах данных и использовании лицензий на управляемых устройствах.

Configuration Manager также включает инструменты удаленного контроля для специалистов технической поддержки и возможности для развертывания обновлений ПО.

Одно из самых важных изменений в последних выпусках System Center Configuration Manager – это возможность сконфигурировать зарегистрированные устройства как собственность компании или собственность пользователя. Персональные устройства не подключаются к домену, и на них

не устанавливается клиент диспетчера конфигурации. В отчет об инвентаризации ПО включается только то ПО, что принадлежит компании. Функции очистки и «освобождения» устройства также предоставляют возможность удаления с устройств только содержимого компании, оставляя личные данные и приложения.

Для управления такими устройствами, которые не подключены к домену и на которых не установлен клиент Configuration Manager, используется Microsoft Intune (описывается в следующем разделе).

Microsoft Intune

Microsoft Intune использует унифицированную веб-консоль администрирования, которая предоставляет возможности управления устройствами, развертывания ПО и обеспечения безопасности. Поскольку это облачная консоль управления, Microsoft Intune не требует VPN-подключения к локальному домену. Microsoft Intune не требует установленной инфраструктуры, хотя и хорошо работает в комбинации с Configuration Manager.

Одна из уникальных возможностей в Microsoft Intune – это настраиваемый портал компании. Портал компании – это интерфейс, настраиваемый с помощью загружаемых приложений, которые IT-администраторы могут сделать доступными для организации. Портал компании также позволяет пользователям напрямую связываться с IT-отделом и запрашивать удаленную помощь. На рис. 13-1 показана панель для управления мобильными устройствами.

The screenshot shows the Microsoft Intune web interface. On the left, there's a navigation sidebar with icons for Dashboard, Groups, Alerts, Apps, Policy, Reports, and Admin. The Admin section is currently selected. The main content area has a header 'Mobile Device Management'. It features a yellow callout box with the text 'Next: Set up and deploy a mobile device security policy.' Below it is a 'Mobile Device Management Authority' section with a 'Set to Microsoft Intune' button. A 'Tasks' sidebar on the right lists 'Manage Mobile Devices', 'Learn About' sections for various platforms, and 'Remote Tasks (0)'. The central part of the screen displays 'Available Mobile Platforms' for Windows, Windows Phone, iOS and Mac OS X, and Android, each with status indicators and configuration links. At the bottom, there's a footer with Microsoft branding and links for Privacy & Cookies and Feedback.

Рис. 13-1. Панели в Intune позволяют управлять мобильными устройствами, в том числе работающими под управлением Windows 10

Для управления ПК с Windows 10 в Microsoft Intune (или на стороннем MDM-сервере) понадобится установить клиентское ПО, которое может развертываться вручную, устанавливаться автоматически с использованием групповой политики или как часть образа. (За деталями обратитесь по адресу: <https://technet.microsoft.com/en-us/library/dn646969.aspx>.) Этот клиент управляет регистрацией (enrollment), процессом, который устанавливает один или несколько сертификатов на мобильном устройстве для управления аутентификацией, а затем периодически синхронизируется с сервером управления для проверки обновлений и применения новых политик.

Microsoft Intune включает возможность развертывания приложений автоматически в ходе регистрации. Пользователи могут и сами устанавливать дополнительные приложения с портала компании. Пользователи могут безопасно обращаться к корпоративной информации, используя мобильные приложения Office и бизнес-приложения, а руководство имеет возможность ограничить действия, которые могут привести к утечке конфиденциальных данных, например, копирование и вставку или сохранение, только приложениями, которые управляются Intune.

Для ПК с Windows 10 можно конфигурировать и развертывать классические Windows-приложений, используя Intune Software Publisher, представленный на рис. 13-2.

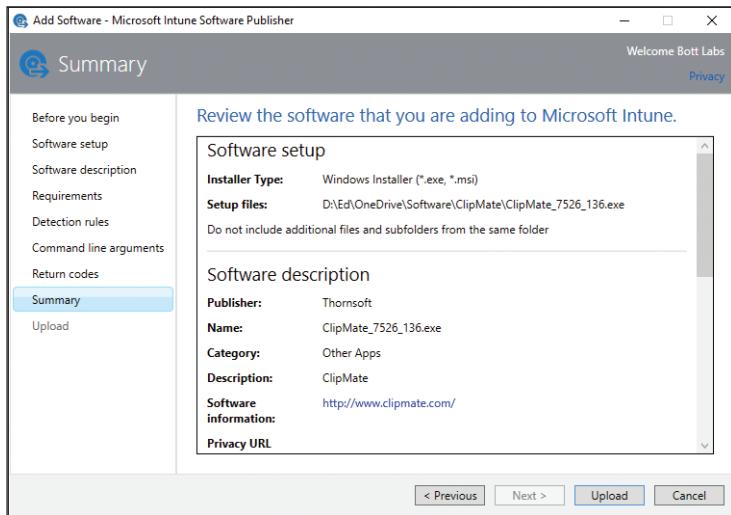


Рис. 13-2. Microsoft Intune включает библиотеку ПК, в которой можно публиковать и развертывать приложения, включая классические настольные Windows-программы для управляемых ПК

Intune также может использоваться для удаления корпоративных данных и приложений, когда регистрация устройства отменяется, устройство утеряно, украдено или списывается с баланса.

Рабочие папки

Рабочие папки – еще одна относительно новая возможность, поддерживаемая устройствами с Windows 10 (и более ранними версиями), а также мобильными устройствами, которые подключаются к Windows Server 2012 R2 или более поздней версии. Когда функция Рабочие папки (Work Folders) включена, пользователь может безопасно синхронизировать данные на своем устройстве со своей папкой в корпоративном дата-центре, что позволяет ему работать без подключения к сети. Файлы, созданные или модифицированные в локальной копии папки, синхронизируются с файловым сервером в корпоративной среде. Рабочие папки могут настраиваться на различных устройствах, работающих под управлением Windows, iOS или другой поддерживаемой платформы. Если пользователь сохранит все свои личные рабочие файлы в рабочих папках (можно создавать любое количество вложенных папок), то они будут передаваться на все устройства пользователя.

Описание этой функции может быть вам знакомо, как минимум на низком уровне. Это новое поколение технологии кэширования на стороне клиента (client-side caching, CSC), которая давно является частью Windows-сетей, обеспечивая такие возможности, как перенаправление папок и Автономные папки (Offline Folders). Разница в том, что для работы Автономных папок (Offline Folders) устройство должно быть подключено к домену. Это сразу отсекает персональные устройства с потребительскими версиями Windows. Эта функция не работает с планшетами с операционными системами, отличными от Windows.

Устройства с Windows 10 не обязательно должны быть подключены к домену для синхронизации с персональными файлами, которые хранятся на сервере. Учетные данные домена разблокируют доступ к рабочим папкам, поддерживая безопасный автономный доступ к файлам.

На стороне сервера функция Рабочие папки (Work Folders) включается ее установкой в составе роли Файловые службы (File Services) на сервере с Windows Server 2012 R2 или позднее. Будет установлена новая панель, которая позволит определить расположение на сервере для синхронизации с конкретным пользователем, а затем либо создать DNS-запись, либо опубликовать собственный URL-адрес для доступа к общим файлам.

Настройка рабочих папок также включает Individual Rights Management (IRM) и Dynamic Access Control (DAC) для файлов в общем расположении. Используя эти возможности, администраторы могут обозначать конкретные документы как ресурсы компании, которыми затем можно управлять, чтобы не допустить несанкционированный доступ с локального устройства.

На стороне клиента синхронизация интегрирована в файловую систему. Для подключения к рабочим папкам откройте Панели управления (Control Panel) и щелкните на ссылке Настроить рабочие папки (Set Up Work Folders), представленной на рис. 13-3.

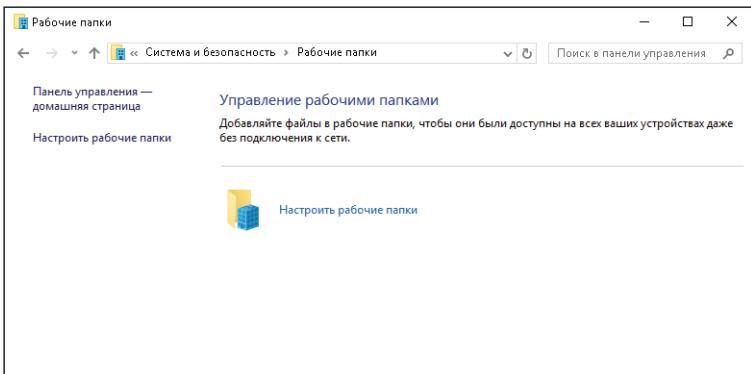


Рис. 13-3. Функция Рабочие папки (Work Folders) встроена в настольную Панель управления (Control Panel) во всех редакциях Windows 10

Будет открыт простой мастер, в котором нужно ввести свой адрес электронной почты или URL-адрес, который настроил администратор, а затем принять политики безопасности, связанные с файлами данных в хранилище рабочих папок, которые включают право удаленного удаления этих данных. Могут потребоваться такие возможности устройства, как шифрование синхронизируемой папки и защищенный паролем экран блокировки.

Функция Рабочие папки (Work Folders) похожа по концепции на другие связанные с файлами возможности компании Microsoft, особенно OneDrive и OneDrive для бизнеса. В чем ее отличие?

OneDrive – это ориентированная на потребителей служба, предназначенная для хранения персональных файлов. Она подключается к учетной записи Microsoft и не может централизованно управляться или архивироваться. Это делает ее неподходящей для корпоративных данных.

OneDrive для бизнеса предоставляет доступ к ресурсам Microsoft SharePoint и персональным файлам, размещенным в облаке Office 365. Она предназначена главным образом для совместной работы с данными в командах со строгими рабочими процессами. Ею можно безопасно управлять, но чрезмерно большой набор возможностей делает ее излишне сложной для простого хранилища файлов и синхронизации между устройствами.

Рабочие папки не включают функций обмена файлами, но чрезвычайно легки в работе. Не нужно использовать VPN-подключение. Администратор может потребовать включение опции Присоединение к рабочему месту (Workplace Join), блокируя потенциальному атакующему (или беспечному работнику) доступ к файлам через недоверенные устройства. Не требуется установка какой-либо утилиты синхронизации или дополнительная конфигурация, помимо начальной настройки.

Для Windows 10 возможность Рабочие папки (Work Folders) была усовершенствована, и синхронизация изменений теперь выполняется гораздо быстрее. (В Windows 8.1 операции синхронизации могли откладываться на 10 минут.) В Windows 10 версии 1511 добавлена интеграция с Enterprise Data Protection; теперь администратор может требовать шифрование на удаленном устройстве, используя ключ, связанный с Enterprise ID, и может очищать данные удаленно с помощью ПО MDM, например, Microsoft Intune.

ГЛАВА 14

Windows 10 на телефонах и маленьких планшетах

Первая забота IT-профессионала – поддержка Microsoft Windows 10 на настольных ПК и ноутбуках. После унификации платформы Windows 10 к ним добавились телефоны и планшеты под Windows 10 Mobile.

Windows 10 Mobile для мобильных устройств построена на том же коде ядра, что и Windows 10 для традиционных ПК и ноутбуков, и выполняет те же универсальные приложения, доставляемые через тот же Windows Store, что и настольный аналог.

Эта версия Windows 10 подразумевает и маленькие планшеты, но на сегодняшний день только в теории. Можно установить Windows 10 Insider Preview для телефонов на таких устройствах, как Lumia 1520, которое имеет 6-дюймовый экран и может заменять планшет. (Телефоны с очень большими экранами иногда называют «фаблетами» [phablet] из-за возможности переключать роли между телефоном и планшетом.)

Знаковая возможность Windows 10 Mobile, которая называется Continuum, позволяет подключить мобильное устройство к внешнему монитору, мыши и клавиатуре и получить, по сути, маленький ПК на Windows 10. Continuum использует универсальную платформу Windows (Universal Windows Platform): встроенные приложения, такие как Почта (Mail), и приложения Office Mobile работают точно так же, как на ПК с Windows 10.

В этой главе предлагается краткий обзор возможностей Windows 10 Mobile. Начнем с истории.

Эволюция Windows на мобильных устройствах

За шесть лет своего существования платформа Windows Phone претерпела несколько важных перемен, постепенно сближающих мобильную и настольную операционные системы. Windows Phone 8 была первой версией на основе ядра Windows NT из настольной операционной системе; она была выпущена в октябре 2012, одновременно с Windows 8 для настольных ПК.

Windows Phone 8.1, выпущенная в середине 2014 года, представила Кортану (Cortana), персонального цифрового ассистента, и первую волну приложений, способных разделять данные и лицензии между настольной и мобильной платформами.

Первый публичный выпуск Windows 10 для телефонов вышел как Technical Preview в феврале 2015, несколько месяцев спустя после выхода первого настольного Windows 10 Technical Preview. Начальный выпуск поддерживал только ряд телефонов. До конца года вышло еще несколько выпусков, расширяющих выбор телефонов.

В конце 2015 года, несколько месяцев спустя после выхода выпуска Windows 10 для ПК, Microsoft выпустила два флагманских телефона, Lumia 950 и Lumia 950XL (представлен на рис. 14-1), с предустановленной Windows 10. Несколько других производителей анонсировали поддержку платформы. Официальный выпуск для других поддерживаемых устройств – начало 2016 года.



Рис. 14-1. Microsoft Lumia 950XL – одно из первых устройств, поставляемых с Windows 10 Mobile

В названии Windows 10 Mobile слово Phone убрано, показывая, что эта операционная система рассчитана для работы на небольших планшетах (с размерами меньше 8 дюймов по диагонали), включая модели на тех же процессорах ARM, которые используются в телефонах и планшетах, работающих под управлением других операционных систем. На момент написания, в начале 2016 года, таких устройств еще не было.



Примечание. Это не первая операционная система Microsoft, способная работать на планшетах с процессором ARM. Windows RT, на которой работают Surface RT и Surface 2, а также несколько сторонних устройств – это, по сути, Windows 8, перекомпилированная для работы с процессорами ARM. Устройства с Windows RT нельзя будет обновить до Windows 10.

ГЛАВА 15

Что нового в групповой политике в Windows 10

Для IT-профессионалов возможность управлять ПК с использованием групповой политики – одна из главных причин выбора Microsoft Windows. Дополненная Active Directory, групповая политика обеспечивает применение политик безопасности для управления содержимым и приложениями на устройствах компании и сокращает затраты на поддержку, не давая пользователям непреднамеренно нарушить работу правильно сконфигурированных систем.

В этом главе приводится подборка самых интересных новых политик Windows 10.

Для удобства большинство примеров в этой главе иллюстрируются в окне редактора локальной групповой политики (Local Group Policy Editor, Gpedit.msc). Эта утилита незаменима при знакомстве с Windows 10, если у вас нет доступа к контроллеру домена или не нужна мощь и сложность Active Directory. Конечно, все рассматриваемые в этой главе политики могут задаваться с использованием групповой политики в домене Active Directory.

Полный список настроек политики, которые включаются с файлами административных шаблонов (.admx), поставляемых с текущими версиями Windows, имеется в последнем обновлении справочника «Group Policy Settings Reference for Windows and Windows Server» в центре загрузок Microsoft по адресу: <http://bit.ly/group-policy-settings>. (Все загрузки на этой странице имеют формат таблицы Microsoft Excel.)

Windows Update для бизнеса

Для многих IT-профессионалов самыми интересными являются те политики безопасности, которые управляют установкой обновлений из Windows Update. Возможности Windows Update для бизнеса позволяют администраторам откладывать установку отдельных и накопительных обновлений с интервалами в одну неделю общим сроком до четырех недель и откладывать главные обновления возможностей общим сроком до восьми месяцев.

Эти две политики находятся в одной настройке Отложить обновления (Defer Upgrades and Updates), расположенной по адресу Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Центр обновления Windows (Computer Configuration > Administrative Templates > Windows Components > Windows Update). Когда Windows Update включена, как показано на рис. 15-1, можно задать разные значения для каждой политики. Если текущее обновление вызывает проблемы в сети вашей организации, установите флагок Приостановить обновления (Pause Upgrades And Updates).

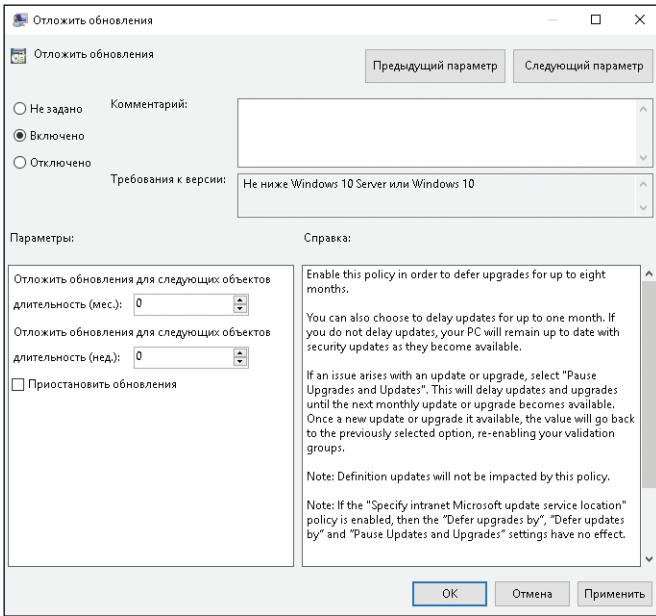


Рис. 15-1. Групповая политика для включения возможностей Windows Update для бизнеса позволяет отложить установку обновлений (updates) и полных обновлений возможностей (upgrades)

Эти настройки не применяются, если доставка обновлений выполняется не с серверов Windows Update, а с помощью другого инструмента, например, служб Windows Server Update Services (WSUS) в вашей сети. Кроме того, если на компьютере с Windows 10 Enterprise политика Разрешить телеметрию (Allow Telemetry) включена и установлена в значение 0, то Windows Update, по сути, отключается, и настройки Windows Update для бизнеса не действуют.

Device Guard

Device Guard, еще одна новая возможность, доступная только в редакции Windows 10 Enterprise, позволяет блокировать устройство так, чтобы оно могло выполнять только приложения из утвержденного списка. Credential Guard, связанная возможность обеспечения корпоративной безопасности, использует аппаратную виртуализацию для защиты учетных данных.

Развертывание Device Guard, с или без Credential Guard, - это сложный процесс, включающий аппаратные возможности защиты, создание политики целостности кода и применение этой политики к отдельным устройствам. Настройки групповой политики представляют собой маленькую, но очень важную часть в этом процессе развертывания. Эти настройки, представленные на рис. 15-2 и 15-3, находятся в Конфигурация компьютера > Административные шаблоны > Система > Device Guard (Computer Configuration > Administrative Templates > System > Device Guard).

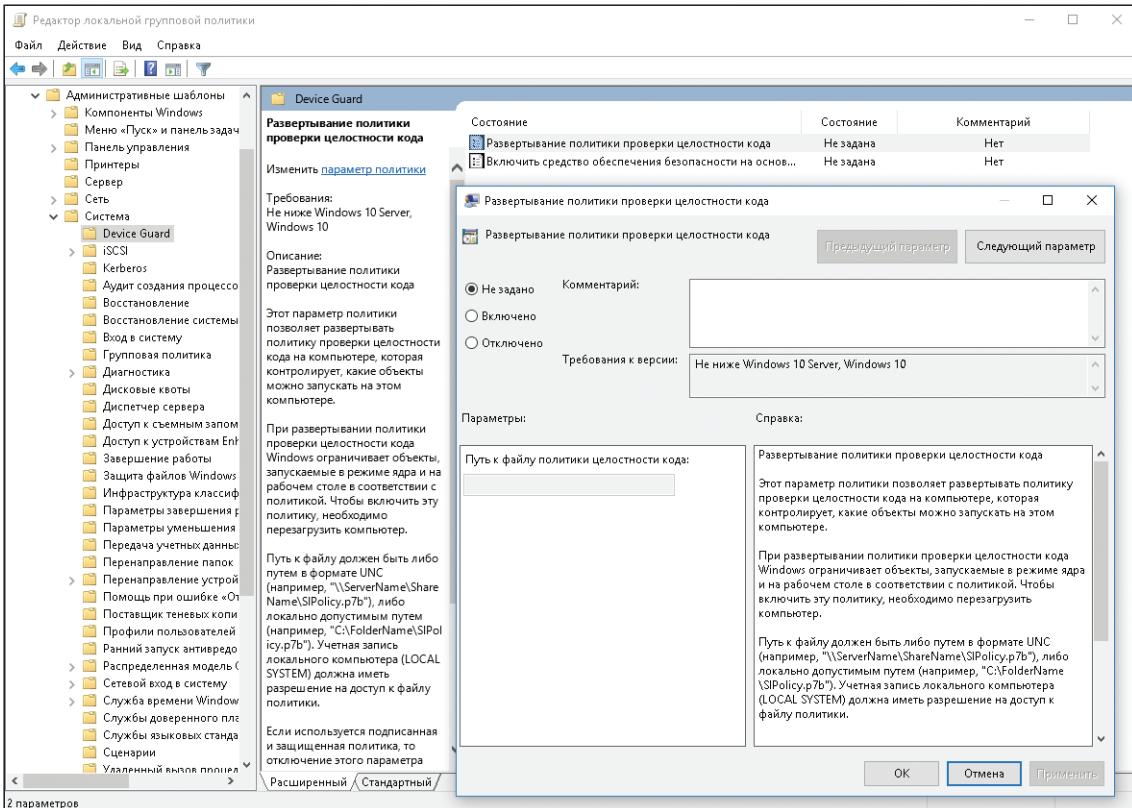


Рис. 15–2. Device Guard – это новая возможность, которая позволяет заблокировать устройство с Windows 10 так, чтобы выполнялись только доверенные программы. Эти настройки политики – малая часть процесса развертывания

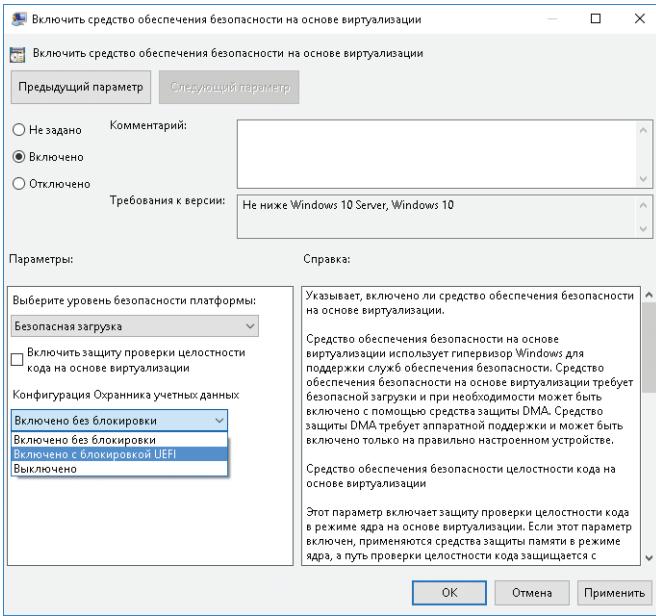


Рис. 15-3. На системах с Windows 10 Enterprise Credential Guard предлагает улучшенную защиту учетных данных домена



Примечание. Device Guard рассматривается в разделе «Блокировка корпоративных ПК с помощью Device Guard» в главе 5. Официальное (и очень подробное) руководство по развертыванию Device Guard находится по адресу: <http://bit.ly/DG-deploy>.

Microsoft Passport для работы

Подключенные к домену устройства с Windows 10 могут использовать новую возможность Microsoft Passport для защищенного обмена учетными данными без использования паролей. После регистрации устройства путем аутентификации в службе, подобной Azure AD или Active Directory, пользователь сможет выполнять вход с помощью жеста, биометрии или ПИН-кода.

Администратор может управлять конфигурацией Microsoft Passport, требуя, например, наличия аппаратного устройства защиты (TPM) или проведения биометрической аутентификации, а также задавая требования сложности для ПИН-кода. Эти настройки находятся в разделе Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Microsoft Passport для работы (Computer Configuration > Administrative Templates > Windows Components > Microsoft Passport for Work).

Microsoft Edge и Internet Explorer

С введение браузера Microsoft Edge в Windows 10 появились и новые объекты групповой политики, управляющие его поведением и конфигурацией. Кроме того, Internet Explorer 11 теперь поддерживает Режим предприятия (Enterprise Mode), который также настраивается через групповую политику.

Windows 10 версии 1511 включает больше десятка настроек для Microsoft Edge, которые доступны из нового административного шаблона Microsoftedge.admx. Эта группа настроек представлена на рис. 15-4. Путь к ней: Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Microsoft Edge (Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge).

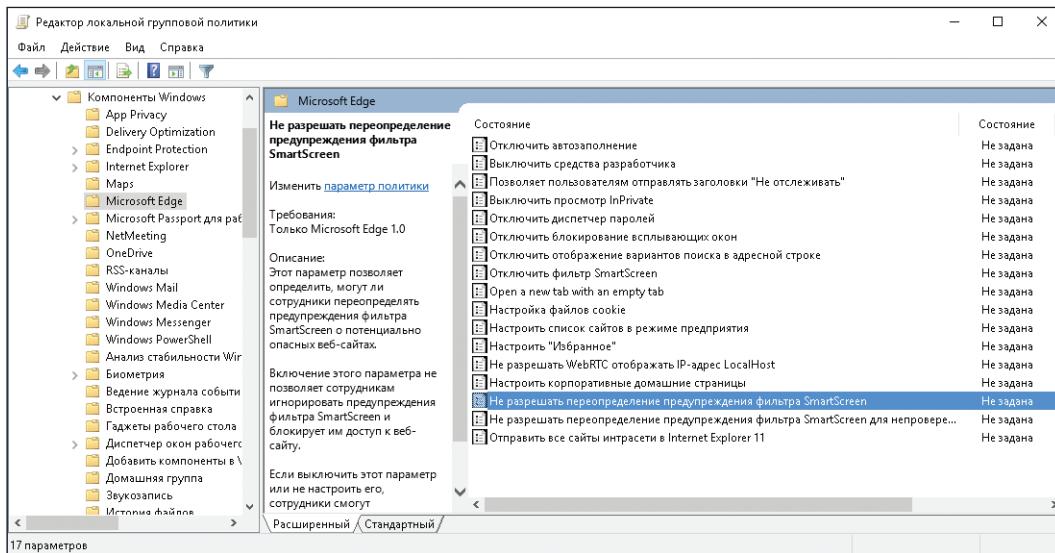


Рис. 15-4. Новый браузер по умолчанию в Windows 10, Microsoft Edge, поставляется со своим собственным набором настроек групповой политики

Конфигурирование режима предприятия включает настройку групповой политики в разделе Microsoft Edge и две настройки в Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Internet Explorer (Computer Configuration > Administrative Templates > Windows Components > Internet Explorer). Эти настройки определяют, могут ли пользователи включать и использовать режим предприятия из меню Сервис (Tools), и позволяют указать расположение списка веб-сайтов режима предприятия, как показано на рис. 15-5.

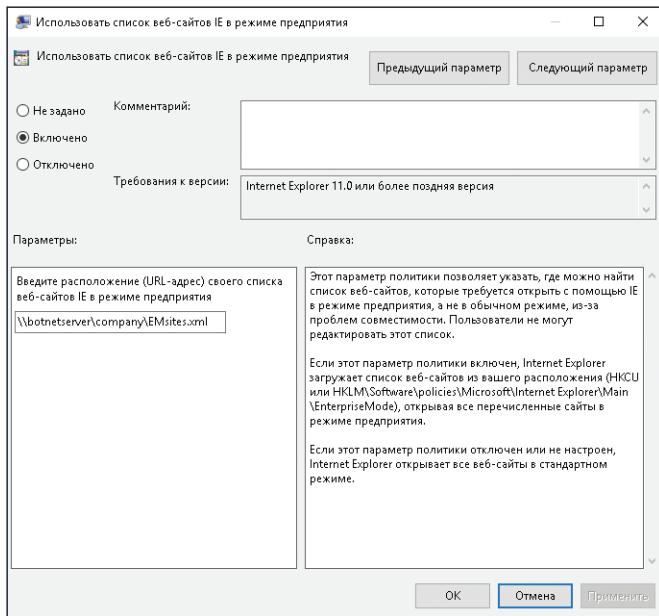


Рис. 15-5. Конфигурирование режима предприятия для Internet Explorer 11 позволяет пользователям открывать сайты, которые не отвечают современным веб-стандартам

Еще одна настройка для Internet Explorer в Windows 10, заслуживающая внимания, – это политика, управляющая использованием сетевого протокола HTTP2.

Управление доступом к предварительным сборкам и данным телеметрии

Важный вклад в разработку Windows 10 вносят добровольные участники программы Windows Insider, которые первыми получают предварительные сборки для тестирования. Такие предварительные сборки подразумевают риск нестабильной работы или потери данных.

Ограничить доступ к предварительным сборкам позволяют настройки политики в разделе Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Сборки для сбора данных и предварительные сборки (Computer Configuration > Administrative Templates > Windows Components > Data Collection And Preview Builds), представленные на рис. 15-6.

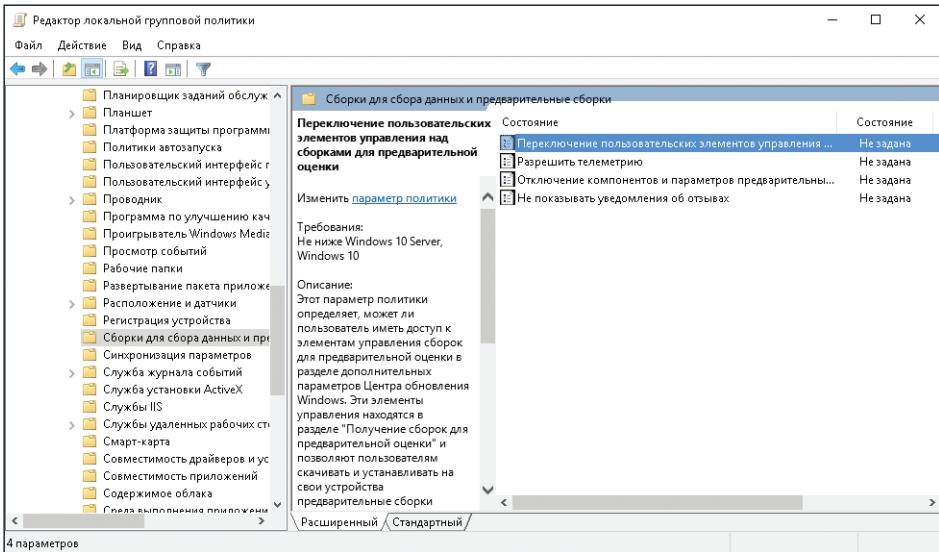


Рис. 15-6. Эта политика позволяет запретить пользователям устанавливать предварительные сборки Windows 10

Установка настройки Переключение пользовательских элементов управления над сборками для предварительной оценки (Toggle User Control Over Insider Builds) в значение Отключено (Disabled) запрещает пользователям получение предварительных сборок. Следует отметить, что эта настройка политики применяется только к устройствам с редакциями Pro, Enterprise и Education Windows 10.

Настройка Разрешить телеметрию (Allow Telemetry), которая также находится в этой группе, создает четвертую опцию, минимизирующую объем данных, отправляемых в компанию Microsoft как часть политики сбора данных диагностики и использования. (Три других опции находятся по адресу Параметры > Конфиденциальность > Отзывы и диагностика [Settings > Privacy > Feedback & Diagnostics]). Эта минимальная настройка отправляет только данные средств защиты Malicious Software Removal Tool и Защитника Windows (Windows Defender) (если включена) и настройки клиента телеметрии.

Управление оптимизацией доставки обновлений Windows

Windows 10 преднамеренно создает систему доставки «точка-точка», которая помогает распределить нагрузку доставки приложений и обновлений Windows. В управляемой среде может потребоваться ограничить этот пиринговый обмен устройствами в одной локальной сети или домене и управлять пропускной способностью, которую может использовать эта возможность.

Эти и другие настройки политики находятся в Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Delivery Optimization (Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization). Путает то, что в тексте описания для этой настройки указываются числовые значения (от 0 до 3, 0 отключает эту возможность), в то время как в самом интерфейсе этой настройки в редакторе групповой политики имеется раскрывающийся список, элементы которого соответствуют числовым значениям, как показано на рис. 15-7.

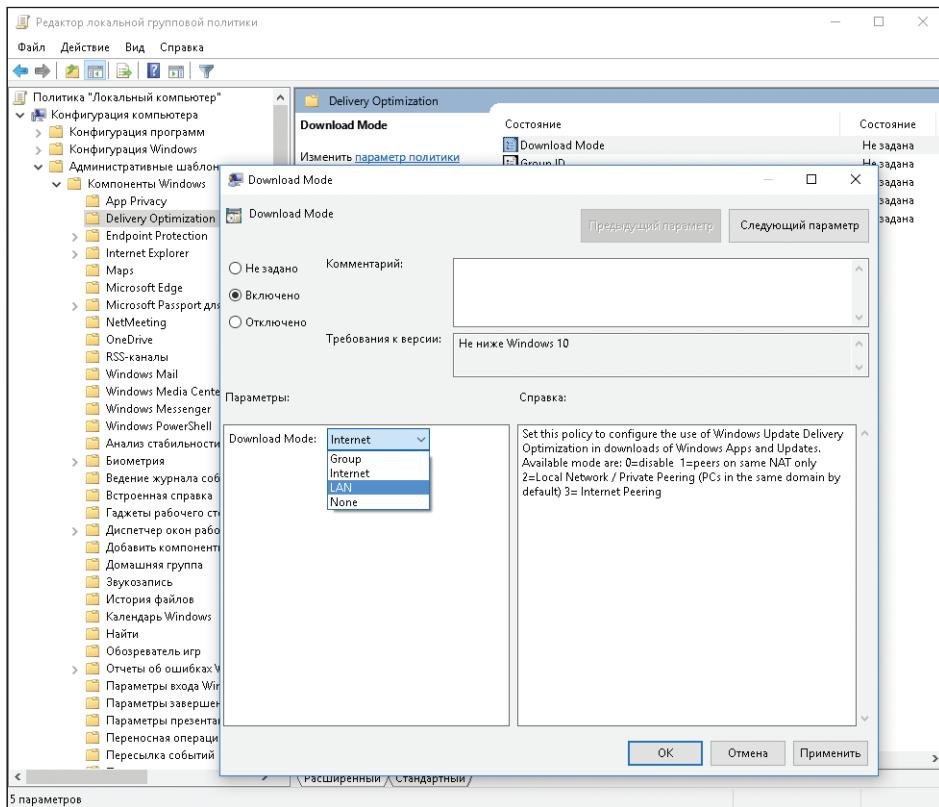


Рис. 15-7. Политики оптимизации доставки позволяют управлять пиринговой доставкой приложений и обновлений Windows в корпоративной сети

Политики безопасности

Список политик безопасности, доступных для ПК с Windows 10, занял бы много страниц. В распоряжении администраторов имеется детальный контроль над каждым аспектом системы. Большинство этих политик в Windows 10 являются расширениями ранее доступных политик, в том числе многие из тех, что появились в выпусках Windows 8 и 8.1.

Несколько новых политик в этой группе для Windows 10 являются особенно интересными.

Например, в разделе Конфигурация компьютера > Административные шаблоны > Система > Параметры уменьшения рисков (Computer Configuration > Administrative Templates > System > Mitigation Options) находится новая настройка Блокировка недоверенных шрифтов (Untrusted Font Blocking), которая не позволит пользователям загружать файлы шрифтов, за исключением правильно установленных в защищенную папку Шрифты (Font).

Еще одна новая политика находится в Конфигурация компьютера > Административные шаблоны > Компоненты Windows\Шифрование диска BitLocker\Диски операционной системы (Computer Configuration > Administrative Templates > Windows Components\BitLocker Drive Encryption\Operating System Drives). Включив настройку политики Настроить сообщение о восстановлении, отображаемое перед загрузкой, и URL-адрес (Configure Pre-boot Recovery Message And URL), можно указать собственное сообщение о восстановлении или заменить существующий URL-адрес на экране восстановления ключа, когда диск с операционной системой заблокирован.

Наконец, новая опция в Windows 10 версии 1511 предлагает новые варианты для алгоритма шифрования и стойкости ключа шифрования, используемые с дисками BitLocker. Новая поддержка шифрования XTS-AES подходит для стационарных дисков; ее нужно использовать с осторожностью со съемными дисками, которые могут также использоваться на более старых версиях Windows, которые не поддерживают этот тип шифрования.

Эти настройки представлены на рис. 15-8.

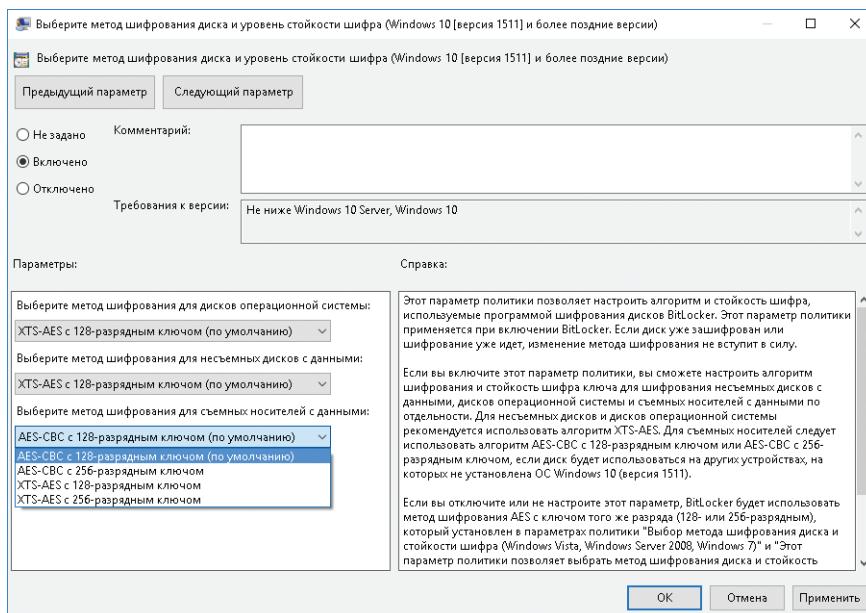


Рис. 15-8. Начиная с Windows 10 версии 1511, можно выбирать алгоритм шифрования XTS-AES с длиной ключа 256 бит. Не применяйте эту возможность на съемных дисках, которые могут использоваться с несовместимыми операционными системами