Работаем из дома?

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам информационной безопасности

В последнее время широко распространена работа сотрудников из дома. Кроме того, наблюдается частое использование домашних компьютеров (ноутбуков) на работе. И в определённой степени это становится проблемой для организации. С одной стороны, сотрудник использует домашний ПК, а с другой – отсутствует гарантия, что этот ПК соответствует политике безопасности компании, в которой он работает.

Ещё большее количество угроз несёт этот вопрос в связи с развитием облачных технологий. Ведь где гарантия, что дома у вашего сотрудника используется лицензионное ПО, установлены и вовремя обновляются операционная система, антивирус, средства защиты и тем более ПО третьих производителей? Где гарантия, что подрастающее поколение не занесло «троян» под видом каких-то «улучшений» для прохождения игр? Вопросов гораздо больше, чем ответов.

На самом деле вариантов ответа несколько:

1. **Компания покупает и выдаёт сотруднику ноутбук для работы из дома.** Вариант наиболее дорогой, но предполагается, что корпоративный системный администратор всегда может управлять этим ПК, не беспокоясь о том, что сотрудник может что-то установить либо изменить в настройках. Потому что при таком подходе прав администратора у сотрудника быть не должно. Это затратное решение, но, с другой стороны, самый правильный выход из положения.
   Примечание. К сожалению, даже такой вариант не безгрешен. Ахиллесова пята заключается в редкой необходимости менять параметры в BIOS или загружать ноутбук в режиме восстановления, например при восстановлении штатной операционной системы при сбое. Как вариант, в этом случае пользователь должен сдать свой ноутбук и получить другой.
2. **Сотрудник работает с домашнего ПК, за который сам и отвечает.** Наиболее дешёвый, но самый рискованный вариант. Ведь фактически безопасность домашнего ПК никто не контролирует! Ну и что, зато бесплатно, – скажет недалёкий руководитель. Бесплатно ли? Не знаю, не знаю. Ведь в случае проникновения «вредоноса» с домашнего ПК сотрудника отвечать придётся всё равно вам – руководителю или системному администратору. А ваши пользователи умеют настраивать свой компьютер? Вовремя ставят обновления? У них всё программное обеспечение лицензионное? Да ну! И игры тоже? И фильмы они смотрят не с пиратских сайтов и торрентов? НЕ ВЕРЮ!
3. И последний вариант, который мне нравится больше всего, – **использование технологии Windows To Go.** В этом случае вы фактически покупаете только USB-флешку или SSD (что, на мой взгляд, куда предпочтительнее, хотя вроде и дороже). На самом деле, дороже, если не смотреть на срок службы. Да, вы можете купить сотруднику и внешний жёсткий диск. Единственное пожелание – покупать его под интерфейс USB 3.0, так он будет работать куда быстрее!

Впервые технология Windows To Go появилась ещё в Windows 8. Для создания соответствующего диска использовался образ корпоративной версии Windows. Причём создать можно было как с помощью мастера (в корпоративной версии), так и руками (в версии Pro).

Бывает, что вам нужно поработать на чужом компьютере, но сделать это так, как будто вы работаете на своём! То есть сделать так, чтобы от вашей работы не осталось бы ни следа. Да-да, любому специалисту покажется, что вас на этом компьютере вообще не было!

Идеальным выходом в этом случае будет режим Windows To Go. Ведь в таком варианте операционная система Windows будет установлена непосредственно на флешку! Однако стоит учесть, что загрузочный диск вы должны подключить непосредственно к USB-порту, то есть подключение через USB-хаб работать не будет!

Естественно, ёмкость вашего флеш-накопителя должна быть не менее 32Гб, но сегодня это не проблема. Учтите, что в ходе первой загрузки на конкретном ПК вам потребуется установить все драйвера для него, поэтому загрузка будет идти несколько дольше, чем в последующем.

Вместе с тем вам придётся вспомнить, что по аналогии с работой Windows To Go, созданной под управлением Windows 8, вам будут недоступны некоторые стандартные возможности:

4. После загрузки в режиме Windows To Go вам станет недоступен жёсткий диск, так как он будет находиться в состоянии off-line.
5. При использовании шифрования BitLocker следует учесть, что Trusted Platform Module (TPM) не используется.
6. Режим гибернации отключён, и понятно почему.

Естественно, среда восстановления Windows недоступна.

Кроме того, в Windows 10, в отличие от Windows 8, создание USB-носителя для Windows To Go теперь доступно не только версии операционной системы Windows 10 Корпоративная, которая, кстати, отдельно уже не выпускается, но и в версии Windows 10 Pro. Поэтому создавать USB-диск с Windows To Go вручную, как это можно было сделать на компьютере под управлением Windows 8 Professional, по-прежнему можно, но смысла не имеет!

Мало того, создавать такой USB-носитель вручную, используя только Windows 10 Pro, можно, но в результате получим USB-носитель,

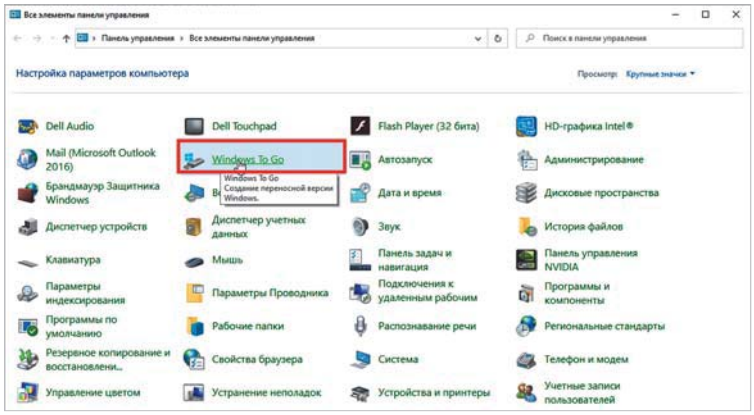

Рисунок 1. Панель управления.

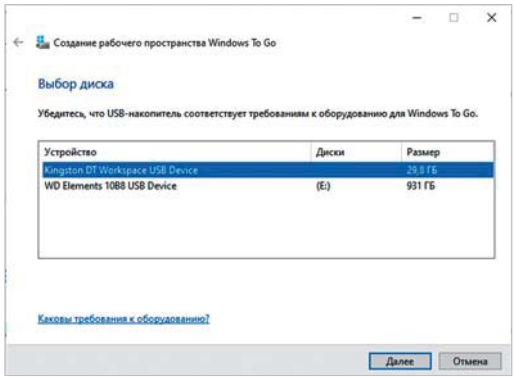

Рисунок 2. Выбор носителя.

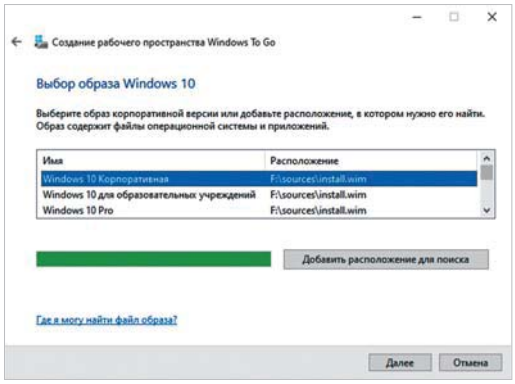

Рисунок 3. Выбор образа для Windows 10.

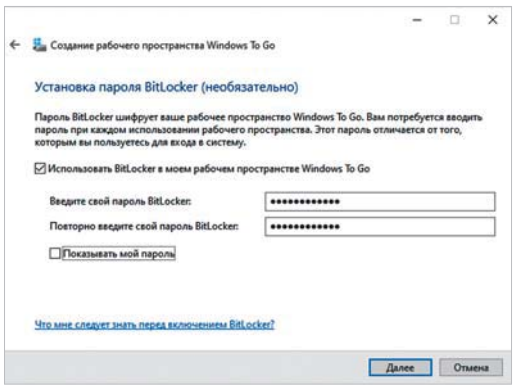

Рисунок 4. Установка BitLocker.

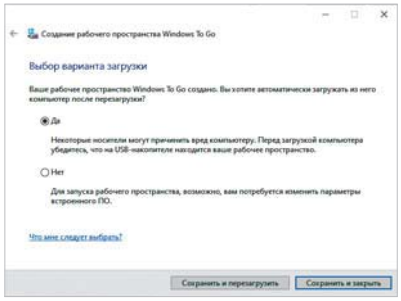

Рисунок 5. Окончание настройки

под управлением которого ваши локальные диски будут полностью видны. В некоторых ситуациях это весьма полезно, но не в случае работы в корпоративной сети из дома.

Создание носителя для Windows To Go с помощью мастера в Windows 10

Для создания диска Windows To Go вы должны войти в Панель управления. Выбрать режим отображения Крупные или Мелкие значки, а затем выбрать Windows To Go (рис. 1). После этого выберите носитель, на котором вы будете создавать Windows To Go (рис. 2). Смонтируйте Business версию ISO-файла Windows 10 и укажите этот образ как рабочее пространство, откуда будут скопированы необходимые файлы (рис. 3).

Если администратор при создании Windows To Go захочет зашифровать носитель с помощью BitLocker, то он может сразу это сделать. Учтите: так как TPM при этом недоступен, то потребуется просто дважды указать свой пароль шифрования. Помните: у вас нет возможности восстановления этого пароля.

Этот шаг является необязательным, но, если вы хотите, чтобы ваши сотрудники могли работать именно из дома, я считаю его обязательным. Ведь любой человек может потерять флешку, не так ли? А если она зашифрована, то весь ущерб от её потери равен стоимости флешки, что, в сущности, не так уж и много (рис. 4).

Не забудьте, что вы потеряете всю информацию, которая хранилась на вашем USB-носителе! Нажимаем «Создать», и ждём окончания процесса (рис. 5).

Таким образом, вместо того, чтобы морочить голову с настройкой домашнего ПК пользователя для доступа в корпоративную сеть, вы получаете зашифрованный носитель, который можно воткнуть в USB-порт и работать из дома или с любого другого «чужого» ПК. Не забудьте, что вы только что создали просто зашифрованный носитель с операционной системой. И не более. Для полноценной работы загрузитесь с такого носителя и установите на него нужное программное обеспечение, например: VPN, антивирус, удалённый доступ в вашу сеть и прочее.

Не забудьте убедиться, что ваш USB-носитель может быть загрузочным, иначе вся работа бессмысленна.

И ещё один совет. Ваш носитель должен обязательно поддерживать USB 3.0. В этом случае вы получите скорость работы не ниже, чем при работе с локального жёсткого диска, а возможно, и выше.

Согласитесь, такой вариант использования технологии существенно дешевле покупки нового ноутбука каждому, кому по тем или иным причинам потребуется работать из дома либо в командировке.