# *Д. В. Угаров, ОКБ САПР*

# Развитие парадигмы доверенного сеанса связи для использования мобильных устройств на предприятии

К BYOD можно относится по-разному: считать мыльным пузырем [1] или же необходимостью для привлечения талантливых сотрудников поколений Y и Z [2]. Однако, с фактами не поспоришь: BYOD с нами уже давно и стал неотъемлемой частью нашей работы. Часто мы его используем, сами того не замечая. Например, предоставляя доступ к электронной почте за пределами компании.

Данный подход завоевывает все большее количество сфер, среди которых обучение [3], здравоохранение и промышленность [4]. Согласно исследованиям [5] в 2016 году более 59% организаций разрешали использовать свои собственные устройства для рабочих целей, а 13% планировали разрешить в ближайший год.

Известно, что «общий уровень защищенности определяется уровнем защищенности самого слабого звена» [6], а значит и приносимые устройства это еще один элемент системы, который компаниям необходимо защищать [7].

Задавшись вопросом защиты оконечных устройств, в первую очередь сталкиваешься с MDM (Mobile Device Management) решениями, которые, во-первых, ограничены в контроле устройств [8], во-вторых явно несут ограничения для пользователей. Как бы ни убеждала компания, отдавая под контроль свое устройство, работник осознает, что его «личное» перестает быть таковым.

Как быть в таком случае? В первую очередь необходимо понимать, что без использования точки опоры в виде резидентного компонента безопасности [9] и построения доверенной среды не обойтись. VPN/Антивирусы/VDI и прочие средства в конечном счете не защитят на 100% от того, что на устройстве появится вредоносное ПО, которое сможет перехватить учетные данные для доступа к системе. Пытаясь совместись «два-в-одном» необходимо подходить к вопросу крайне скрупулёзно [10], иначе построенный «дом на песке» создаст лишь иллюзию безопасности.

Продолжив поиск решений, можно обнаружить такие продукты как МАРШ! [11], Ноутбук руководителя [12] и TrustPad [13], применение которых подразумевает доверенный сеанс связи (ДСС) [14-19]. Однако, указанная парадигма предполагает, что «далеко не все время» работник будет взаимодействовать с удаленными сервисами. В случае же BYOD, работа с корпоративными ресурсами легко может превышать 50% от проводимого за устройством. Такой характер взаимодействия приводит изменению сценариев использования решений:

1. **Использование собственных устройств не только за пределами компании, но и внутри нее**. Их возможное включение (с загруженной не доверенной средой) в сеть компании не должно подвергать опасности заражения остальных клиентов в сети.
2. Работа в компании неизбежно сопряжена с установкой новых и обновлением текущих приложений, изменением настроек системы и т. п. Это значит, что **доверенная среда должна иметь возможность изменяться со временем и механизм обновления должен быть удобным**.
3. Несмотря на растущую карту покрытия интернетом нашей планеты, связь далеко не всегда остается стабильной. Более того, часто можно встретить места, где покрытие попросту отсутствует (например, находясь в самолете или поезде – типичных ситуациях для работников использующих BYOD). Это значит, что для полноценной работы: **необходимо иметь возможность работать локально, сохраняя для этого на устройстве необходимые данные**, **при этом исключая возможность их утечки за пределы устройства, а также допуская утерю самого устройства.**

Рассмотрим по порядку, каким образом можно решить указанные задачи:

1. Указанные ранее продукты, обеспечивающие ДСС, могут использоваться внутри компании, при организации VPN в рамках самого предприятия [3,10]. Однако, просто перевести всех на VPN недостаточно. Во-первых, это никак не спасет от заражения остальных клиентов сети в случае подключения к ней СВТ с не доверенной системой. Во-вторых, в таком случае у сотрудников (не использующих мобильные устройства) на руках будут данные достаточные для того, чтобы развернуть VPN самостоятельно в не доверенной среде дома. Вопрос изоляции можно решить путем внедрения PVLAN [20], но скорее всего это потребует дополнительных вложений в сетевое оборудование. Задачу подключения из не доверенной среды можно решить путем разделения VPN на внутренний (в пределах компании) и внешний (за пределами), что очевидно неудобно. Либо выдав пользователям, задействующим только свое рабочее место, специальные устройства [21], хранящие ключи VPN внутри себя и позволяющие работать с ними только на заданных СВТ внутри защищаемого периметра. Итог: данная задача решаема продуктами представленными на рынке, но это приведет к дополнительным затратам.

Следующим возможным вариантом является выделение отдельного сегмента сети и соответствующих портов на рабочих местах для адептов BYOD. Минус этого решения в том, что оно ограничивает свободу передвижения внутри компании, что идет в разрез с самой концепцией носимых устройств.

Самым эффективным решением данной задачи будет внедрение контроля доступа к сети, на основе стандарта 802.1x [22]. Для продуктов, обеспечивающих ДСС, это потребует дополнительной поддержки в ОС и хранения аутентификационных данных на скрытом разделе устройства [3], но для компаний оно будет наиболее подходящим, так как может быть развернутым на основе существующего оборудования и не потребует изменения структуры сети.

1. Рассматриваемые решения предоставляют функцию обновления, однако его необходимо производить с каждым устройством по отдельности. В случае личного использования это обычная практика, но в масштабах предприятия становится очевидно, что такой подход неудобен. Для защищенной доставки приложений уже существует необходимое решение – ПАК Центр-Т [23]. Данный продукт позволяет распространять ПО и обновления централизованно на конечные клиентские устройства, , а так же управлять состояниями их разделов. Последнее позволяет сохранить полученное ПО на нем для повторного использования (переведя по команде от сервера Центр-Т раздел для ПО в состояние RW и после сохранения вернув его в состояние RO).
2. Управление разделами позволяет решить и задачу локальной работы с данными без необходимости постоянного подключения к удалённой системе. Для этого помимо состояний RO/RW потребуется так же добавить hidden (скрывающее раздел работы с носителем вне доверенной среды). Работа будет осуществляться следующим образом: работник загружается с собственного устройства в доверенной среде. Устройство подключается к серверу Центр-Т, получает назначенное ему ПО для локальной работы (например, офисное) и удаленного подключения к терминальному серверу. В случае указанного разрешения со стороны администратора системы, устройство также получает сигнал на активацию раздела для хранения данных локально (перевод из hidden в RW). В дальнейшем работник может работать с данными, не связываясь с системой, и при необходимости, подключившись к серверу, вновь передать документы обратно. Чтобы утрата устройства не несла опасности для компании, остается лишь шифровать указанный раздел с данными, закрыть доступ к нему PIN-кодом и разрешить работу только на определенных СВТ [24].

В результате рассмотрения новых сценариев становится понятно, что в настоящий момент решения, позволяющего работать по настоящему мобильно в соответствии с идеями, лежащими в основе BYOD, нет. Но все необходимые «кирпичи» для него есть уже сейчас, а значит новый виток развития решений для BYOD, которые мы можем считать не только безопасными, но и удобными, ждет нас уже обозримом будущем.

**Список литературы:**

[1] Мобильная зрелость крупнейших российских компаний [Электронный ресурс] URL: <http://bit.samag.ru/archive/article/1908> (дата обращения 08.04.18).

[2] *Bouk J.* Top BYOD Trends for 2018 [Электронный ресурс] URL: <http://www.casstelecom.com/blog/top-byod-trends-for-2018> (дата обращения 06.04.18).

[3] *Алтухов А. А.* Доверенный сеанс связи на службе академического процесса // Новые Информационные Технологии и Системы, Сборник научных статей XII Международной научно-технической конференции г. Пенза 23-25 ноября 2016г., C. 217–219.

[4] *Bouk J.* How BYOD is Perfect for Manufacturing [Электронный ресурс]. URL:

<http://www.casstelecom.com/blog/how-byod-is-perfect-for-manufacturing> (дата обращения 06.04.18).

[5] [*Lazar*](https://www.insight.com/en_US/learn/view-all-pages/authors/michael-lazar.html) *M.* BYOD Statistics Provide Snapshot of Future [Электронный ресурс]. URL: <https://www.insight.com/en_US/learn/content/2017/01182017-byod-statistics-provide-snapshot-of-future.html> (дата обращения 06.04.18).

[6] *Конявская С. В.* О происхождении видов, или как лечить болезнь, а не симптомы // Защита информации. Inside. Спб., 2017. № 5. С. 64–74.

[7] *Алтухов А. А.* Решение задачи безопасного использования мобильных устройств на предприятии с помощью доверенного сеанса связи // Вопросы защиты информации, 2017. № 3. С. 34–41.

[8] *Старостина Е. В., Наймарк В. Г.* Защита от информационных рисков при внедрении BYOD // Внутренний контроль в кредитной организации. 2014. № 3 (23) С. 60–65. [Электронный ресурс]. URL: <https://www.pwc.ru/ru/blogs/ekaterina_starostina/posts/assets/cpl.pdf> (дата обращения 06.04.18).

[9] *Конявский, В. А., Гадасин В. А.*Основы понимания феномена электронного обмена информацией (Библиотека журнала «УЗИ»; Кн. 2). Мн.: «Беллитфонд», 2004. — 282 c.

[10] *Конявская С. В.* Практика совмещения функций в защите информации: за и против // Вопросы защиты информации, 2017. № 3. С. 46–53.

[11] [Средство обеспечения доверенного сеанса «МАРШ!»](http://xn--80axn6a.xn--p1ai/) [Электронный ресурс]. URL: [http://марш.рф](http://www.sodsmarsh.ru/) (дата обращения: 20.04.2017).

 [12] *Счастный Д. Ю.* [Ноутбук руководителя](http://www.okbsapr.ru/schastny_2015_3.html) // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015. С. 112.

[13] В России создали защищенный от вирусов планшет. 17.06.2016. РБК [Электронный ресурс]. URL:

https://www.rbc.ru/technology\_and\_media/17/06/2016/5763ecfc9a794721da3fb33a (дата обращения: 11.04.2018).

[14] *Конявский В. А.* [Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ!](http://www.okbsapr.ru/konyavskiy_2010_1.html) // Комплексная защита информации. Материалы XV международной научно-практической конференции (Иркутск (Россия), 1–4 июня 2010 г.). М., 2010.

[15] *Каннер А. М.* [Средство организации доверенного сеанса как альтернатива доверенной вычислительной среде](http://www.okbsapr.ru/kanner_2010_4.html) // Информационные технологии управления в социально-экономических системах. Вып. 4. М., 2010. С. 140–143.

[16] *Чугринов А. В.* [Доверенные сеансы связи и средства их обеспечения](http://www.okbsapr.ru/chugrinov_2010_1.html) // Information Security/Информационная безопасность. 2010. № 4 (август–сентябрь). С. 54–55.

[17] *Конявский В. А., Чугринов А. В.* Съемный носитель информации. Патент на полезную модель № 102139. 02.2011, бюл. № 4.

[18] *Конявский В. А.* Съемный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. 27.12.2012, бюл. № 36.

[19] *Конявский В. А.* Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 20.07.2013, бюл. № 20.

[20] A quick summarized view to Private VLAN (PVLAN) [Электронный ресурс]. URL: <https://learningnetwork.cisco.com/docs/DOC-16110> (дата обращения: 11.04.2018).

[21] *Кравец В. В.* Идеальный токен // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19-21 мая 2015 г. – Минск: РИВШ, 2015. С. 114–115.

[22] IEEE 802.1X Remote Authentication Dial In User Service (RADIUS). Usage Guidelines [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc3580 (дата обращения: 11.04.2018).

[23] ПАК «Центр-Т» [Электронный ресурс]. URL: http://proterminaly.ru/center\_terminal.html (дата обращения: 11.04.2018).

[24] Секрет Особого Назначения. [Электронный ресурс]. URL: http://prosecret.ru/specsecret.html (дата обращения: 11.04.2018).