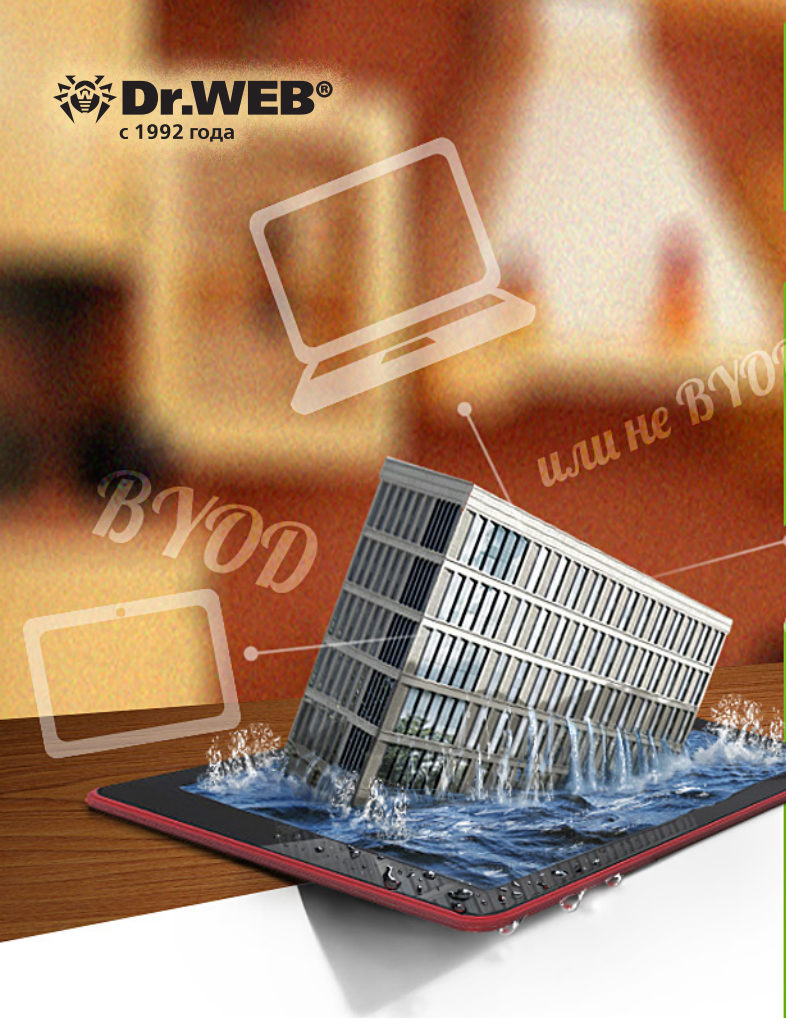
Dr.WEB®
с 1992 года



BYOD

Памятка ответственного сотрудника

Изучите памятку сами
и отправьте ее своим коллегам.

ООО «Доктор Веб», 2013

Оторвались

Сегодня большая часть устройств, находящихся в пределах помещений компании, ей не принадлежит — это собственность сотрудников — их ноутбуки, планшеты и смартфоны. Увлеченные сотрудники работают не только в рабочее время, но также в дороге и дома. Они нередко жертвуют часами отдыха, постоянно находясь на связи. И бизнес с удовольствием использует преимущества таких перемен. А еще во многих компаниях сотрудники работают удаленно.

Использование на работе личных компьютеров и смартфонов / планшетов получило особое название: **BYOD** (от английского *bring your own device* — принеси свое личное устройство).

BOYD = Идеальный сотрудник?

Сотрудники компаний, использующие на работе собственные ноутбуки и смартфоны, отличаются от тех своих коллег, которые пользуются только офисными компьютерами.

- Они работают в год в среднем на 240 часов больше, чем остальные и всегда на связи — в выходные, в праздники и во время отпуска.
- А еще можно экономить на загрузке фильмов и других тяжелых файлов, скачивая их на компьютер через корпоративную сеть, а не через домашнего провайдера...
- И чем они занимаются на самом деле на своем устройстве – знают только они сами...

Нести или не нести?

Удивительно, но подавляющее большинство руководителей компаний разного уровня одобряют BYOD!

Однако, посмотрим на статистику – **до 70% заражений компьютеров локальной сети происходят с принадлежащих сотрудникам устройств** — в том числе, принесенных ими из дома.

Почему происходят заражения компьютеров локальных сетей с личных устройств?

Признайте, вы ведь тоже это делаете?

- Используете USB-устройства, не проверяя их на вирусы?
- Открываете почтовые сообщения с вложениями от неизвестных отправителей?

Дата создания 9 апреля 2013 г.

- Путешествуете по Интернету вне рабочих целей в рабочее время?
- Работаете в Windows с правами администратора?
- Используете простые пароли, подбор которых не составляет труда?
- Не обновляете программное обеспечение, установленное на ПК?

И это еще не все! До 60% личных устройств россиян (в части мобильных устройств эта цифра значительно выше) вообще не имеют средств антивирусной защиты. А ведь именно они являются источниками вредоносных файлов и отличным плацдармом для проникновения хакеров в сетевую инфраструктуру компании в обход всех средств защиты.

Парадокс, но заражения локальных сетей компаний с личных устройств сотрудников происходят, в том числе, из защищенных антивирусом систем!

Даже если устройство и/или установленное на нем ПО принадлежит компании, но используется сотрудником за ее пределами — на выезде или для удаленной работы — компания чаще всего не контролирует, как используется устройство, работают или отключены средства безопасности, какие приложения устанавливает сотрудник, какие обновления проводит, какие сайты посещает, кому разрешает работать со своим устройством.

Сотрудники компаний являются отличными специалистами в своей области, но единицы из них являются экспертами в сфере информационной безопасности.

В результате компании оказываются незащищенными от утечек/хищений паролей и заражений корпоративной сети.

Отдельно стоит сказать об угрозах мобильного BYOD. Границы между мобильными устройствами и десктопами давно стерты — по мощности и функциональности планшеты и смартфоны уже почти не уступают офисным ПК.

Они обладают функционалом, несущим еще больше угроз для своего владельца:

- возможностью отслеживать местоположение владельца устройства;
- возможностью записывать переговоры и фотографировать участников встреч;
- возможностью высылать информацию с захваченного устройства на электронные адреса заинтересованных лиц.

«А у нас только директор BYODится, у него наверняка все в порядке с безопасностью».

В 2010 году Комиссия по ценным бумагам и биржам установила, что более половины сотрудников госучреждений и компаний США, пойманные за

просмотром материалов порнографического характера, оказались представителями **старшего руководящего персонала**.

Заражение личных устройств руководства компании и финансовых работников представляет особую опасность, так как с их устройств, как правило, есть доступ к системам дистанционного банковского обслуживания.

Помните:
для кражи ВСЕХ средств компании троянцу достаточно 1–3 минут!

Что делать?

Если руководство вашей компании благосклонно относится к использованию вами личного устройства в служебных целях — скорее всего, вы работаете в современно мыслящей компании.

Использование в вашей компании явления BYOD налагает на сотрудников определенную социальную ответственность, и лично ваше правильное отношение к оказанному вам доверию будет только способствовать росту благосостояния вашего предприятия.

Что можно и нужно делать, а чего нельзя делать категорически, если ваш ноутбук или смартфон служит вам не только средством развлечения, но и рабочим инструментом?

Необходимо:

1. **Соблюдать установленные в компании политики** использования личных устройств.
2. **Доверить право выбора антивируса** для вашего ноутбука или смартфона **системному администратору** вашей компании — специалисту в этой области. Желательно, чтобы офисные ПК и личные устройства сотрудников компании были защищены одним антивирусом, т.к. в этом случае они все будут администрироваться из единого центра.
3. **Завести на устройстве 2 учетные записи:** одну для личных нужд, другую для рабочих. Обе эти записи не должны быть администраторскими. Помните: вирус, попав в систему, пользователь которой использует администраторскую запись, получает равные администратору права — т.е. может в ней делать ВСЕ.

Дата создания 9 апреля 2013 г.

Например, **Dr.Web Launcher** разграничит пространство вашего устройства на личное и служебное на смартфоне под управлением Android. Дополнительно это приложение использует специальный безопасный браузер Dr.Web, который ограждает от просмотра нежелательных или потенциально опасных с точки зрения вашей компании веб-ресурсов. Это позволит вам соблюсти политику BYOD вашей компании.

4. **Отключить** на компьютере **учетную запись Гость**.
5. **Отключить на компьютере автозапуск** (зачем это нужно, вам поможет понять тест ВебIQметра «Наша тактика — профилактика»).
6. Использовать стойкие пароли для входа в учетные записи. Об опасности простых паролей расскажут тесты ВебIQметра «DoB2ff5E, или Безопасность паролей» и «PIN хакеру в помощь».
7. **Своевременно скачивать и устанавливать все обновления** и новые версии **ВСЕГО** установленного на компьютере или мобильном устройстве программного обеспечения — не только операционной системы. Для этого все используемое ПО должно быть лицензионным. Если устройство включено в корпоративную систему безопасности, необходимо использовать **систему централизованной установки обновлений** всего установленного программного обеспечения — это позволит администратору системы в режиме реального времени контролировать отсутствие известных уязвимостей на защищаемых объектах.
8. **Скачивать** и устанавливать **программы** либо **с рекомендованного компанией ресурса**, либо из **собственного хранилища приложений компании**.
9. **Использовать** для защиты устройства не просто антивирус, а **систему антивирусной защиты**, которая должна включать:
   - **Антивирус** — причем такой, который:
     - **умеет лечить** не только поступающие (неактивные) вредоносные программы, но и уже запущенные (активные), но ранее неизвестные вирусной базе;
     - **имеет стойкую систему самозащиты** — чтобы антивирус мог продержаться в зараженной системе до получения обновления и не дал вирусу возможности вывести себя из строя;
     - **имеет систему обновлений**, которая находится под контролем системы самозащиты и не использует компоненты операционной системы, которые могут быть скомпрометированы; которая позволяет мгновенно, по сигналу системы централизованного управления доставить обновления для лечения активного заражения (если устройство включено в корпоративную систему безопасности).
   - **Систему защиты доступа** (т.н. Родительский контроль)
   - **Систему защиты от спам-рассылок**

Дата создания 9 апреля 2013 г.

- **Систему шифрования данных**, а также безвозвратного их уничтожения (криптограф)
- **Систему уничтожения или блокирования информации** в случае утери или кражи устройства (антивор)
- **Возможность включения в корпоративную систему безопасности** для централизованного управления.

Отнеситесь с пониманием к тому, что эти компоненты нельзя отключать ни при каких условиях, а еще пройдите посвященный этому вопросу тест «Кашу маслом не испортить». Кстати, в системах, подключенных к централизованному управлению защитой, отключение компонентов антивируса невозможно.

10. **Удалять корпоративные данные** с помощью специальных программ, делающих невозможным их восстановление (например, такая функция есть в продукте Dr.Web Бастион Pro для ОС Windows), если:
    - вам необходимо сделать перепрошивку устройства,
    - вы решили уволиться,
    - вы решили передать / продать / подарить свое устройство (например, отдать его ребенку).

    Желательно, чтобы операцию удаления произвел системный администратор вашей компании — в случае утечки конфиденциальных данных вас не смогут обвинить в этом даже после вашего увольнения.
11. **Чтобы облегчить поиск вашего устройства** в случае его утери или похищения, запишите серийный номер устройства в блокнот и храните его дома. На мобильном устройстве используйте программу **Антивор** — она позволит удаленно заблокировать устройство и даже стереть на нем всю информацию.

Нельзя

- **Не рекомендуется** использовать ранее принадлежавшие кому-то устройства для хранения важной информации.
- **Не рекомендуется** разрешать ребенку и другим домочадцам использовать ваш ноутбук/смартфон на регулярной основе — только вы и никто другой имеете право пользоваться устройством, на котором хранится в том числе не принадлежащая вам информация.
- **Нельзя** отключать автоматические обновления антивируса — работа этого ПО как никакого другого сильно зависит от обновлений.
- Если ваше устройство включено в корпоративную систему безопасности — **нельзя** требовать от системного администратора компании отключать обновления и регулярные сканирования.
- Если вы используете устройство для проведения платежей через систему дистанционного банковского обслуживания — **не рекомендуется** использовать это устройство для других целей.

Дата создания 9 апреля 2013 г.

Защита без границ

Только обеспечив защищенность всех устройств, на которых работает персонал, можно **гарантировать**, что с личных компьютеров и мобильных телефонов вредоносные программы не попадут в корпоративную сеть.

Эффективные решения, позволяющие организовать качественную защиту любых устройств, имеющих доступ в корпоративную сеть — как принадлежащих самой компании, так и ее сотрудникам лично, — есть и у компании «Доктор Веб». Это комплекс продуктов для защиты всех узлов корпоративной сети **Dr.Web Enterprise Security Suite**.

Dr.Web Enterprise Security Suite позволяет из единого центра управлять защитой и сети компании, и домашних компьютеров сотрудников, и мобильных устройств — где бы ни хранилась конфиденциальная информация, она не останется без защиты. При покупке лицензии для защиты для рабочих станций, защита мобильных устройств компании предоставляется **бесплатно**.

Организация единой защитной экосистемы несет множество выгод для компаний:

- Лояльность сотрудников. Антивирус в подарок — это отличный бонус!
- Удешевление и систематизация защиты.
- Возможность контроля любых защищенных машин из единственной точки.
- Возможность работы сотрудников в любом месте мира с равной защищенностью.
- Гарантия безопасности данных (в том числе персональных) в любой момент времени.
- Снижение простоев по причине заражения.

Полезные ссылки

- Тесты о безопасности.
- Видео по настройке Dr.Web Enterprise Security Suite для защиты мобильных устройств сотрудников.
- Запрос доступа к сервису онлайн-тестирования Dr.Web Enterprise Security Suite.

125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Телефон: +7 (495) 789–45–87 (многоканальный)
Факс: +7 (495) 789–45–97