



При переходе к корпоративным мобильным технологиям организации, чтобы остаться конкурентоспособными в мобильную эпоху, должны адаптировать свои бизнес-стратегии к новым условиям. Однако внедрить и поддерживать мобильные технологии в актуальном состоянии непросто: переход к корпоративным мобильным решениям требует значительных изменений в приоритетах организации и ее бизнес-процессах.

Применение мобильных технологий позволяет ускорить и облегчить последние, что ведет к повышению их эффективности. С другой стороны, за «мобилизацией» бизнес-процессов организации кроются различные риски и угрозы, которые необходимо соотносить с перспективами и выгодами, получаемыми при их внедрении.

В представленном пособии рассмотрены основные составляющие проблемы обеспечения безопасности мобильных технологий в корпоративном секторе. В нем не только собран и систематизирован огромный объем материала по использованию мобильных решений в госорганах и корпоративном сегменте, но и приведены текущие и перспективные подходы, направления и тенденции развития мобильных технологий в корпоративном секторе в части обеспечения информационной безопасности, даны взвешенные оценки рисков различных сценариев их использования.

Изложенный материал предназначен для ИТ- и ИБ-менеджеров российских компаний и организаций любого масштаба и форм собственности.

Введение

Глава 1. Предметная область

Глава 2. Концепции использования мобильных устройств в корпоративных информационных системах

- 2.1 Корпоративное устройство, управляемое пользователем
- 2.2 «Принеси свое устройство»
- 2.3 Достоинства и недостатки концепций COPE и BYOD
- 2.4 «Выбери свое устройство»

Глава 3. Модели предоставления мобильных услуг в корпоративном секторе

Глава 4. Виды, классификация и статистика угроз

- 4.1 Программные угрозы
- 4.2 Использование уязвимых мобильных ОС и приложений
- 4.3 Web-угрозы
- 4.4 Сетевые угрозы
- 4.5 Физические угрозы
- 4.6 Угрозы мобильных устройств для организации
- 4.7 Пользовательские угрозы
- 4.8 Угрозы со стороны поставщика услуг
- 4.9 Статистика угроз

Глава 5. Общие меры обеспечения безопасности мобильных устройств

Глава 6. Методы обеспечения безопасности в мобильных ОС

- 6.1** Контейнер или «песочница»
- 6.2** «Двойной профиль»
- 6.3** Кодовый контейнер
- 6.4** Упаковка приложений
- 6.5** Виртуализация

Глава 7. Технологии и функции управления мобильными устройствами и обеспечения их безопасности

- 7.1** Управление мобильными устройствами
- 7.2** Управление мобильными приложениями
- 7.3** Управление мобильными данными
- 7.4** Управление мобильными сотрудниками

Глава 8. Корпоративные мобильные приложения

Глава 9. Управление корпоративными мобильными технологиями

Глава 10. Корпоративная политика безопасности мобильных технологий

Глава 11. Мобильные технологии как элемент бизнес-процессов организации

- 11.1** Правила мобильной политики
- 11.2** Особенности внедрения мобильных технологий в организации
- 11.3** Практические подходы к внедрению мобильных технологий
- 11.4** Мобильное обслуживание клиентов

Глава 12. Национальная мобильная платформа

Глава 13. Проектирование мобильных бизнес-процессов и обеспечение их безопасности

Заключение

Список терминов и сокращений



Дополнительные материалы: публикации из журнала «Защита информации. Инсайд»