УДК 004.72.056.52:334
DOI: 10.15587/2313-8416.2014.31881

ОСНОВНІ ПРИНЦИПИ ТА ПРАВИЛА ВПРОВАДЖЕННЯ MOBILE DEVICE MANAGEMENT І BRING YOUR OWN DEVICE У РОБОТУ СУЧАСНОГО ПІДПРИЄМСТВА

© О. О. Мартинюк

Розглянуто основні принципи Mobile Device Management (MDM) і Bring Your Own Device (BYOD) та правила їх впровадження в роботу сучасного підприємства. Проаналізовано умови запобігання витоку корпоративної інформації під час використання мобільних пристроїв. Вивчено призначення, налаштування параметрів безпеки та основні можливості програмних продуктів компаній McAfee та Websense в процесі використання мобільних пристроїв у корпоративній мережі
***Ключові слова**: мобільні пристрої, політика безпеки, MDM, BYOD, McAfee, Websense, витік корпоративної інформації*

Main principles and rules of implementation of Mobile Device Management (MDM) і Bring Your Own Device (BYOD) to nowadays business were described. Conditions of prevention confidential information leakage caused by using mobile devices were analyzed. Appointment and settings of security parameters and main opportunities of McAfee and Websense software during using of mobile devices in corporative network were explored
***Keywords:** mobile devices, security policy, MDM, BYOD, McAfee, Websense corporative information leekage*

1. Вступ

Сучасна корпоративна мережа обмежується не лише стаціонарними обчислювальними станціями, але й включає в себе мобільні пристрої типу планшетів, ноутбуків, смартфонів тощо. Їх використання значно спрощує обробку даних, дозволяє не прив'язуватись до робочого місця та є досить зручним, наприклад, під час відряджень чи на зустрічах за межами офісу тощо. Для того, щоб правильно побудувати політику безпеки для таких пристроїв у корпоративній мережі було розроблено ряд принципів, об'єднаних під назвою BYOD (Bring Your Own Device). Для полегшення роботи адміністраторів низка компаній розробили пакети спеціалізованого програмного забезпечення типу MDM (Mobile Device Management). Аналіз методики BYOD та двох конкретних програмних розробок, що розглянуто у статті, дозволяє детальніше визначити недоліки та переваги сучасних методів введення мобільних пристроїв у корпоративну мережу й оцінити функціональні можливості вже готових програм для управління ними.

2. Постановка проблеми

Сучасний розвиток інформаційно-комунікаційних технологій досягнув такого рівня, при якому немає необхідності знаходитись на робочому місці, щоб вийти в мережу Інтернет, опрацювати певні дані чи переслати їх. Наявність безпровідних мереж, а також зростання обчислювальних можливостей мобільних пристроїв, поставили смартфони та планшети на один рівень із персональними комп'ютерами. Більше того, люди постійно використовують їх для спілкування, щоденної роботи та навіть розваг. Тому не дивно, що з часом такі пристрої все частіше стали використовувати для обробки та збереження даних користувача, що стосуються його трудової діяльності. Користувачі без вагань підключають свої пристрої до корпоративної мережі, зберігають та обробляють інформацію, готують презентації, пересилають дані та спілкуються у соціальних мережах. Це надзвичайно зручно, якщо враховувати темп життя сучасної людини.

Проте така безпечність може дорого коштувати. Втрата мобільного пристрою виявиться невеликою проблемою, в порівнянні із небезпеками, пов'язаними із доступом до Інтернету через безпровідні корпоративні мережі. Зловмисники вигадують все більше й більше способів доступу до конфіденційної інформації, яка зберігається на мобільному пристрої. І навіть якщо такої інформації на ньому немає, мобільний пристрій може стати зручним способом для доступу до корпоративної мережі. Тому перед початком використання таких засобів, необхідно, по-перше, оцінити доцільність такого кроку, по-друге, правильно побудувати політику безпеки у мережі та проінформувати співробітників про безпеку під час роботи з ними.

Провідні закордонні компанії уже активно застосовують принципи BYOD у свої діяльності. Проте в Україні використання мобільних пристроїв в корпоративних цілях або повністю заборонено, або ж допускається із недотриманням норм безпеки. Адже працівники часто самі не бажають встановлювати програми-агенти та відкривати доступ до свого пристрою адміністраторові. Тому важливо, щоб фахівці, які займаються корпоративною діяльністю чи обслуговують корпоративні мережі, були ознайомлені із принципами введення мобільних пристроїв у діяльність працівників компаній та на конкретному прикладі MDM-програм могли оцінити широкий спектр їхніх можливостей. Така інформованість дозволить пришвидшити процес введення мобільних пристроїв у діяльність компаній, а також зменшити ймовірність нанесення збитків.

3. Аналіз досліджень та публікацій

Захист мобільних пристроїв в корпоративній мережі – проблема досить нова, хоча принципи впровадження мобільних пристроїв у роботу великих компаній з метою полегшення та покращення якості роботи працівників з'явились порівняно давно. Вперше термін BYOD було згадано в статті Р. Балагаса та Дж. Шеридана в 2005 році [9]. У 2009 році, компанія Intel звернула увагу на те, що її працівники масово використовують свої пристрої в корпоративній мережі. Проте BYOD не набув великої популярності, доки до його розповсюдження не залучились Unisys, VMware і Citrix Systems, що відбулось у 2011 р. Через рік Комісія рівності при працевлаштуванні у США прийняла політику BYOD [3].

Ці принципи мають місце, якщо працівник втрачає свій мобільний пристрій, що використовував для роботи в компанії, або ж він припиняє в ній працювати, оскільки всі додатки та інформація залишаться в нього на пристрої, бо компанія не має права вилучити його власний пристрій [5]. Однак лише близько 20 % працівників погоджуються, аби їхня робота із мобільними пристроями в корпоративній мережі обмежувалась принципами BYOD [8].

Згідно з результатами досліджень, що проводились на замовлення компанії TrendMicro, безпека близько половини компаній постраждала від підключення мобільних пристроїв до своєї мережі. Проте, як свідчать дослідження Forrester Research, близько 70 % компаній збільшили свій прибуток саме завдяки використанню BYOD [1]. Принципи BYOD вирішують проблеми безпеки мобільних пристроїв лише в поєднанні із засобами віртуалізації, контейнеризації та управління мобільними пристроями (MDM). MDM включає в себе додатки, налаштування конфігурації та дані, що стосуються смартфонів, планшетів, захищених комп'ютерів, принтерів та інших мобільних пристроїв, що можуть належати компанії або працівнику [7]. Виходячи із публікації М. Фіннерана – провідного спеціаліста з безпеки безпровідних мереж dBrn Associates – MDM може скоротити витрати на підтримку та бізнес ризики, а також зекономити витрати та час простою шляхом оптимізації функціоналу й безпеки мережі мобільного зв'язку [6]. Таким чином, впровадження BYOD для корпорації може не стати важким тягарем для безпеки даних, якщо паралельно використовувати і MDM.

У багатьох статтях, що присвячені мобільній безпеці, автори наголошують на тому, що використання BYOD в діяльності корпорації та впровадження MDM-систем передбачає наявність у компанії якісно налаштованої внутрішньої мережі, захищеного сервера для збереження корпоративних даних, або ж можливостей для використання хмарних технологій. Не менш важливим є також проведення ознайомлювалюної роботи із працівниками, аби вони розуміли необхідність захищати власні пристрої не лише в корпоративних, але й у власних інтересах. Тому такі компанії як Websense та McAfee пропонують розроблені пакети програмного забезпечення, для контролю пристроїв та даних, що розраховані на велику корпоративну мережу із великою кількістю користувачів [10].

На українському ринку ще небагато компаніїй застосовують системи дистанційного контролю мобільних пристроїв у своїй діяльності, не вбачаючи в цьому необхідності, або уникаючи пов'язаних із цим матеріальних витрат. Багато іноземних компаній, чиї філіали працюють в Україні, подають приклад і підтримують введення таких засобів захисту інформації.

Метою статті є аналіз та дослідження основних принципів BYOD для захисту мобільних пристроїв у корпоративній мережі та базового функціоналу програмних пакетів типу MDM на прикладі рішень компаній McAfee та Websense.

4. Основні принципи BYOD та базовий функціонал програмних пакетів типу MDM (на прикладі рішень компаній McAfee та Websense).

Використання мобільних пристроїв працівниками у бізнес-діяльності компанії є дуже важливим. Перевагами такої політики компанії є:

– збільшення швидкості та зростання якості виконання співробітниками їхніх завдань;

– швидкий доступ до централізованих корпоративних даних;

– можливість виконувати завдання поза робочим місцем;

– використання мобільних додатків компанії;

– синхронізація потоків інформації.

В Україні принцип BYOD набуває популярності серед IT-спеціалістів компаній різних видів діяльності. Проведений у Києві в 2013 році форум CISCO „Мобільність без меж" показав, що значна частина представників компаній-учасників були зацікавлені у такій концепції [4]. Проте використання персональних мобільних пристроїв на робочих місцях із можливістю доступу до корпоративних даних несе в собі багато загроз:

– втрата працівником його девайсу;

– можливі помилки працівників при пересиланні даних;

– використання працівниками даних компанії у власних цілях;

–викрадення пристрою з метою отримання інформації з обмеженим доступом;

– неякісне адміністрування мережі та неправильне налаштування політики безпеки для мобільних пристроїв;

– нерозуміння працівниками відповідальності при використанні мобільних пристроїв для роботи із корпоративними даними.

Тому очевидно, що для того, щоб використовувати принципи BYOD для діяльності працівників підприємства, необхідно зважити всі переваги та ризики. Необхідно враховувати, що інформація, яка буде доступна працівникам, наприклад у Cloud, потребуватиме захисту від несанкціонованого доступу до неї, оскільки мобільні пристрої працюють весь час і синхронізація даних може відбуватись безперервно і навіть тоді, коли

пристрій неактивний. Для протидії пов'язаним із цим загрозам необхідно правильно визначити політику доступу до об'єктів, відповідно до політики доступу в локальній мережі компанії, налаштувати додаткові сервіси для доступу до інформації, обмежити дії користувачів при роботі в корпоративній мережі. Це все потребує значних затрат, що і визначає доцільність, чи недоцільність, використання BYOD. Тобто лише при перевазі всіх позитивних наслідків використання даної концепції над ризиками та недоліками є доцільним її впровадження.

Для того, щоб полегшити введення BYOD в політику роботи компанії, можна використовувати готові програмні пакети типу Mobile Device Management, що дозволяють налаштувати політику безпеки для кожного окремого працівника чи груп працівників, а також забезпечити дистанційне управління пристроями в разі необхідності закриття на них доступу до інформації. Сценарій введення MDM такий [2]:

I. Ініціалізація.

1) Інвентаризація та аналіз необхідності користувачів використовувати мобільні пристрої.

2) Класифікація інформаційних ресурсів.

3) Визначення інформаційних ризиків та моделі загроз.

II. Розробка.

1) Розробка політики та стандарту використання мобільних пристроїв.

2) Розробка угоди із працівниками.

3) Складання угоди про рівень обслуговування.

4) Розробка регламентів захисту та управління мобільними пристроями (підключення пристроїв, обмін та збереження даних, аутентифікація користувачів, управління пристроями)

III. Введення.

1) Налаштування базових компонентів для управління

2) Підключення тестової групи користувачів та пристроїв

3) Досвідчена експлуатація механізмів управління

4) Масштабування системи

IV. Супровід.

1) Реалізація сервісу супроводу мобільних пристроїв.

2) Контроль використання мобільних пристроїв.

3) Контроль використання та дотримання корпоративних політик для мобільних пристроїв.

4) Аналіз контенту й трафіку, що генерується мобільними пристроями.

5) Моніторинг діяльності працівників.

6) Централізоване управління ідентифікаційними даними.

V. Вивід пристроїв.

1) Розробка та виконання правил виходу мобільного пристрою з корпоративної мережі (наприклад, у випадку звільнення працівника, чи заміни його пристрою).

2) Реалізація регламенту дій у випадку викрадення пристрою.

Звичайно ж, можна створювати і власний програмний продукт, що буде використовуватись у цілях компанії та враховувати особливість її діяльності. Проте це приведе до недоцільних витрат, оскільки вимоги до систем мобільного управління пристроями зазвичай схожі. Тому раціональніше використати вже готові програмні продукти, які необхідно спочатку встановити та налаштувати на сервері компанії, а потім встановити клієнти для кожного користувача.

До основних можливостей систем MDM входять:

– централізоване управління налаштуваннями мобільних пристроїв (парольні політики та шифрування);

– заборона запуску небажаних додатків;

– відключення камери та деяких засобів комунікації;

– розповсюдження додатків та оновлень;

– інвентаризація апаратних та програмних засобів на пристроях;

– механізм віддаленого очищення даних на пристрої.

Розглянемо функціональні можливості програмних продуктів на основі готових рішень від компаній McAfee та Websense.

Технологія TRITON Mobile Security компанії Websense дозволяє керувати мобільними пристроями працівників компанії за допомогою визначених індивідуальних політик безпеки протягом часу роботи пристрою. Для початку роботи необхідно зареєструвати пристрій в TRITON Mobile Security, а тоді налаштовувати політику безпеки із облікового запису на порталі Mobile Srcurity та Cloud Email Security. При вході користувача генерується PIN-код, що діє протягом однієї доби. Для кожного пристрою визначається черга завдань (Job Queue). Список зареєстрованих пристроїв та визначених для них завдань міститься у спеціальній таблиці, редагування якої дозволяє налаштовувати завдання індивідуально. Черга очищується автоматично кожні 7 діб. До першочергових завдань входять:

1) дистанційне блокування;

2) віддалене стирання;

3) видалення паролю доступу;

4) видалення та редагування профілю MDM;

5) установка та видалення профілю електронної пошти.

Налаштування політики безпеки відбувається і для корпоративних пристроїв, і для персональних. Існують політики за замовчуванням, що передбачають базовий захист. Проте адміністратор може також налаштувати індивідуальну політику. Зокрема можна вимкнути певні функції, що стосуються завантажування та встановлення додаткового програмного забезпечення на пристрій, функцій камери та шифрування. Важливими налаштуваннями профілю є ті, що стосуються роботи в iCloud, доступу до Youtube, Safari, контенту для дорослих. Для того, щоб пристрій безпечно працював з безпровідною мережею, необхідно налаштувати профіль Wi-Fi. Також передбачено гнучке

налаштування роботи із електронною поштою та VPN. Для того, щоб мати можливість дистанційно керувати пристроєм, необхідно визначити параметри дистанційного керування, що також передбачені в цьому програмному продукті. Якщо ж користувач покинув компанію, або необхідно видалити його профіль, то це відбувається в два етапи:

1) видалення клієнта на пристрої та облікового запису;

2) повернення пристрою до заводських налаштувань [11].

5. Апробація результатів досліджень

Очевидно, що цей програмний продукт передбачає широкий спектр налаштувань пристроїв працівників, частину з яких було описано вище. Недоліком TRITON Mobile Security є те, що він працює лише із пристроями компанії Apple. Хоча зараз відбувається розширення класу пристроїв, що підлягають налаштуванню, зокрема розробляється відповідне програмне доповнення для пристроїв із Android OS.

Указаного недоліку немає у пакеті програм McAfee Enterprise Mobile Management, оскільки тут передбачено функції налаштування пристроїв на базі Android, iOS та Windows Phone. Щоправда, для кожної системи визначений свій перелік налаштувань. Найгнучкішим є налаштування пристроїв з iOS. Для них можна побудувати політику безпеки при роботі із електронною поштою, заблокувати багато функціональних можливостей пристрою та доступ до контенту та програм, а також налаштувати профілі VPN та APN. Для пристроїв із операційною системою Android передбачено гнучке налаштування електронної пошти та синхронізації пристрою, обмеження доступу до функціональних можливостей та контроль роботи додатків. Крім того, можна використовувати антивірусні програми для сканування пристрою в реальному часі, підключивши для цього відповідні клієнти та налаштувавши їхню взаємодію з McAfee EMM. Набір функціональних можливостей керування для Windows Phone досить обмежений та включає лише базові функції, такі як синхронізацію пошти та налаштування паролю доступу до пристрою [12].

Важливою перевагою McAfee Enterprise Mobile Management є наявність гнучкої системи звітування, що дозволяє покращити якість контролю не лише за кожним окремим пристроєм, але й за усіма, що включені у систему.

5. Висновки

Впровадження BYOD та MDM у корпоративній мережу – це зручний спосіб полегшити роботу працівників підприємства та збільшити їхню мобільність. Проте це вимагає виконання клопіткої роботи для попередження нових ризиків, що з'являються із використанням мобільних технологій при роботі із важливою корпоративною інформацією. На ринку є досить багато програмних продуктів, що за своїм функціоналом схожі на TRITON Mobile Security та McAfee EMM. Вони дозволяють полегшити роботу адміністраторам, проте потребують додаткових затрат на встановлення та супровід. Проте необхідно враховувати усі переваги та недоліки використання мобільних пристроїв працівниками компанії.

7. Перспективи подальших пошуків у напрямку дослідження

Перспективи вбачаємо у аналізі роботи та тестуванні інших продуктів для управління мобільними пристроями в корпоративній мережі, а також у проведенні детальнішого аналізу переваг та недоліків впровадження BYOD та MDM на реальних підприємствах, або на їх моделях.

Література

1. Защита мобильных устройств и ориентированность ИТ на пользователя [Електронний ресурс] / Режим доступу: http://www.trendmicro.com.ru/technology-innovation/mobile-security-consumerization/

2. MDM и BYOD – смешать, но не взбалтывать [Електронний ресурс] / Режим доступу: http://www.volgablob.ru/blog/?p=101

3. Bring your own device [Електронний ресурс] / Available at: http://en.wikipedia.org/wiki/Bring_your_own_device

4. Тренд BYOD набирает силу в Украине [Електронний ресурс] / Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=143082

5. BYOD – Research findings released [Electronic resource] / Available at: http://cxounplugged.com/2013/01/byod-policy/

6. BYOD Requires Mobile Device Management [Electronic resource] / Available at: http://www.informationweek.om/mobile/byod-requires-mobile-device-management/d/d-id/1097576?

7. Mobile device management (MDM) [Electronic resource] / Available at: http://searchmobilecomputing.techtarget.com/definition/mobile-device-management

8. No BYOD Policy? Time to grasp the nettle [Electronic resource] / Available at: http://cxounplugged.com/2013/01/byod-policy/

9. Ballagas, R. BYOD: Bring Your Own Device [Electronic resource] / R. Ballagas, M. Rohs, J. G. Sheridan, J. Borchers. – Available at: http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf

10. When workers go mobile, your data goes mobile and your security risk goes up [Electronic resource] / Available at: http://www.websense.com/content/triton-mobile-security-features.aspx

11. McAfee Enterprise Mobility Management 11.0 Software. Product Guide [Electronic resource] / Available at: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24468/en_US/EMM_11_0_ProductGuide.pdf

12. Websense TRITON Mobile Security. Product Guide [Electronic resource] / Available at: https://www.websense.com/content/support/library/mobile/eu_help/Mobile%20Security%20End-User%20Guide.pdf

References

1. Security of mobile devices and IT user-orientation. Available at: http://www.trendmicro.com.ru/technology-innovation/mobile-security-consumerization/

2. MDM and BYOD, shake but not mix. Available at: http://www.volgablob.ru/blog/?p=101

3. Bring your own device. Available at: http://en.wikipedia.org/wiki/Bring_your_own_device

4. BYOD trend has force in Ukraine. Available at: http://www.pcweek.ua/themes/detail.php?ID=143082
5. BYOD – Research findings released. Available at: http://cxounplugged.com/2013/01/byod-policy/
6. BYOD Requires Mobile Device Management. Available at: http://www.informationweek.com/mobile/byod-requires-mobile-device-management/d/d-id/1097576?
7. Mobile device management (MDM). Available at: http://searchmobilecomputing.techtarget.com/definition/mobile-device-management
8. No BYOD Policy? Time to grasp the nettle. Available at: http://cxounplugged.com/2013/01/byod-policy/
9. Rafael Ballagas, Michael Rohs, Jennifer G. Sheridan, and Jan Borchers. BYOD: Bring Your Own Device. Available at: http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf
10. When workers go mobile, your data goes mobile and your security risk goes up. Available at: http://www.websense.com/content/triton-mobile-security-features.aspx
11. McAfee Enterprise Mobility Management 11.0 Software. Product Guide. Available at: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24468/en_US/EMM_11_0_ProductGuide.pdf
12. Websense TRITON Mobile Security. Product Guide. Available at: https://www.websense.com/content/support/library/mobile/eu_help/Mobile%20Security%20End-User%20Guide.pdf

Рекомендовано до публікації д-р фіз.-мат. наук Михайлюк В. О.
Дата надходження рукопису 25.11.2014

Мартинюк Олександр Олександрович, Фізико-технічний інститут, Національний технічний університет України „Київський політехнічний інститут”, пр. Перемоги, 37, м. Київ, Україна, 03056
E-mail: oleksandr_lutsk@ukr.net

УДК 656.225:629.463
DOI: 10.15587/2313-8416.2014.31645

МОДЕЛИРОВАНИЕ ПРОЦЕССА ОБРАБОТКИ ГРУЗОВОГО ВАГОНОПОТОКА НА ПРИГРАНИЧНОЙ СТАНЦИИ В УСЛОВИЯХ ИЗМЕНЕНИЯ ШИРИНЫ КОЛЕИ

© Д. В. Ломотько, А. Л. Обухова

Предложен подход к оценке параметров вагонопотока на приграничных станциях с изменением ширины коли. Моделирование технологии осуществлено с использованием теории систем массового обслуживания с учетом фактора сложности технологии обработки вагонопотока в подсистемах станции. Осуществлена оценка параметров системы и отдельных технологических линий, обеспе чивающих повышение показателей результативности работы – пропускной и перерабатывающей способности
***Ключевые слова**: железная дорога, пограничная станция, технологический процесс, вагонопоток, изменение ширины колеи*

An approach to the estimation of wagon cargo parameters at border stations with railway track gauge change is proposed. Technology simulation is carried out using the theory of queuing systems, taking into account the complexity factor of wagon cargo traffic processing in the station subsystems. It is made the estimation of system parameters and separate production lines that enhance the work efficiency indicators- traffic and handling capacity
***Keywords**: railway, border station, technological process, wagon cargo traffic, railway track gauge change*

1. Введение

Приграничные станции являются важнейшими звеньями, от четкости работы которых зависит равномерность и ритмичность работы международных транспортных коридоров, сроки доставки грузов, степень использования технических средств транспорта.

В частности, наиболее сложными с технологической точки зрения являются приграничные станции с изменением ширины колеи. Структуру перерабатывающих возможностей перегрузочных комплексов, расположенных на территории Львовской железной дороги, приведено на рис. 1.

Рис. 1. Структура перерабатывающих возможностей перегрузочных комплексов, расположенных на территории Львовской железной дороги, ваг/сут