Vasylenko I.A.
Ukrainian State University of Chemical Technology

STUDY OF THE BASIC PROPERTIES OF MODIFIED IRON OXIDE PIGMENTS

Summary
The basic properties of modified iron oxide pigments are studied. A comparison of the properties of modified and industrial designs of iron oxide pigments is carried out. It is proved that chemical bond occurs between the particles of goethite precipitated with modifier. It is proved that the modified materials have advantages over their industrial counterparts.
Keywords: properties, pigments, paint, heat resistance, filtration.

УДК 336.72

ЗАГАЛЬНІ ПРИНЦИПИ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ В КОРПОРАТИВНІЙ МЕРЕЖІ

Жованик М.О.
Фізико-технічного інститут
Національного технічного університету України
«Київський політехнічний інститут»

У статті розглянуто переваги та недоліки використання мобільних пристроїв у корпоративних мережах. Наведено базові заходи захисту мобільних пристроїв від втрати інформації. Визначено поняття BYOD та MDM. Вказано переваги цих методик. Описано основні принципи впровадження їх у реальне корпоративне середовище.
Ключові слова: політика безпеки, впровадження, корпоративна мережа, мобільні пристрої, BYOD, MDM.

Постановка проблеми. Поява мобільних пристроїв стала не лише переворотом у розвитку, але і кардинально змінила життя сучасних людей. Тепер немає необхідності знаходитись у офісі, чи їздити в різні міста для обговорення важливих корпоративних питань, оскільки використання сучасних мобільних пристроїв – головним чином сматфонів та планшетів – дозволило людям отримувати віддалений доступ до своїх даних та пошти, спілкуватись на відстані у реальному часі та зберігати інформацію на віртуальних носіях. Проте розширення можливостей і широкий спектр використання мобільних пристроїв призводить до появи все нових загроз. А враховуючи, що ринок саме таких пристроїв є відносно молодим, то і програмних засобів для якісного адміністрування та захисту від вірусів та витоку даних є не так і багато. В основному проблемами захисту своїх мобільних пристроїв займаються виробники, що користуються базовими засобами захисту, які передбачені в сучасних операційних системах, таких як iOS, Android, Windows Phone. Але цих засобів може бути недостатньо для якісного ведення корпоративної діяльності. Тому на сучасному ринку програмного забезпечення з'явились рішення, що дозволяють виконувати адміністрування, захист мобільних пристроїв у корпоративній мережі, та даних, які ними використовуються.

Аналіз останніх досліджень та публікацій. Згідно зі сучасними дослідженнями, ринок мобільних пристроїв уже перегнав за продажами ринок персональних комп'ютерів. Згідно з дослідженнями, проведеними IDC, близько 95% співробітників компаній вже використовують принаймні один особистий пристрій для робочих цілей. За оцінками Gartner, близько 90% компаній планують підтримувати бізнес-додатки на пристроях, що належать кінцевим користувачам, оскільки це дозволить скоротити витрати на обладнання на 40% [7]. Крім того, широке поширення мобільних пристроїв допоможе «вийти на зв'язок» із співробітником навіть після закінчення робочого дня. Наприклад, службовці зможуть переглядати електронну пошту або працювати над презентацією в свій вільний час. У США 78% офісних працівників використовують пристрої мобільного доступу в робочих цілях, 65% офісних працівників використовують мобільний зв'язок для виконання роботи. За даними експертів, в 2015 році на кожного працівника розумової праці в середньому припадає 3,3 підключених пристрої (у свою чергу в 2012 році цей показник складав 2,8 одиниці). Мобільні рішення також завоювали популярність у приватних користувачів. Згідно з останніми даними асоціації Allensbacher Computer and Technical Analysis (ACTA), в 2011 році в Німеччині 7,3 млн. чоловік планували придбати смартфон. Згідно з даними Bitkom, в 2011 році в Німеччині було продано 2,1 млн. планшетних ПК, що перевершує їх власну більш ранню оцінку в 1,5 млн. штук. «Планшетні комп'ютери – це основний сегмент ринку пристроїв. Аудиторія їх користувачів постійно зростає «, – зазначає президент «Bitkom» Дітер Кемпф [7]. Аналітики Gartner підтверджують, що ця тенденція охопить й інші країни. Згідно з їхніми прогнозами, високі темпи зростання будуть зберігатися до 2015 року, причому приблизно 326 300 000 планшетних пристроїв до того часу змінять власника. Цей процес кардинально пов'язаний з тим, що обчислювальні можливості смартфонів та планшетів стали близькими до обчислювальних можливостей стаціонарних комп'ютерів, а використання мережі та серверів дозволило обмінюватись файлами, синхронізувати пошту, проводити відео-конференції та розподіляти навантаження між мобільним пристроєм та віддаленим сервером для отримання максимальних можливостей.

Робота з мобільними пристроями і даними на мобільних пристроях пов'язана з ризиком їх втрати і крадіжки, а також з ризиком несанкціонованого доступу до них. За даними досліджень, в великих компаніях в середньому відбувається 91% крадіжок мобільних пристроїв, 53% крадіжок в офісі, 24% втрат мобільних пристроїв на корпоративних заходах, 50% користувачів зберігали персональні дані, номери банківських рахунків на мобільних пристроях та іншу конфіденційну інформацію. Статистика стверджує, що в світі викрадають в середньому 1 лептоп кожні 53 секунди. В зв'язку з цим великі компанії задумались над забезпечення захисту даних в корпоративній мережі. Тому набирає популярність тенденція (Bring Your Own Device – BYOD) – «принеси свій власний пристрій», що дає співробітникам свободу у виборі власних засобів телекомунікації. Термін BYOD з'явився досить давно (як мінімум з 2004 року). BYOD – «принеси свій власний пристрій». Дана концепція відповідає на питання «що робити з особистими мобільними пристроями співробітників при їх використанні в корпоративному середовищі». Тим не менш, вибухову популярність ця ідея знайшла порівняно недавно і в основному за рахунок активності постачальників IT-послуг та стрімкого розвитку функціоналу та різноманітності хмарних сервісів. Проте, як відзначають в «Vanson Bourne», три чверті опитаних стверджують, що BYOD принесе значні переваги тільки в тому випадку, коли є розуміння конкретних вимог користувачів і того, як необхідно розмежувати їх права. Лише 17% організацій готові брати під контроль будь-який користувальницький пристрій [7]. В цілому, респонденти назвали чотири позитивних зміни для співробітників: збільшення гнучкості робочого графіка, підвищення креативності, новаторство і більше активна взаємодія з колегами. Крім того, компанії, які дотримуються стратегії BYOD, відзначають підвищення продуктивності праці, скорочення часу на реагування на запити клієнтів і поліпшену операційну ефективність. Згідно з дослідженнями Gartner, перехід на технології BYOD може допомогти компаніям заощадити до 40% від вартості витрат на придбання та технічне обслуговування програмного забезпечення для співробітників. Використання в компанії технологій BYOD забезпечує потенційну економію на обладнанні, програмному забезпеченні, інфраструктурі, а також сприяє модернізації IT – систем та IT – підтримки [7].

Мета статті. Головною метою цієї роботи є аналіз та дослідження основних принципів захисту мобільних пристроїв в корпоративній мережі. Переваги та недоліки впровадження та застосування технологій MDM та BYOD для запобігання витоку корпоративної інформації при втраті чи пошкодженні мобільних пристроїв.

Виділення не вирішених раніше частин загальної проблеми. Коли працівник дізнається, що в організації діє система управління мобільними пристроями MDM чи BYOD, вимагаючи використовувати PIN-код або функцію віддаленого стирання, у нього може виникнути питання: до якої міри IT – персонал контролює його пристрій? Правильне впровадження MDM чи BYOD не може переступати межі приватності: IT – персонал не повинен відстежувати всі дії на особистому пристрої або зчитувати особисті дані, і цей факт слід донести до всіх службовців. MDM та BYOD дає організаціям більше контролю над особистими пристроями службовців та їх доступом до корпоративної мережі. Але кінцевою метою мобільної безпеки є всеосяжний захист даних.

Виклад основного матеріалу. Створення об'єктів інтелектуальної власності, списків партнерів і клієнтів, а також комерційних секретів потребує від компаній значних зусиль, тому одним з основних пріоритетів у їх роботі є захист цих мобільних даних за допомогою простих у використанні і легких в управлінні засобів захисту на основі політик [2].

Якщо пристрій, що належить співробітнику, використовується в робочих цілях, то виникає ряд додаткових питань, що стосуються конфіденційності користувача, контролю за пристроєм, порядку використання пристрою, політик безпеки та захисту даних, на які необхідно знайти відповідь для забезпечення захищеності комерційних даних.

У зв'язку з цим було запропоновано деякі загальні правила захисту мобільних пристроїв [2]:

1. Блокування пристрою.

При втраті мобільного пристрою необхідно блокувати пристрій паролем (стійким або з обмеженою кількістю спроб введення), після яких дані на пристрої стираються або пристрій блокується.

2. Використання криптографічних засобів.

Необхідно використовувати шифрування знімних носіїв, карт пам'яті – всього, до чого може отримати доступ зловмисник.

3. Заборона на збереження паролів в браузері мобільного пристрою.

Не можна зберігати паролі в менеджерах паролів браузерів, навіть мобільних. Бажано встановити обмеження на доступ до листування поштового та SMS, використовувати шифрування.

4. Заборона використання менеджерів паролів для корпоративних облікових записів.

Існує безліч додатків, створених для зберігання всіх паролів на мобільному пристрої. Доступ до програми здійснюється введенням майстер-ключа. Якщо він недостатньо стійкий, вся парольна політика організації компрометується.

5. Заборона на установку ПЗ з неперевірених джерел.

Бажано використовувати ПЗ відомих розробників.

6. Використання корпоративних політик та засобів антивірусного захисту.

Якщо це можливо, дозволить уникнути безлічі загроз (в тому числі нових), а в разі втрати або крадіжки пристрою, здійснити його блокування і знищення даних на ньому.

7. Обмежити список даних, які можна передавати через хмарні сервіси.

Сучасні мобільні пристрої і додатки орієнтовані на використання безлічі хмарних сервісів. Необхідно стежити, щоб конфіденційні дані і дані, які стосуються комерційної таємниці, не були випадково синхронізовані або відправлені в один з таких сервісів.

Для полегшення управління мобільними пристроями працівників компаній було сформовано та запропоновано принципи побудови політики захисту мобільних пристроїв «Bring Your Own Device» та «Mobile Device Management». Вони включають в себе вище вказані правила захисту мобільних пристроїв, а також враховують особливості введення корпоративної діяльності.

Mobile Device Management (MDM) – «управління мобільними пристроями». Використання рішень класу MDM дозволяє здійснити управління і контроль над різними типами мобільних пристроїв.

MDM – це технологія управління всіма мобільними пристроями, а технологія BYOD – орієнтована на специфіку управління пристроями співробітників в корпоративному середовищі. BYOD ближче до тактичного і в деяких аспектах стратегічного рівня управління інформаційними технологіями та

інформаційною безпекою, тоді як MDM передбачає прикладну технічну реалізацію, і знаходиться скоріше на операційному рівні [5].

В загальному випадку системи типу MDM – це допоміжне програмне забезпечення, що дозволяє управляти мобільними пристроями на кожному етапі життєвого циклу, від ініціалізації до виводу з експлуатації [6]. Одна із головних задач MDM – досягнення оптимального стану між безпекою і зручністю використання мобільних пристроїв, при мінімізації затрат на обслуговування. Це досягається за рахунок таких можливостей систем типу MDM [3]:

· Централізоване управління мобільними налаштуваннями (парольні політики, параметри шифрування);

· Заборона запуску небажаних додатків;

· Інвентаризація програмних та апаратних засобів на мобільних пристроях;

· встановлювати політики безпеки, сертифікати безпеки і паролі на пристроях користувачів;

· налаштовувати WiFi і VPN відповідно до корпоративних стандартів;

· інсталювати мобільні додатки, вести чорний / білий список програм;

· надавати віддалену підтримку користувачів;

· віддалено блокувати пристрій і знищувати корпоративні дані в разі його втрати або крадіжки;

· налаштовувати обмеження для пристроїв, наприклад, заборона передачі даних в роумінгу, відключення камери, використання USB, Bluetooth, магазинів додатків (AppStore, Google Play та ін.);

· контролювати відповідність пристрою встановленим корпоративним політикам;

· виконувати резервне копіювання і шифрування даних на пристроях;

· здійснювати групову підготовку, конфігурування та обслуговування пристроїв.

Виходячи з функціональних можливостей систем типу MDM було запропоновано загальний сценарій впровадження MDM [5]:

1. Ініціалізація, до якої входять такі етапи – інвентаризація, аналіз потреб користувачів в частині використання пристроїв та інформаційних ресурсів, класифікація інформаційних ресурсів, визначення інформаційних ризиків і моделювання загроз.

2. Розробка

Розробка політики та стандарту застосування мобільних пристроїв та розробка регламентів захисту і управління мобільними пристроями.

3. Впровадження

Налаштування базових компонентів управління, дослідна експлуатація механізмів управління, масштабування системи.

4. Супровід

Реалізація сервісу супроводу мобільних пристроїв, контроль використання мобільних додатків, контроль застосування і дотримання корпоративних політик для мобільних пристроїв, моніторинг діяльності користувачів.

5. Вивід пристроїв з обігу

Розробка та виконання правил утилізації мобільного пристрою, реалізація регламенту дій у разі крадіжки або втрати мобільного пристрою.

З іншого боку, рішенням питання забезпечення політики безпеки інформації в корпоративній мережі є впровадження технології BYOD. Системи типу BYOD – це програмне забезпечення, яке управляє доступом до мережі користувачів, що підключаються до різних мережних пристроїв (точки Wi-Fi, комутатори, VPN концентратори). І залежно від того, чи знаходиться користувач в інтернеті або всередині мережі, це програмне забезпечення встановлює відповідний профіль із заданими правами [4]. А інтелектуальна мережна інфраструктура виконує завдання з реалізації прав доступу для кожного конкретного користувача. Основою ж для застосування такого сучасного підходу є розробка корпоративних політик використання особистих пристроїв [4]. Для коректного забезпечення такого підходу, системи типу BYOD мають такі можливості [1]:

· Плавне розміщення з використанням автоматичної реєстрації і створення профілю пристрою забезпечує збереження рівня продуктивності користувача.

· Конвергентне управління для провідних і безпровідних мереж, клієнтських пристроїв.

· Оптимізоване планування ресурсів з повним відстеженням трафіку і дій користувачів при використанні концепції BYOD.

· Повна масштабована продуктивність провідних і безпровідних мереж.

· Модульна система прямого управління дозволяє додавати ресурси і функції в міру необхідності.

Маючи такі функціональні можливості, технологія BYOD має такий сценарій впровадження в корпоративну мережу [5]:

1. Планування (проектування)

Визначення стратегії BYOD, розробка корпоративної політики, інвентаризація, аналіз потреб користувачів в частині використання пристроїв та інформаційних ресурсів, моделювання загроз інформаційної безпеки,розробка регламенту управління ризиками, розробка регламенту реагування на інциденти безпеки, розробка нормативних документів, що розмежовують сфери відповідальності співробітників і організації при використанні персональних пристроїв, розробка стандарту щодо застосування особистих пристроїв в корпоративному середовищі.

2. Впровадження

Впровадження централізованих механізмів управління персональними пристроями співробітників, інтеграція централізованої системи управління з діючими інфраструктурними та прикладними системами і засобами захисту, навчання персоналу.

3. Контроль (періодичний аудит)

4. Супровід, модернізація – робота служби технічного супроводу.

Відповідно до цього можна виділити ключові переваги систем типу BYOD [1]:

· Ідентифікація, управління мережею і доступом до додатків для будь-яких користувацьких пристроїв.

· Безпека доступу до мережі і додатків незалежно від місцезнаходження.

· Організація провідних і безпровідних мереж з використанням єдиного інтерфейсу прямого управління.

· Спрощення проектування мереж для забезпечення масштабованості провідних і безпровідних локальних мереж.

· Забезпечення доступу для мобільних пристроїв до мультимедійного вмісту.

Висновок і пропозиції. В цілому, можна зробити висновок, що при сучасному розвитку інформаційних технологій та широкому використанні мобільних пристроїв, обидва рішення надають широкий набір можливостей по управлінню мобільними пристроями, що використовуються у корпоративній діяльності. Зокрема, вони дозволяють керувати доступом до пристрою, синхронізувати передачу та отримання даних, обмежити доступ до інформації, функцій та додатків, надають адміністратору зручний користувацький інтерфейс, а також передбачають використання політик та завдань, що дозволяє не виконувати щоразу рутинну роботу для кожного пристрою

окремо. Але з іншого боку, перш ніж почати впровадження технологій MDM чи BYOD в корпоративній мережі, треба чітко зрозуміти, від яких нових загроз доведеться захищатися та оцінити, чи не буде впровадження цих технологій для захисту інформаційних ресурсів коштувати дорожче власне самих ресурсів. Це одне із головних питань при прийнятті рішення стосовно впровадження технологій MDM та BYOD в корпоративну мережу. Тому на даний час технології MDM та BYOD – це досить нові рішення, а зважаючи на те, що темпи використання мобільних пристроїв збільшуються в геометричній прогресії, дослідження в даній галузі будуть актуальні ще не одне десятиліття. Вирішення питання захисту мобільних пристроїв буде знаходитись на одному рівні з темпами виникнення нових технологій в галузі мобільних пристроїв. Загалом, це прості та ефективні рішення, що стосуються питань безпеки інформаційних ресурсів в корпоративній мережі, що будуть актуальні ще не один рік.

Список літератури:

1. Использование концепции BYOD и других компонентов [Електронний ресурс] – Режим доступу: http://h17007.www1.hp.com/ru/ru/ solutions/technology/BYOD/
2. Мобильная безопасность: Защита мобильных устройств в корпоративной среде [Електронний ресурс] – Режим доступу: https://xakep.ru/2011/10/13/57058/Услуги и возможности в области
3. Mobile Device Management [Електронний ресурс] – Режим доступу: http://www.lanit.ru/business/ 238/
4. BYOD (Bring your own device) [Електронний ресурс] – Режим доступу: http://www.artoint.ru/solutions/byod/
5. MDM и BYOD – смешать, но не взбалтывать [Електронний ресурс] – Режим доступу: http://www.volgablob.ru/blog/?p=101
6. Mobile Device Management. Управление жизненным циклом мобильных устройств [Електронний ресурс] – Режим доступу: http://library.croc. ru/
7. Корпоративная мобильность Bring Your Own Device – BYOD [Електронний ресурс] – Режим доступу: http://www.tadviser.ru/index.php/ (Bring_Your_Own_Device_-_BYOD)

Жованик М.А.
Физико-технический институт
Национального технического университета Украины
«Киевский политехнический институт»

ОБЩИЕ ПРИНЦИПЫ ЗАЩИТЫ МОБИЛЬНЫХ УСТРОЙСТВ В КОРПОРАТИВНОЙ СЕТИ

Аннотация
В статье рассмотрены преимущества и недостатки использования мобильных устройств в корпоративных сетях. Приведены базовые меры защиты мобильных устройств от потери информации. Определено понятие BYOD и MDM. Указано преимущества этих методик. Описаны основные принципы внедрения их в реальную корпоративную среду.
Ключевые слова: политика безопасности, внедрение, корпоративная сеть, мобильные устройства, BYOD, MDM.

Zhovanyk M.O.
Institute of Physics and Technology
of National Technical University of Ukraine
«Kyiv Polytechnic Institute»

THE GENERAL PRINCIPLES OF THE PROTECTION OF MOBILE DEVICES ON THE CORPORATE NETWORK

Summary
The article examines the advantages and disadvantages of using mobile devices in corporate networks. Basic protections from mobile data loss were shown. The concept of BYOD and MDM were determined. The advantages of these techniques were specified. The basic principles of putting them in a real corporate environment were described.
Keywords: security policy, implementation, corporate network, mobile devices, BYOD, MDM.