УДК 004.056.5 **doi: 10.26906/SUNZ.2019.3.131**

К. В. Нечволод[1], О. В. Сєвєрінов[1], А. В. Власов[2]

[1] Харківський національний університет радіоелектроніки, Харків, Україна
[2] Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

АНАЛІЗ БЕЗПЕКИ ДАНИХ В EMM СИСТЕМАХ

Предметом дослідження в статті є аналіз методів, що забезпечують безпеку корпоративних даних та порядок доступу до них за умови використання систем керування власними пристроями в корпоративних цілях - EMM (Enterprise Mobility Management) систем. **Мета роботи** – розгляд та порівняння різних існуючих EMM систем, дослідження їх характеристик та можливостей. В статті вирішуються наступні **завдання**: розгляд задач, структури та складових функцій EMM систем, визначення їх переваг та недоліків, аналіз найпопулярніших EMM систем. Отримано наступні результати: розглянута структура, основні підсистеми, переваги та недоліки систем керування власними пристроями, проаналізовані найпопулярніші програмні EMM системи. **Висновки**: Проведений аналіз основних концепцій побудови EMM системи в цілому та найпопулярніших представників ринку систем керування мобільними пристроями показав, що вибір однієї з них залежить від напрямків діяльності організації, операційної системи та фірми виробника пристроїв, що використовуються співробітниками в професійної діяльності. Застосування EMM систем для ведення бізнесу можна назвати цілком оправданим однак лише при коректному налаштуванню та впровадженню цих систем.

Ключові слова: EMM система, BYOD система, віддалене керування мобільними пристроями, захист корпоративної інформації.

Вступ

Постановка проблеми. В даний час все більше особисті мобільні пристрої, такий як смартфон, планшет чи ноутбук, використовуються не тільки для повсякденних цілей, а в тому числі і для виконання завдань професійної діяльності. Однак користуватися ними в робочих питаннях буває досить складно, або взагалі неможливо через встановлені політики безпеки в організаціях. Тому на початку XXI сторіччя було запропоновано використання нової IT-політики, яку назвали Bring Your Own Device (BYOD), або «візьми свій власний пристрій». Але найбільшої популярності ця концепція досягла лише в 2010-х роках за підтримки таких компаній як Intel, Citrix Systems та Unisys [1–17].

Першою реалізацією цієї політики стали Mobile Device Management (MDM) системи, які включали набір сервісів та технологій, що забезпечували контроль та захист мобільних пристроїв, які використовує організація та її співробітники. Керування мобільними пристроями переслідує дві задачі: забезпечення безпеки корпоративної інформації на пристроях, які знаходяться поза мережевої інфраструктури, а також контроль за станом самих пристроїв. Одними з найпоширеніших проблем, з якими стикається більшість компаній є такі: втрата або крадіжка мобільного пристрою; атаки на пристрої, які вже утилізуються; вірусні атаки; фішингові атаки; автоматичне завантаження недозволених додатків; атаки через небезпечні мережі. Ці загрози можуть впливати на такі активи компанії, як особисті данні, інтелектуальна власність підприємства, фінансові активи, справність та доступність пристроїв та сервісів. Захист від цих загроз і є призначенням MDM систем.

Еволюцією MDM систем стали Enterprise Mobility Management (EMM) системи, які включали окрім MDM також і Mobile Identity Management, Mobile Application Management, Mobile Content Mamgemet системи [1, 18].

Метою статті є аналіз можливостей та недоліків EMM систем, виявлення можливих погроз при їх застосуванні.

Виклад основного матеріалу

Загальна структура системи. В першу чергу призначенням EMM систем є корпоративне керування, безпека та контроль мобільних розрахунків. Система охоплює усі процеси і політики на всіх мобільних пристроях, які являються частиною або основними елементами бізнес-процесів. Сфера діяльності EMM в основному направлена на безпеку, інтеграцію додатків та керуванні, а також на фінансові наслідки таких рішень.

При використанні EMM систем корпоративна політика повинна гарантувати, що додаток буде інтегровано і він може бути використаним на мобільному пристрої, водночас повинні забезпечуватися необхідні механизми безпечного доступу. Крім того організація повинна контролювати і керувати усіма процесами, пов’язаними з бізнесом та фінансовими расходами, пов’язаними з використанням таких рішень пристроям які можуть належати організації або співробітнику. Таким чином, EMM система - це набір людей, процессів і технологій, зосереджених на керуванні мобільними пристроями, бездротовими мережами та іншими сервісами мобільних обчислень в контексті бізнесу. Для досягненя розділення особистої та корпоративної інформації в мобільному пристрої застосовуються методи:

1) управління мобільними додатками (Mobile application management, MAM) - управління пристроями на рівні додатків. Наприклад, налаштування їх доступу до інформації;

2) управління мобільною ідентифікацією (Mobile identity management, MIM) - функціонал, що обмежує використання мобільного пристрою. Наприклад, призначення ролей користувачів;

3) управління мобільним контентом (Mobile content management, MCM) - повний контроль на

рівні корпоративного контенту. Може включати в себе обмеження копіювання і вставки, доступу до репозиторіїв бізнес-контенту. Майже завжди є частиною EMM системи;

4) управління мобільним пристроєм (Mobile device management, MDM) - система, що працює на рівні мобільного пристрою та забезпечує повний доступ до всіх його можливостей.

Не дивлячись на те, що усі методи розділення особистої та бізнес інформації мають одну й ту ж саму мету, а саме захист корпоративних додатків та інформації, підходи їх реалізації можуть розрізнюватись [18–20].

EMM система потребує, що на пристрої обов'язково створюється додатковий простір для збереження корпоративної інформації (рис. 1) [18]. Це дозволяє досягти розподілення контенту на персональному девайсі користувача, що забезпечує безпеку. Реалізація цієї функції може бути різною та напряму впливати на рівень захищеності від атак. Вона дозволяє забезпечувати різні механізми безпеки такі як: завантаження оновлень контенту напряму до захищеного контейнера; обмеження доступу до даних в контейнері в залежності від часу або місцю розташування пристрою; дистанційне видалення даних в контейнері.

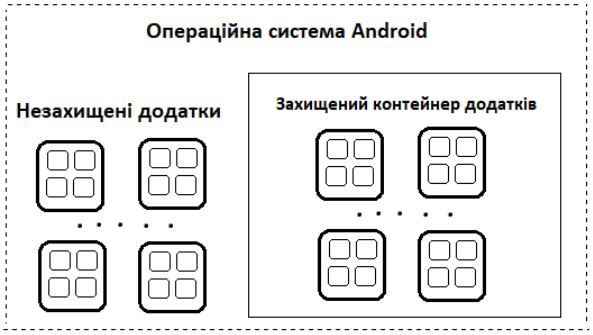

Рис. 1. Розділення даних в EMM системі

Переваги та недоліки системи. До переваг EMM систем можна віднести те, що організацією може контролюватися використання співробітниками їх пристроїв в робочій мережі.

Підвищується ефективність комунікацій співробітників організації, покращується якість забезпечення корпоративної безпеки через те, що адміністраторам безпеки не потрібно окремо налаштовувати кожен пристрій, а політики встановлюються масово на підключені пристрої. Окрім цього, з'являється можливість доставки електронної пошти, синхронізації календаря та контактів на смартфонах, планшетах та інших персональних пристроях. Для досягнення безпеки застосовується захист каналу за допомогою віртуальної приватної мережі (VPN) і служб віддалених робочих столів.

До недоліків перш за все потрібно віднести вартість впровадження таких систем. По-друге це фрагментованість пристроїв та їх програмного забезпечення [21]. Результати аналізу фрагментованості ОС Android наведена в табл. 1. В більшості випадків цей фактор, якщо не унеможливлює, то дуже ускладнює керування, налаштування та своєчасне оновлення програмного забезпечення на всіх пристроях. Для нормального функціонування системи в цілому потрібно мати в штаті кваліфікованих адміністраторів. Деякі співробітники можуть негативно ставитись до щільного контролю збоку організації, тому можуть виникнути складнощі. Політика безпеки в компанії може взагалі унеможливлювати використання персональних пристроїв, що робить недоцільним впровадження EMM системи.

Таблиця 1 **–Фрагментованість ОС Android**

Версія	Кодове ім'я	API	Поширеність
2.3.3-2.3.7	Gingerbread	10	0.3%
4.0.3-4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.5%
4.3		18	0.5%
4.4	KitKat	19	6.9%
5.0	Lollipop	21	3.0%
5.1		22	11.5%
6.0	Marshmallow	23	16.9%
7.0	Nougat	24	11.4%
7.1		25	7.8%
8.0	Oreo	26	12.9%
8.1		27	15.4%
9	Pie	28	10.4%

Порівняння найпопулярніших систем. На сьогодняшний день на ринку існує достатньо багато EMM систем [22]. Лідером на ринку EMM систем вважається система AirWatch by VMware [23]. Ця продукція користується попитом в таких галузях як енергетика, роздрібна торгівля, перевезення та інші. AirWatch by VMware підтримується всіма актуальними операційними системами, такими як Android, IOS, Windows, MacOS. Може використовуватися для налаштувань пристроїв з Android Enterprise або Samsung Knox та складається з чотирьох підсистем:

– Mobile device management, що забезпечує можливість швидкої ініціалізації пристроїв для корпоративного використання, застосування політики безпеки та захисту корпоративних данних за умови доступу з мобільних систем;

– Mobile Application Management, що забезпечує можливість керування та встановлення або видалення окремих додатків на рівні співробітників, персональних або робочих станцій підприємства;

– Mobile Email Management, що забезпечує можливість захищеності корпоративної пошти;

– Mobile Content Management, що забезпечує можливість захищеного доступу до робочих даних.

MobileIron Platform це продукт компанії MobileIron, який є найбільш швидко розвивається у світі [24]. Він об'єднує класичний набір засобів безпеки та EMM функціоналу, таких як MDM, MAM, MCM. Також підтримує багато популярних операційних систем, що дозволяє швидко впровадити цю систему до існуючої бізнес інфраструктури. Технологічно складається з двох серверів: MobileIron VSP та MobileIron Sentry. Перший відповідає за керування системою, облік пристроїв та поширення політики безпеки на кожен

пристрій. Інший контролює підключення пристроїв, веде облік усіх спроб підключення, контролює доступ до поштового серверу. Обидва сервери можуть бути встановлені як віртуальна машина або як окремий дистрибутив.

Платформа MaaS360Cloud від IBM дозволяє керувати операційними системами – Android, IOS, Windows та MacOS [25]. Дозволяє Керувати документами, поширювати додатки. Існує можливість захисту від різних вірусних атак та компрометації пристрою, наприклад втрати або крадіжки. Забезпечує створення VPN каналу для захисту інтернет з'єднань. Також сумісний з такою технологією як Android Enterprise та Samsung KNOX. Також плюсом даного продукту є його інтеграція з іншим продуктом компанії штучним інтелектом IBM Watson.

Samsung KNOX for Enterprise є розробкою компанії Samsung, яка доступна тільки на пристроях цієї фірми виробника [26]. Це можна віднести до найголовнішого недоліку цієї системи, однак це забезпечує наявність функцій, які недоступні для інших програмних продуктів. Головними перевагами цієї системи є глибока інтеграція з «залізом» та програмним забезпеченням пристроїв, забезпечення гарантованого захисту корпоративних даних, наявності окремих VPN каналів для кожного додатка в так званому захищеному контейнері, окремому захищеному середовищу для бізнес додатків, корпоративної інформації тощо. Наявність контролю за станом пристрою, можливість повного керування адміністраторами даними на окремому пристрої. Однією з можливостей, яка виділяє цю систему від інших є можливість реєстрації пристрою в системі, налаштування на ньому усіх політик безпеки, встановлення необхідного програмного забезпечення ще до відкриття заводського пакування та першого запуску пристрою, що значно облегшує та пришвидшує імплементацію цього продукту.

Використання EMM систем не може вберегти пристрій від втрати, або крадіжки, але вони дозволяють мінімізувати ризики, які можливі при даних випадках. Однією з основних можливостей є віддалене керування, видалення усіх даних. Можливе навіть блокування доступу до робочої зони, якщо зловмисник знає пароль доступу. Для захисту від досліджень зловмисниками утилізованих пристроїв в системі обов'язково застосовується шифрування усіх важливих даних. Для захисту від встановлення небезпечного програмного забезпечення застосовуються механізми налаштувань прав на пристрої. Наприклад, адміністраторами можливе блокування встановлення будь-яких програм, окрім програм з офіційного магазину додатків, який керується організацією. Крім того, деякі системи постійно моніторять стан системи і виявляють будь-яке вторгнення, що забезпечує гарантію якості та надійності системи в цілому. Що стосується захисту під час мережевого обміну інформацією, то основним засобом є VPN. Окремі системи також можуть використовувати автентифікацію при доступі до корпоративної мережі шифрування усього трафіку. Присутня можливість створювати для кожного додатка окремий VPN канал, що також забезпечує додаткову захищеність за умови використання загальнодоступних або ненадійних мереж. Це також створює додаткові переваги для сервера, тому що не потрібує постійної підтримки каналу для усіх додатків.

Висновки

Збільшення ринку мобільних пристроїв сприяє їх більш масовому використанню в корпоративному сегменті для оптимізації робочого процесу та економії коштів. Достатньо стрімкий розвиток систем керування мобільними пристроями показує, що це є перспективним напрямком в IT та бізнес індустрії. Велике різноманіття компаній, які надають такі сервіси сприяє більш якісному розвитку технологій для забезпечення захисту корпоративної інформації як на самих пристроях, так і під час віддаленого доступу до корпоративної мережі. Проведений аналіз основних концепцій побудови EMM системи в цілому та найпопулярніших представників ринку систем керування мобільними пристроями показав, що вибір однієї з них залежить від напрямків діяльності організації, операційної системи та фірми виробника пристроїв, що використовуються співробітниками в професійної діяльності. Але кожна з розглянутих EMM систем дозволяє забезпечити базовий набір функцій безпеки інформації.

СПИСОК ЛІТЕРАТУРИ

1. Madden J., Madden B. Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD. – Jack Madden, 2013. 176 p.
2. Saravana, Balaji B,, Karthikeyan, N.K. and Raj Kumar, R.S., (2018), "Fuzzy service conceptual ontology system for cloud service recommendation", *Computers & Electrical Engineering*, Vol. 69, pp. 435–446.
3. Saravana, Balaji B., Mohamed, Uvaze Ahamed, Eswaran C. and Kannan R., (2019), "Prediction-based Lossless Image Compression", Lecture Notes in Computational Vision and Biomechanics (Springer), Vol. 30, No 1, pp.1749 – 17961,
4. Amin Salih M., Potrus M.Y. A Method for Compensation of TCP Throughput Degrading During Movement Of Mobile Node. *ZANCO Journal of Pure and Applied Sciences*. 2015. Vol. 27, No 6. P. 59–68.
5. Dhivakar B., Saravanan S.V., Sivaram M., Krishnan R.A. Statistical Score Calculation of Information Retrieval Systems using Data Fusion Technique". *Computer Science and Engineering*. 2012. Vol. 2, Issue 5. pp.43-45.
6. Sivaram, M., Batri, K., Amin Salih, Mohammed and Porkodi V. (2019), "Exploiting the Local Optima in Genetic Algorithm using Tabu Search", *Indian Journal of Science and Technology*, Volume 12, Issue 1.
7. Kuchuk G., Nechausov S., Kharchenko, V. Two-stage optimization of resource allocation for hybrid cloud data store. *International Conference on Information and Digital Technologies*. 2015. P. 266-271.
8. Ruban, I. Redistribution of base stations load in mobile communication networks / I. Ruban, H. Kuchuk, A. Kovalenko // Innovative technologies and scientific solutions for industries. – 2017. – No 1 (1) – P. 75-81.
9. Коваленко А.А. Сучасний стан та тенденції розвитку комп'ютерних систем об'єктів критичного застосування / А.А. Коваленко, Г.А. Кучук // Системи управління, навігації та зв'язку. – Полтава . ПНТУ, 2018. – Вип. 1(47). – С. 110-113. DOI : https://doi.org/10.26906/SUNZ.2018.1.110

10. Кучук Г. А. Модель процесса эволюции топологической структуры компьютерной сети системы управления объектом критического применения / Г.А. Кучук, А.А. Коваленко, А.А. Янковский // Системи обробки інформації. – 2014. – № 7(123). – С. 93-96.
11. Кучук Г.А. Метод мінімізації середньої затримки пакетів у віртуальних з'єднаннях мережі підтримки хмарного сервісу / Г.А. Кучук, А.А. Коваленко, Н.В. Лукова-Чуйко // Системи управління, навігації та зв'язку. – Полтава . ПНТУ, 2017. – Вип. 2(42). – С. 117-120.
12. Sivaram, M., Yuvaraj, D., Amin Salih, Mohammed, Porkodi, V. and Manikandan V. (2018), "The Real Problem Through a Selection Making an Algorithm that Minimizes the Computational Complexity", *International Journal of Engineering and Advanced Technology*, Vol. 8, iss. 2, 2018, pp. 95-100.
13. Sivaram, M., Porkodi, V., Mohammed, A.S., Manikandan V. Detection of Accurate Facial Detection Using Hybrid Deep Convolutional Recurrent Neural Network. *ICTACT Journal on Soft Computing*. 2019. Vol. 09, Issue 02. pp. 1844-1850.
14. Mohammed, A. S. Optimal Forecast Model for Erbil Traffic Road Data. ZANCO Journal of Pure and Applied Sciences. 2017. Vol. 29, No 5. P. 137–145. **DOI:** https://doi.org/10.21271/ZJPAS.29.5.15
15. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування. *Сучасні інформаційні системи*. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04
16. Свиридов А. С., Коваленко А. А., Кучук Г. А. Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку. *Сучасні інформаційні системи*. 2018. Т. 2, № 2. С. 139–144. DOI: https://doi.org/10.20998/2522-9052.2018.2.24
17. Kravets A. G., Bui N. D., Al-Ashval M. Mobile security solution for enterprise network //Joint Conference on Knowledge-Based Software Engineering. – Springer, Cham, 2014. – С. 371-382.
18. Peraković D., Husnjak S., Cvitić I. Comparative analysis of enterprise mobility management systems in BYOD environment //The 2nd Reseach Conference In Technical Disciplines, RCITD. – 2014. – С. 82-85.
19. Redman P., Girard J., Wallin L. O. Magic quadrant for mobile device management software //Gartner G00211101. – 2011.
20. Ortbach K., Brockmann T., Stieglitz S. Drivers for the adoption of mobile device management in organizations. – 2014.
21. Android developer[Електроний ресурс]: https://developer.android.com/about/dashboards Distribution dashboard
22. Android Enterprise Solutions Directory [Електроний ресурс]. -Режим доступу:
23. https://androidenterprisepartners.withgoogle.com/emm/ EMMs
24. VMWare AirWatch[Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.air-watch.com/
25. MobileIron[Електроний ресурс]:[Веб-сайт]-Режим доступу: https://www.mobileiron.com/
26. IBM MaaS360 with Watson[Електроний ресурс].—Режим доступу: https://www.ibm.com/security/mobile/maas360
27. Samsung. WhitePaper: Knox Platform for Enterprise, 2018.

Рецензент: д-р техн. наук, проф. І. В. Рубан,
Харківський національний університет радіоелектроніки, Харків
Received (Надійшла) 23.04.2019
Accepted for publication (Прийнята до друку) 29.05.2019

Анализ безопасности данных в EMM системах

К. В. Нечволод, А. В. Северинов, А. В. Власов

Предметом исследования в статье является анализ методов, обеспечивающих безопасность корпоративных данных и порядок доступа к ним при использовании систем управления собственными устройствами в корпоративных целях - EMM (Enterprise Mobility Management) систем. **Цель работы** - рассмотрение и сравнения различных существующих EMM систем, исследование их характеристик и возможностей. В статье решаются следующие **задачи**: рассмотрение задач, структуры и составляющих функций EMM систем, определение их преимуществ и недостатков, анализ самых популярных EMM систем. Получены следующие **результаты**: рассмотрена структура, основные подсистемы, преимущества и недостатки систем управления собственными устройствами, проанализированы самые популярные программные EMM системы. **Выводы**: Проведенный анализ концепций построения EMM системы в целом и популярных представителей рынка систем управления мобильными устройствами показал, что выбор одной из них зависит от направлений деятельности организации, операционной системы и фирмы производителя устройств, используемых сотрудниками в профессиональной деятельности. Применение EMM систем для ведения бизнеса можно назвать вполне оправданным только при корректной настройке и внедрению этих систем.

Ключевые слова: EMM система, BYOD система, удаленное управление мобильными устройствами, защита корпоративной информации.

Data security analysis in EMM systems

K. Nechvolod, O. Sievierinov, A. Vlasov

The subject of research in the article is the analysis of methods that ensure the security of corporate data and the order of access to it when using its own device management systems for corporate purposes - EMM (Enterprise Mobility Management) systems. **The purpose** of the work is to review and compare various existing EMM systems, to study their characteristics and capabilities. The article solves the following **tasks**: consideration of the tasks, structure and constituent functions of EMM systems, determination of their advantages and disadvantages, analysis of the most popular EMM systems. The following **results** were obtained: the structure, main subsystems, advantages and disadvantages of the systems for managing their own devices were considered, the most popular software EMM systems were analyzed. **Conclusions**: The analysis of the main concepts of EMM system construction as a whole and the most popular representatives of the market for mobile devices management systems has shown that the choice of one of them depends on the directions of the organization, operating system and manufacturer's devices companies used by the employees in their professional activities. The use of EMM systems for business can be called fully justified only with the correct configuration and implementation of these systems.

Keywords: EMM system, BYOD system, remote control of mobile devices, protection of corporate information.