**Список використаних джерел:**

1. Маннинг К. Д., Рагхаван П., Шютце Х. Введение в информационный поиск. – Москва: «Вильямс», 2011.
2. Клюшин Д. А. Розпізнавання образів. (Курс лекцій), факультет кібернетики, КНУ: Київ, 2011.
3. Elzbieta Pekalska, Robert Duin. The dissimilarity representation for pattern recognition. – Delft, The Netherlands, 2005.
4. Воронцов К. В. Машинное обучение. (Курс лекций). ВмиК МГУ. – Москва, 2009.
5. Петунин Ю. И., Тимошенко Я. Г., Петунина М. Ю. Критерий для идентификации генеральной совокупности в случае конечного класса альтернативных гипотез. Докл. АН УССР. – Сер. А. – 1984, № 6. – С. 29-32.
6. Ван дер Варден. Математическая статистика. – Москва: «Мир», 1988.
7. Barnett V. The ordering of multivariate data. Journal of the Royal Statistical Society. Series A (General). – Vol. 139. – 1976. – № 3. – Pp. 318-355.
8. Ляшко С. И., Клюшин Д. А., Алексеенко В. В. Многомерное ранжирование и эллиптический пилинг. Кибернетика и системный анализ. – 2013. – № 4. – С. 29-36.
9. Клюшин Д. А., Присяжная М. В. Многомерное ранжирование с помощью эллипсов Петунина. Журнал обчисл. та прикл. математика. – 2013. – № 4. – С. 1-7.
10. Schapire R. E., Freund Y., Lee W. S., Bartlett P. Boosting the margin: a new explanation for the effectiveness of voting methods. Annals of Statistics. – 1998. – Vol. 26, № 5. – Pp. 1651–1686.
11. Freund Y., Schapire R. E. Experiments with a new boosting algorithm. International Conference on Machine Learning. – 1996. – Pp. 148–156.

**Вовченко Є.В.**

*студент,*
*Національний технічний університет України*
*«Київський політехнічний інститут»*

## АРХІТЕКТУРА УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ SAP AFARIA

Значення мобільності об’ємне для більшості організацій. Мобільність може дозволити організаціям краще взаємодіяти з клієнтами, поліпшити бізнес-процеси і включити нові можливості для бізнесу. Всебічна мобільна стратегія безпеки повинна охоплювати всі аспекти мобільних користувачів і їх взаємодію з корпоративними даними. Проте, зростання мобільності не може відбуватися без експлуатаційної цілісності і надійності, яка досягається, зокрема, за рахунок використання концепції управління мобільними пристроями.

Управління мобільними пристроями (Mobile device management, MDM) – технологія управління життєвим циклом платформи, яка включає функціонал обліку використовуваних пристроїв, управління конфігураціями ОС, управління мобільними додатками (в тому числі їх ініціалізація і деініціалізація, віддалена очистка, віддалений моніторинг та контроль за збійними ситуаціями). Зазвичай ці завдання реалізуються через установку на мобільний пристрій відповідних MDM-профілів. MDM рішення призначені для

забезпечення безпеки і централізованого управління мобільними пристроями з метою захисту корпоративних даних, що зберігаються на пристроях, а також даних, до яких мають доступ ці пристрої.

SAP Afaria – це реалізація системи управління мобільними пристроями, яка дозволяє захистити і управляти мобільними пристроями, мобільними додатками і даними. З Afaria, можливо віддалено підключатися до зареєстрованих мобільних пристроїв для налаштування пристрою і установки необхідних додатків.

Розглянемо архітектуру MDM рішення Afaria.

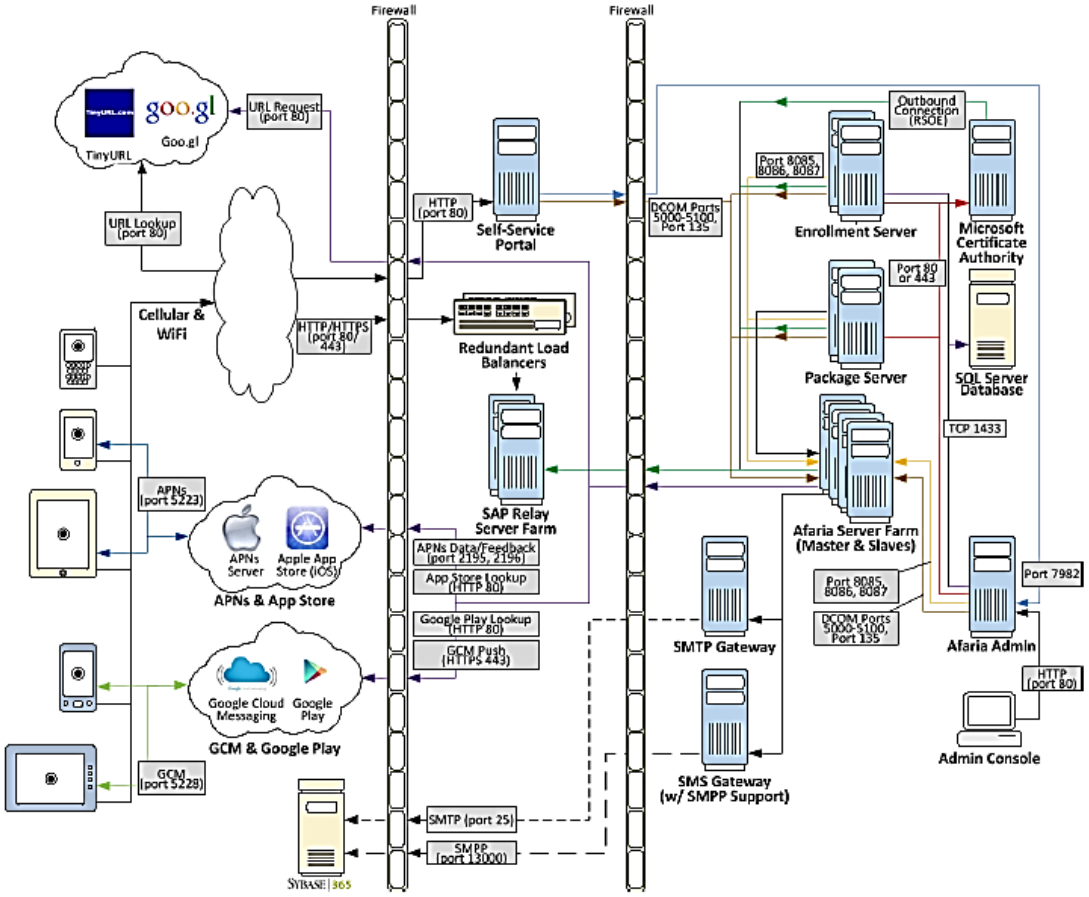


**Рис. 1. Архітектура Afaria – Інтернет, DMZ і корпоративна мережа**

Afaria є розподіленою мобільною системою управління пристроєм, що складається з декількох окремих компонентів програмного забезпечення.

MDM архітектуру можна розділити на такі частини:

1. Інтернет – сукупність пристроїв та громадських організацій.

Пристрої – це смартфони і комп'ютери, якими управляє Afaria. Пристрої мають встановлений додаток Afaria або мають власне рішення, яке Afaria використовує для взаємодії з пристроєм хостингу. Пристрої підключаються до серверів Afaria або проксі-серверів з використанням HTTP і SSL. Громадські організації – юридичні особи, які підтримують управління пристроями і функції, такі як Push Notification Service компанії Apple (APNS) для управління iOS пристроями, або використовують комерційний ринок додатків.

2. DMZ – релейні або проксі-сервери, такі як сервер управління загроз шлюзу Microsoft Forefront або SAP Sybase SQL Anywhere Relay Server для забезпечення дотримання правил брандмауера і отримання повідомлення на пристрій, перш ніж його ретранслюють на сервер Afaria в корпоративну мережу. Для контролю доступу до електронної пошти існує додаткова функція: проксі-сервер електронної пошти використовує фільтр контролю доступом, щоб дозволити або блокувати вхідні запити, засновані на інформації про політику управління доступом від Afaria. Використання релейних серверів в DMZ для радіорелейного зв'язку не є обов'язковим, але рекомендується для підвищення безпеки мережі підприємства.

3. Мережа управління – використовується для зв'язку компонентів сервера і мережі електронних листів з сервером Afaria, а також базою даних.

Основними компонентами архітектури MDM Afaria є:

Afaria сервер – це сервер, що взаємодіє з пристроями під управлінням MDM та з застосуванням політик конфігурації і збору даних інвентаризації.

Консоль адміністрування Afaria – веб-інтерфейс користувача для конфігурації Afaria, та управління пристроями, а також звітності по TEM і інвентаризації. Сервер подачі заявок – це привід для реєстрації пристроїв в мережі Afaria, а також для забезпечення корисного навантаження в управлінні пристроями. Сервер реєстрації повинен бути встановлений на тому ж сервері, що і сервер Afaria.

Пакет-сервер – обслуговує пакети прикладних програм Afaria до пристроїв, а також обробляє сертифікати і дані пристрою виділення ресурсів для виклику сторонніх додатків. Сервер порталу пакетів не обслуговує комерційних додатків для пристроїв.

Портал самообслуговування – дозволяє кінцевим користувачам зареєструвати свій пристрій в управлінні Afaria, і дозволяє користувачам переглядати інформацію і використовувати команди на пристрої, наприклад, змінити паролі. Портал не є обов'язковим для реєстрації і дозволяє користувачам встановлювати політику додатків за підтримки з боку сервера пакетів.

Afaria також поставляється з цілим рядом додаткових компонентів і програмних пакетів.

SMS Gateway – це можливість використання SMS повідомлень, для віддаленого стирання команд. SMS Gateway використовує бібліотеки продуктів Cygwin і інструменти з Cygnus Solutions, а також інші інструменти з відкритим вихідним кодом. SMS Gateway не обов'язковий для використання. Afaria використовує SMS Gateway для пристроїв і клієнтів, які підтримують управління через SMS повідомлення, для доставки вихідних повідомлень та віддаленого стирання команд.

Релейний сервер – проксі для HTTP і HTTPS з'єднання з Інтернетом через сервер компонентів, таких як сервер Afaria або сервер реєстрації. Релейний сервер не є обов'язковим, але рекомендується для підвищення безпеки корпоративної мережі.

Контроль доступу до електронної пошти – це елементи управління доступом,що дозволяють обмежити доступ до електронної пошти.

Мережевий контроль корпоративного доступу (Network Access Control (NAC)) – він дозволяє обмежити доступ до мережі.

Управління мобільними пристроями набуває все більшої важливості, і його продукти, можливо, стануть одним з ключових компонентів IT-стратегії багатьох організацій. MDM не вимагає великих витрат і приносить явні вигоди – особливо при роботі в регульованої галузі. MDM рішення Afaria добре масштабується і може підтримувати дуже великі мережі. Можливо встановити Afaria на одному сервері для невеликої мережі або поширювати Afaria через кілька серверів для великих мереж.

**Список використаних джерел:**

1. Terrence Cosgrove, Rob Smith, Chris Silva, John Girard, Bryan Taylor. «Critical Capabilities for Enterprise Mobility Management Suites.» USA: Gartner, Jun 2015. – P. 13-15.

2. «SAP Afaria Overview». – USA: SAP, Dec 2014. – P. 7-10.

**Головенко Т.М.**

*кандидат технічних наук, завідувач наукових лабораторій;*

**Бойко Г.А.**

*кандидат технічних наук, старший лаборант;*

**Іваненко О.О.**

*аспірант,*

*Херсонський національний технічний університет*

**Шовкомуд О.В.**

*кандидат технічних наук, старший викладач;*

*Луцький національний технічний університет*

## ПОНЯТТЯ ТЕХНІЧНОГО ТЕКСТИЛЮ ТА РОЗШИРЕННЯ ЙОГО АСОРТИМЕНТУ

Нетрадиційні сфери використання текстильних волокон та виробів характеризують поняттям «технічний текстиль», який охоплює різні сфери використання нетканих матеріалів, геотекстилю, тканин, трикотажу та інших виробів. В США більше 25% споживання волокон пов’язано з використанням їх для технічних (промислових) цілей.

Технічний текстиль виготовляється з текстильних волокон (нетканий технічний текстиль) та текстильних ниток (тканий технічний текстиль). Важливим фактором, що визначає нижчу собівартість нетканих полотен в порівнянні з тканиною і трикотажем, є можливість використання для їх отримання коротких волокон непридатних для прядіння волокон, а також відходів прядильного виробництва. Створення високопродуктивних технологій отримання нетканих матеріалів з одночасним наданням спеціальних