

АНАЛИЗ ПОКАЗАТЕЛЕЙ КАЧЕСТВА МОБИЛЬНЫХ КОРПОРАТИВНЫХ СЕТЕЙ

Аль-Ашвал М.С., Кравец А.Г.

«Волгоградский государственный технический университет», Волгоград, Россия (400005, Волгоград, пр. им. Ленина, 28), al_ashwal2008@mail.ru

В статье рассмотрен подход к реализации автоматизированной системы управления качеством мобильных корпоративных систем (МКС). Разработанная система критериев качества позволила выделить группу из 3 критериев, соответствующую уровню управления службы безопасности, и 12 показателей, которые позволяют оценить эти критерии качества. Созданная методика создания и управления мобильными корпоративными сетями основана на предложенной авторами концепции параллельной многоконтурной безопасности. В рамках концепции выделено 4 вида функций управления: управление устройством, управление приложениями, управление контентом, управление доступом. Для реализации методики создания и управления качеством МКС были разработаны: модуль управления мобильным доступом к корпоративным ресурсам и модуль управления персональным контентом. В ходе опытного внедрения были получены данные, подтверждающие достоверность разработанных теоретических положений. Желаемые тенденции показателей критериев качества МКС были достигнуты.

Ключевые слова: управление качеством мобильных корпоративных систем, концепция параллельной многоконтурной безопасности, управления персональным контентом

ANALYSIS OF INDICATORS OF QUALITY MOBILE CORPORATE NETWORKS

Al - Ashval M.S., Kravets A.G.

"Volgograd State Technical University", Volgograd, Russia (400005, Volgograd, Lenin av, 28), al_ashwal2008@mail.ru

The article describes the approach to the implementation of the mobile enterprise systems (MES) quality management automated system. The quality criteria developed system made it possible to identify a group of 3 criteria, proper management of security service level, and 12 indicators to assess these quality criteria. The technique of creating and managing mobile enterprise networks based on the concept proposed by the authors of parallel multi-loop security. The concept of allocated 4 types of management functions: device management, application management, content management, access control. To implement the technique of creating and managing the quality of the MES were developed: the control module of mobile access to corporate resources and personal content management module. In the experimental implementation, data were obtained confirming the accuracy of the developed theoretical propositions. Desired trend indicators of quality criteria MES were achieved.

Keywords: Quality management of mobile enterprise systems, the concept of parallel multi-loop security, personal content management

Анализ данных, представленных в литературных источниках [1] и, прежде всего, в научно-технических отчетах фирм Cisco, Siemens, Hewlett Packard и других, позволил выделить 9 критериев качества МКС, а также 28 показателей для оценки этих критериев, и оценить их применимость для целей управления МКС (таб.1). В результате исследования был выявлен проблемный сегмент предметной области – инфраструктура и безопасность. Разработанная система критериев качества позволила выделить группу из 3 критериев, соответствующую уровню управления службы безопасности, и 12 показателей, которые позволяют оценить эти критерии качества.

Таблица 1

Система критериев и показателей качества

Служба безопасности	Безопасное подключение только к нужным ресурсам	Уровень обеспечения безопасности и конфиденциальности	Мониторинг МКС	Рост
		Время получения доступа к авторизованным сетевым ресурсам	Мониторинг МКС	Снижение
		Интенсивность зашифрованного сетевого трафика	Мониторинг МКС	Снижение
		Уровень обеспечения защиты персонального контента	Мониторинг МКС	Рост
		Сложность аутентификации пользователей и устройств	Мониторинг МКС	Снижение
	Политики подключений и исключений	Групповая аутентификация	Мониторинг МКС	Рост
		Гранулированный контроль устройств	Мониторинг МКС	Рост
	Оперативный анализ рисков	Количество анализируемых состояний устройств	Мониторинг МКС	Рост
		Регламент в случае потери/кражи устройства	Наличие	1
		Регламент в случае увольнения персонала	Наличие	1
Количество новых устройств в МКС за период времени		Мониторинг МКС	Рост/ стабильность	

		Количество выбывших устройств в МКС за период времени	Мониторинг МКС	Снижение/ стабильность
--	--	--	-------------------	---------------------------

Для разработки методики создания и управления мобильными корпоративными [2,3] сетями предложена концепция параллельной многоконтурной безопасности (рис.1).

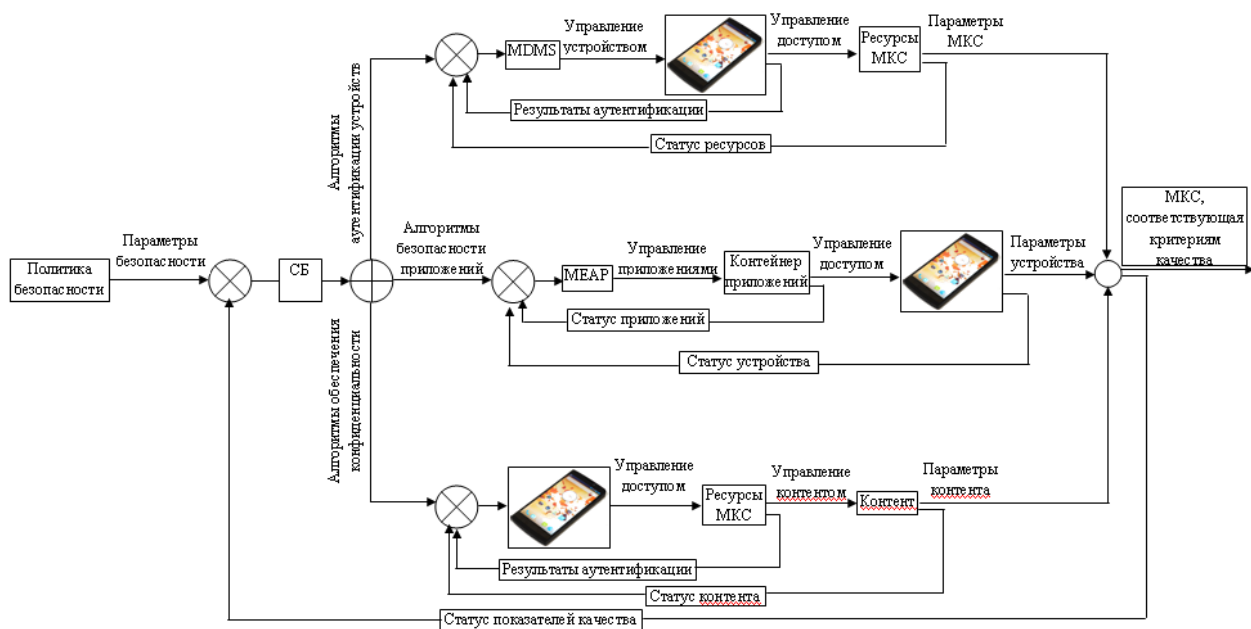


Рис. 1. Схема методики создания и управления мобильными корпоративными.

В рамках концепции выделено 4 вида функций управления: управление устройством, управление приложениями, управление контентом, управление доступом; в трёх параллельных процессах управления: управление устройствами, управление приложениями, управление персональным контентом. Основная управляющая подсистема – система безопасности (СБ) делегирует распараллеленную функцию управления трём субуправляющим подсистемам: MDMS, MEAP, устройство. Делегирование осуществляется путем реализации алгоритмов аутентификации устройств, безопасности приложений и обеспечения конфиденциальности. Контроль показателей качества МКС («Статус показателей качества») обеспечивается за счет мониторинга состояния (статуса, ST) управляемых подсистем и параметров каждого контура в параллельных субсистемах управления. Наиболее хорошо разработанными на данный момент являются алгоритмы безопасности приложений: антивирусные программы, программы контроля версий и другие. В связи с этим, было принято допущение, что безопасность приложений обеспечивается сторонними средствами и не влияет на прочие показатели качества МКС на уровне «Служба безопасности» (таб. 1). Таким образом, в данной статье рассматриваются алгоритмы аутентификации устройств и обеспечения конфиденциальности персонального контента.

Существующие методы аутентификации пользователей (логин/пароль, ЭЦП, биометрия и другие) и мобильных устройств (IMEI, ключ беспроводной сети и другие) не позволяют реализовать механизмы групповой идентификации и гранулированного контроля устройств. Кроме того, эти методы требуют сетями на основе концепции параллельной многоконтурной безопасности дополнительных ресурсов сети и не учитывают постоянно возрастающей вычислительной мощности мобильных устройств.

Комплексный алгоритм аутентификации мобильных устройств в рамках методики создания и управления МКС использует следующие обозначения показателей качества (таб.2).

Таблица 2

Обозначение контролируемых показателей качества МКС.

Наименование критерия	Показатель	Обозн.
Безопасное подключение только к нужным ресурсам	Уровень обеспечения безопасности и конфиденциальности	<i>LS</i>
	Время получения доступа к авторизованным сетевым ресурсам	<i>TA</i>
	Интенсивность зашифрованного сетевого трафика	<i>NT</i>
	Уровень обеспечения защиты персонального контента	<i>LC</i>
	Сложность аутентификации пользователей и устройств	<i>CA</i>
Политики подключений и исключений	Групповая аутентификация	<i>GID</i>
	Гранулированный контроль устройств	<i>GCD</i>
Оперативный анализ рисков	Количество анализируемых состояний устройств	<i>NS</i>
	Регламент в случае потери/кражи устройства	<i>RLT</i>
	Регламент в случае увольнения персонала	<i>RUP</i>
	Количество новых устройств в МКС за период времени	<i>NN</i>
	Количество выбывших устройств в МКС за период времени	<i>NA</i>

Комплексный алгоритм аутентификации мобильных устройств в МКС основан на коллаборативной реализации алгоритмов библиотеки OpenPGP для выдачи сертификатов устройствам и шифрования на базе 2048 – битных ключей RSA [4], алгоритма QSPN для групповой аутентификации в одноранговой самоорганизующейся сети (например, подразделения предприятия) и алгоритма ZKP (доказательство с нулевым разглашением) для анонимной идентификации устройства и/или ресурса МКС [5].

Предлагается следующая информационная модель контейнера приложений со

встроенными наборами идентификаторов объектов системы безопасности:

$$CONT = \{AppSet, CertSet, QSPNSet\}, \quad (1)$$

где AppSet – набор корпоративных приложений, включая программное обеспечение системы безопасности;

CertSet – набор идентификаторов сертификатов, по которым данный контейнер может быть предоставлен устройству, ICERT ∈ CertSet;

QSPNSet – набор идентификаторов сетей QSPN, которым данный контейнер может быть предоставлен при групповой аутентификации.

Предлагается следующая информационная модель ресурса МКС со встроенными наборами идентификаторов объектов системы безопасности:

$$RES = \{ResType, ResSet, CertSet, QSPNSet, ZKPAcc\}, \quad (2)$$

где ResType – тип ресурса: информационный, персональный, групповой;

ResSet – набор идентификаторов доступных ресурсов;

CertSet – набор идентификаторов сертификатов, по которым данный набор ресурсов может быть предоставлен устройству, ICERT ∈ CertSet;

QSPNSet – набор идентификаторов сетей QSPN, которым данный набор ресурсов может быть предоставлен при групповой аутентификации, GRES ∈ QSPNSet;

ZKPAcc – идентификатор предоставления доступа к ресурсу при анонимной идентификации.

Рассмотрим показатели качества МКС на примере «Уровень обеспечения безопасности и конфиденциальности» и «Время получения доступа к авторизованным сетевым ресурсам»:

$$LS = \begin{cases} LS_{QSPN} + LS_{ZKP} & \text{при } GID=1, CONT=0, \\ LS_{QSPN} + LS_{CERT} & \text{при } GID=1, CONT=1, ICERT=1 \end{cases} \quad (3)$$

$$TA = \begin{cases} TA + \Delta TA_{QSPN} & \text{при } GID=1, ICERT=0, \\ TA + \Delta TA_{CERT} & \text{при } GID=1, ICERT=1, \\ TA + \Delta TA_{ZKP} & \text{при } GID=0 \end{cases} \quad (4)$$

При этом показатель LS принимает лингвистические значения {«Низкий», «Ниже среднего», «Средний», «Выше среднего», «Высокий»} и определяется с шагом 0,2 в интервале [0,1] на диапазонах соотношения:

$$LS_p = N_p / N, \quad (5)$$

где p – алгоритм из {OpenPGP, QSPN, ZKP}, N_p – количество подключений к ресурсам с использованием алгоритма p за текущую сессию (период времени), N – общее количество подключений к ресурсам за текущую сессию (период времени).

Таким образом, качество МКС из таб. 1 и формул (1)-(4) для выделенных показателей:

$$QLT = \begin{cases} \sum_{j=1}^k LS_{QPSN} * x_j + \max \left(\sum_{i=0}^n LS_{ZKP} * y_i, \sum_{i=0}^n LS_{CERT} * z_i \right) \rightarrow \max, \\ TA + \sum_{i=0}^n \Delta TA_{QPSN} * x_i + \min \left(\sum_{i=0}^n \Delta TA_{ZKP} * y_i, \sum_{i=0}^n \Delta TA_{CERT} * z_i \right) \rightarrow \min \end{cases} \quad (6)$$

где n – количество устройств в МКС, $i=0, n$; k – количество групп в МКС, $j=1, k$;

$$x_j = \begin{cases} 1, & \text{если устройство имеет доступ к ресурсам МКС,} \\ 0, & \text{в обратном случае (доступ ресурса МКС к персональному контенту);} \end{cases}$$

$$y_i = \begin{cases} 1, & \text{если устройство прошло анонимную идентификацию,} \\ 0, & \text{в обратном случае;} \end{cases}$$

$$z_i = \begin{cases} 1, & \text{если устройство сертификат безопасности,} \\ 0, & \text{в обратном случае.} \end{cases}$$

При этом, исходя из концепции BYOD, $\sum_{i=0}^n z_i \rightarrow 0$, $\sum_{i=0}^n y_i \rightarrow \max$, $\sum_{j=1}^k x_j \rightarrow \max$.

Поэтому $QLT=f(QSPN\ GID)$ при доступе устройства к ресурсам МКС и $QLT=f(ZKP)$ при доступе к персональному контенту.

Для реализации методики создания и управления качеством МКС были разработаны: модуль управления мобильным доступом к корпоративным ресурсам (СУБД Oracle и Oracle JDeveloper), встраиваемый в MDM, и модуль управления персональным контентом PCM (Java). Интерфейс модулей представлен на рис. 2.

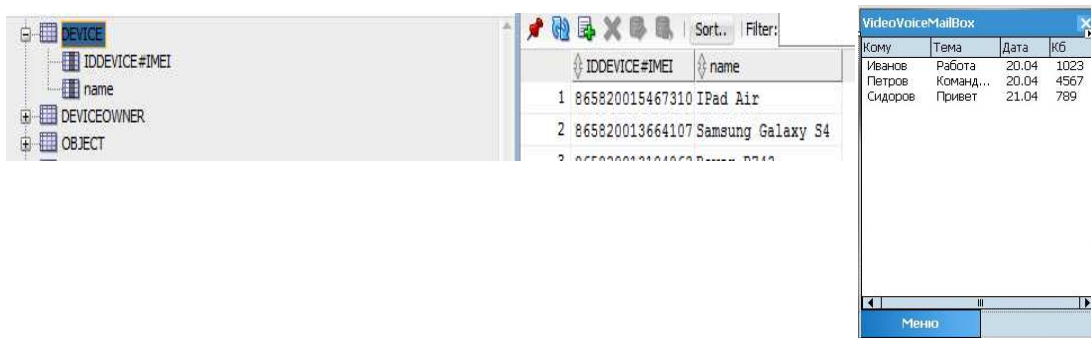


Рис. 2. Экранные формы модулей платформы.

В ходе опытного внедрения были получены данные, подтверждающие достоверность разработанных теоретических положений. Желаемые тенденции показателей критериев качества МКС (таб.1) были получены.

Список литературы

1. Аль-Ашваль, М.С. Система критериев и показателей качества мобильных корпоративных сетей / Аль-Ашваль М.С., Кравец А.Г. // Инновации на основе

информационных и коммуникационных технологий. Инфо 2014 : матер. XI междунар. науч.-практ. конф. (г. Сочи, 2014 г.) /Национальный исследовательский ун-т "Высшая школа экономики" [и др.]. - М., 2014. - С. 501-504.

2. Аль-Ашваль, М.С. Выбор протокола для построения сети с использованием технологии IP-телефонии / Аль-Ашваль М.С., Кравец А.Г., Юдин Д.В. // Известия ВолгГТУ. Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах». Вып. 13 : межвуз. сб. науч. ст. / ВолгГТУ. - Волгоград, 2012. - № 4 (91). - С. 170-172.

3. Аль-Ашваль, М.С. Разработка мобильного клиента видео-голосовой почты / Аль-Ашваль М.С., Кравец А.Г. // Инновационные информационные технологии : матер. междунар. науч.-практ. конф., г. Прага, Чехия, 2013 г. В 4 т. Т. 4 / МИЭМ НИУ ВШЭ [и др.]. - М., 2013. - С. 362-366.

4. Кравец, Е.Г. Подход к реализации автоматизированной системы дистанционного проведения следственных действий /Кравец Е.Г., Попов Е.Ю., Кравец А.Г., Аль-Ашваль М.А.С.//Известия Волгоградского государственного технического университета. 2012. Т. 4. № 13. С. 161-164.

5. Кравец, А.Г. Mobile Security Solution for Enterprise Network / Кравец А.Г., Ngoc Duong Bui, Аль-Ашваль М.С. // Knowledge-Based Software Engineering : Proceedings of 11th Joint Conference, JCKBSE 2014 (Volgograd, Russia, September 17-20, 2014) / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Tadashi Iijima ; Volgograd State Technical University [etc.]. – [Б/м] : Springer International Publishing, 2014. – P. 371-382. – (Series: Communications in Computer and Information Science ; Vol. 466).

Рецензенты:

Олянич А.В., д.фил.н., профессор, заведующий кафедрой иностранных языков ФБГОУ ВПО «Волгоградский государственный аграрный университет», г. Волгоград;

Фоменков С.А., д.т.н., профессор, профессор кафедры «Системы автоматизированного проектирования и поискового конструирования» ФБГОУ ВПО «Волгоградский государственный технический университет» г. Волгоград.