УДК 004.77+004.72+004.65+004.4'23

Оспанова Адеми Бекжановна, к.ф.-м.н.,

Евразийский национальный университет им. Л. Н. Гумилева,

Астана, Казахстан

Ademi Ospanova,

L. N. Gumilyov Eurasian National University,

e-mail: [o.ademi111@gmail.com](mailto:o.ademi111@gmail.com)

Шарип Нурмуханбет, студент,

Евразийский национальный университет им. Л. Н. Гумилева,

Астана, Казахстан

Sharip Nurmukhanbet,

L. N. Gumilyov Eurasian National University,

e-mail: [o.ademi111@gmail.com](mailto:o.ademi111@gmail.com)

ИНСТРУМЕНТЫ MICROSOFT ДЛЯ АВТОМАТИЗАЦИИ БЕЗОПАСНОГО УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ СЕТЯМИ НА БАЗЕ WINDOWS

MICROSOFT TOOLS FOR SAFE CONTROL AUTOMATION OF ENTERPRISE NETWORKS BASED ON WINDOWS

Аннотация: Рассмотрен инструментарий Windows Information Protection (WIP) для защиты корпоративных данных, интегрированный в операционную систему Windows 10 последних сборок. Развернута модель корпоративной сети, в которой налажена работа WIP. Созданы и протестированы политики для безопасного управления корпоративными и персональными данными. Создан подключаемый модуль для разработки приложений, управляемых WIP.

Abstract: The Windows Information Protection (WIP) – tool for enterprise data protection integrated into the last assemblies of operating system Windows 10 is considered. Model of enterprise network in which WIP is adjusted is deployed. Policies for enterprise and personal data safe control are created and tested. The software plug-in for programming of applications controlled by WIP is created.

Ключевые слова: Корпоративные сети, защита корпоративных данных, персональные данные, Active Directory, Windows Information Protection (WIP), System Center Configuration Manager (SCCM).

Keywords: Enterprise Networks, Enterprise Data Security, Private Information, Active Directory, Windows Information Protection (WIP), System Center Configuration Manager (SCCM).

Согласно статистике распределения серверов в мире, работающих под управлением различных операционных систем, доля Windows составляет более трети [1]. В последнее время корпорация Microsoft уделяет большое внимание вопросам обеспечения безопасности своих продуктов. Так, Windows 10, по различным оценкам независимых экспертов, на сегодняшний день можно назвать одной из самых защищенных операционных систем. На рынке продуктов для корпоративных сетей наблюдаются такие же тенденции. Инструментарий Windows Information Protection (WIP), ранее известный как средство защиты корпоративных данных Enterprise data protection (EDP), – это решение от Microsoft, позволяющее эффективно (удаленно) управлять как персональными данными сотрудников, так и корпоративными данными, предотвращать утечки и несанкционированный доступ [2]. В отличие от других средств WIP полностью интегрирован в платформу Windows 10, начиная со сборки 1607, Windows 10 Mobile (также 1607 и более поздние версии).

В данной работе описывается WIP, раскрываются некоторые узкие вопросы установки и настройки необходимого программного обеспечения для работы с WIP, описываются созданные политики для эффективного и автоматизированного управления клиентами – рабочими станциями в корпоративной сети; при создании уклон делался на обеспечении безопасности корпоративных и персональных данных сотрудников. Далее описывается созданный подключаемый программный модуль для разработки так называемых корпоративно-грамотных приложений – приложений, подчиняющихся политикам WIP; а также создано приложение с графическим интерфейсом пользователя для удобного манипулирования политиками WIP.

Для работы с WIP необходимо иметь установленным System Center Configuration Manager (SCCM) или Microsoft Intune. В данной работе рассматривается продукт SCCM, разработанный для управления IT-инфраструктурой на базе Windows и обладающий широкими возможностями ([3]). При установке и настройке рекомендуется опираться на источники [4], которые следует считать основными несмотря на то, что там используется программное обеспечение более ранних версий.

* Необходимое программное обеспечение для установки SCCM.

- Windows Server (в данной работе Windows Server 2016 x64) – для Site server;

- SQL Server (в данной работе SQL Server 2017 Developer) – для Site database.

* Необходимые действия до установки SCCM после распаковки образа SCCM 2016 (можно скачать с сайта Microsoft также и весь System Center 2016).

- Установка домена Active Directory в Windows Server 2016 ([5]).

- Установка оснастки «Схема Active Directory» (это оснастка консоли управления (MMC), которая используется для просмотра схемы доменных служб Active Directory и управления ею) ([6]).

- Установка административных разрешений в оснастке «Схема Active Directory» ([7]).

- Необходимые настройки в средствах администрирования «ADSI Edit» и «Active Directory Users and Computers» ([4]).

- Расширение схемы Active Directory. Утилита extadsch.exe для расширения схемы Active Directory находится в подкаталоге Microsoft.System.Center.Configuration.Manager.2016\SMSSETUP\BIN\X64 распакованного образа SCCM 2016, ее следует запустить в командной строке с правами администратора.

- Установка нужных ролей в Windows Server ([4, 8]).

- Установка Windows ADK ([9]).

- В корне того диска, на котором нежелательно присутствие файлов Configuration Manager, необходимо создать файл no\_sms\_on\_drive.sms.

* Установка SCCM 2016 ([4]). Дополнительные источники – [10].
* Настройка и конфигурация SCCM 2016 ([4]).

- В меню консоли SCCM Administration-->Cloud Services-->Updates and Services отражены доступные обновления и указан их статус (Downloading, Available и др.). Здесь заметим, что с установкой этих обновлений могут возникнуть проблемы, а в разных источниках даются решения, приводящие к одному из предыдущих шагов ([11]). Рекомендуется устанавливать последние версии программ.

- Конфигурация Network account.

- Задание групп границ.

- Cоздание Custom Client (Device) Policy ([4]).

На рисунках 1-2 представлена консоль SCCM 2016 с сконфигурированными настройками ролей и компонентов сайтов.

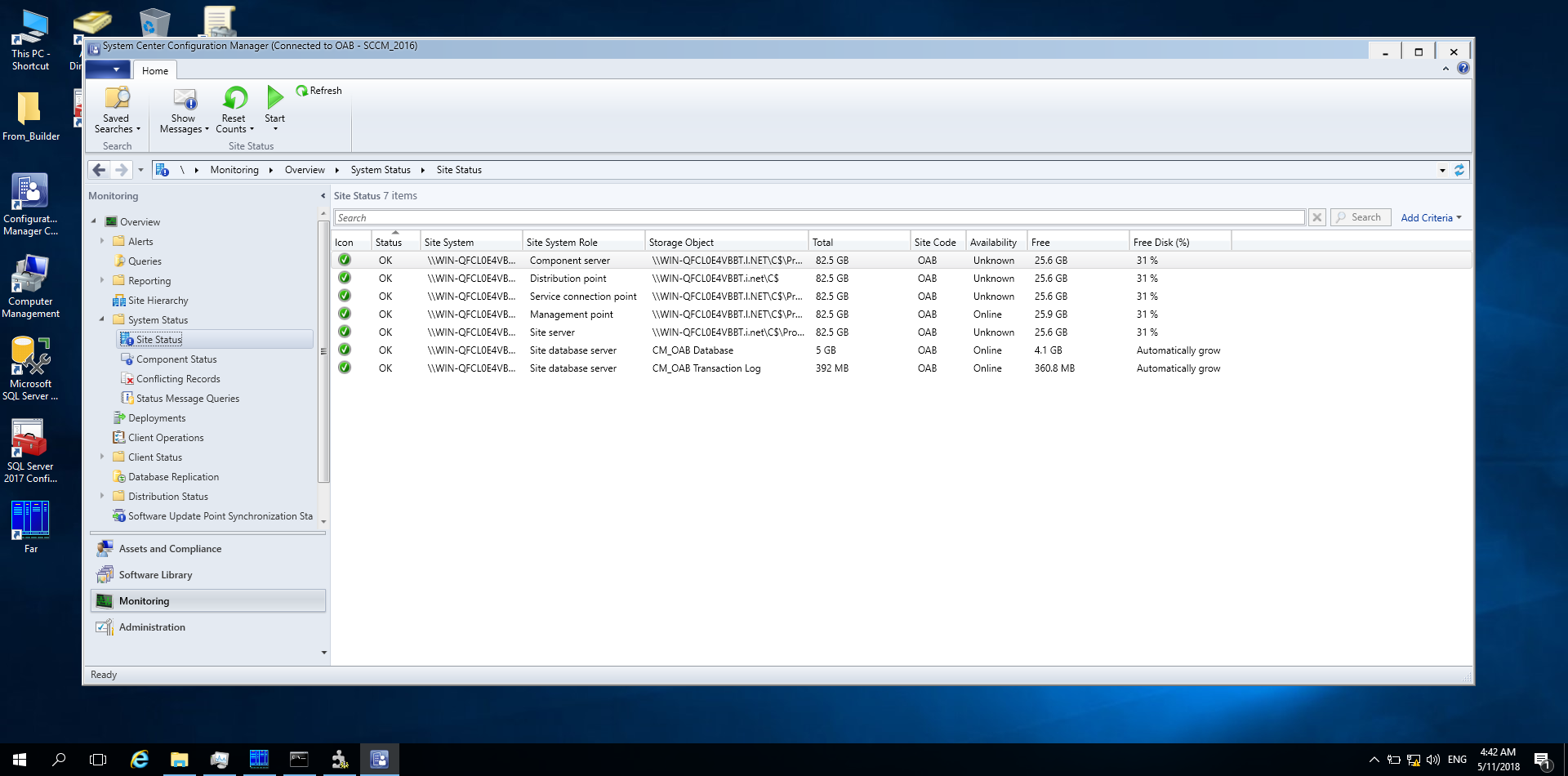


Рисунок 1. Статусы ролей в разделе Monitoring консоли SCCM

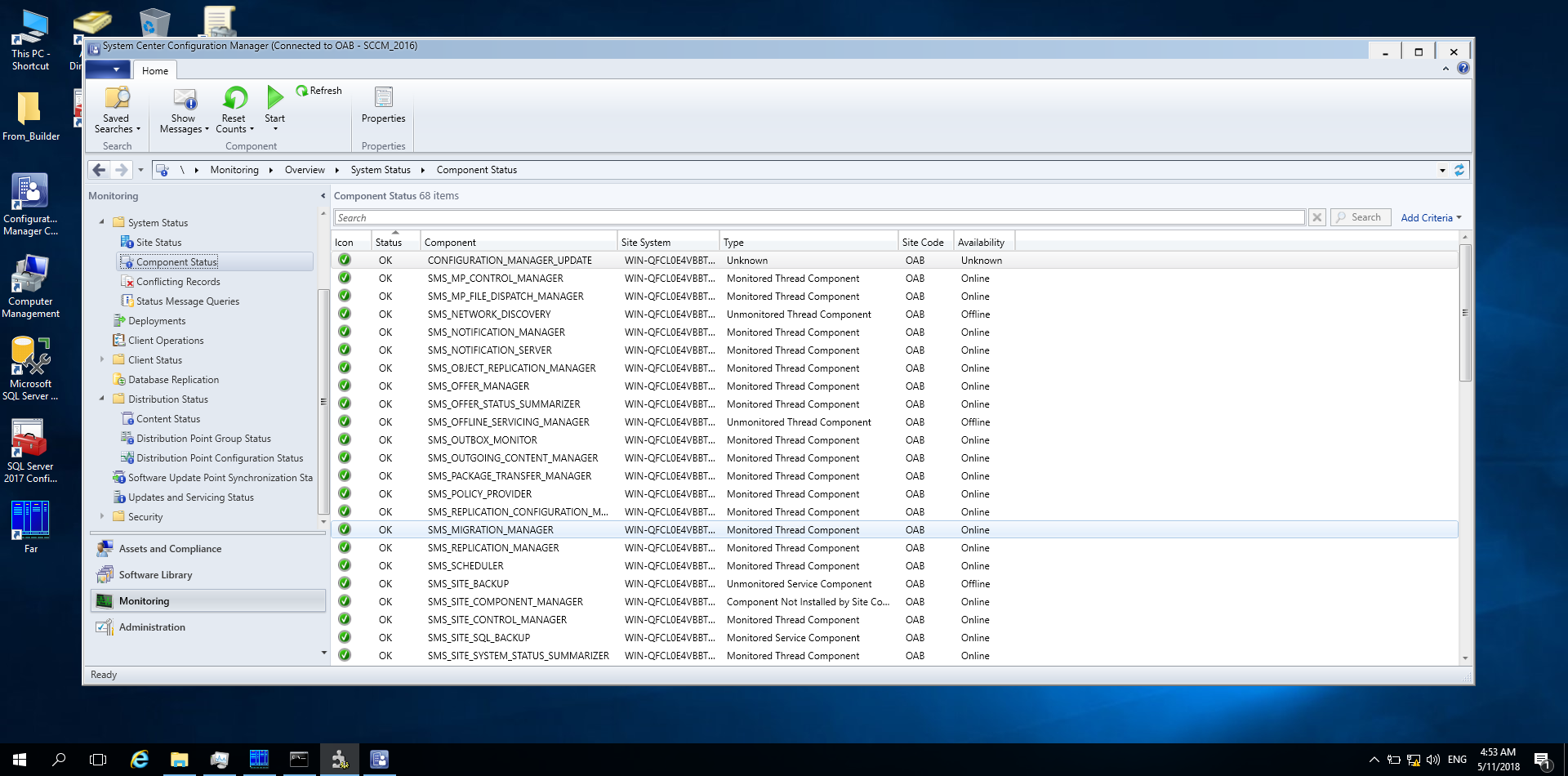


Рисунок 2. Статусы компонентов в разделе Monitoring консоли SCCM

Некоторые решения по устранению неправильно настроенных ролей и компонентов сайтов предполагают удаление пакетных обновлений с помощью SQL-запросов, перезапуск некоторых служб (SMS Executive, SMS Site Component Manager, SMS Distribution Manager), удаление и переустановка ролей и др. (к примеру, [12]).

* Установка клиентов на компьютеры в корпоративной сети.

Как клиенты поддерживаются компьютеры и мобильные устройства с различными операционными системами – таблица 1.

Таблица 1. Поддерживаемые операционные системы клиентов в корпоративной сети под управлением SCCM

|  |  |
| --- | --- |
| Для стационарных ПК | Для мобильных устройств |
| Windows 7 и выше | Apple iOS 7.1 и выше |
| Mac OS X, начиная с 10.9 Mavericks | Google Android 4.0 и выше |
| Серверные корпоративные дистрибутивы Linux | Windows Phone 8.0 и выше |

- Развертывание сети для машины, на которой установлен Site Server, и клиентов. В реализованной в данной работе модели сети Site Server установлен на виртуальной машине (Windows Server 2016 x64), а клиентом является хост-машина (Windows 10 x64). В настройках виртуальной машины (в Virtual Box) следует установить и настроить виртуальный адаптер хоста и добиться, чтобы локальные IP-адреса указанных машин были в одной подсети.

- Установка собственно клиентов не составляет труда ([4]).

* Установка и развертывание политики WIP в SCCM.

- Создание сертификата – [13].

- Создание политик для приложений в консоли SCCM – [14]. Процесс создания политики представляет собой последовательность шагов, выполняемых в консоли SCCM: меню «Assets and Compliance»--> «Configuration Items»--> «Create Configuration Items». Отметим лишь то, что необходимо будет указать данные об издателе приложения, для которого создается политика, в правильном формате и применить созданный выше сертификат – см., к примеру [14].

* Создание корпоративно-грамотных приложений.

Корпоративно-грамотные приложения представляют собой сторонние разработки для корпоративных сетей, выполненные таким образом, что являются управляемыми политиками WIP, действующими на остальные работающие в сети приложения. Для создания таких приложений во избежание конфликтов или уязвимостей используется Visual Studio 2017. Разработана программа, с помощью которой автоматизировано применение политики защищенного доступа к сетевым ресурсам. То есть можно включением этой программы (как модуля) создавать корпоративно-грамотные приложения.

* Создание прототипа информационной системы для облегченной работы с политиками WIP.

Выполнено приложение с графическим интерфейсом пользователя, позволяющее быстро применить и отменить различные политики для приложений, работающих в корпоративной сети: вывести информацию о корпоративных и персональных данных, зашифрованных данных, приложениях под управлением той или иной политики и др.

Защита корпоративных данных и персональных данных сотрудников – одно из приоритетных направлений в политике безопасности любой страны и Казахстана, в частности. Общественные отношения в сфере персональных данных в Казахстане регулируются Законом Республики Казахстан «О персональных данных и их защите» (с [изменениями и дополнениями](https://online.zakon.kz/document/?doc_id=31396234) по состоянию на 28.12.2017 г.). В стране в 2017 году принята Концепция кибербезопасности «Киберщит Казахстана», которая определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий – [15].

Выполненные разработки представляют собой работающую модель корпоративной сети с установленным и настроенным эффективным и надежным современным инструментарием обеспечения защиты информации с функционирующим прототипом информационной системы, обеспечивающей быстрый доступ и установку политик безопасности корпоративных данных на всех уровнях корпоративной сети.

**Список литературы**

1. Usage share of operating systems. URL: <https://en.wikipedia.org/wiki/Usage_share_of_operating_systems> (дата обращения: 15.06.2018).
2. Windows Information Protection (WIP). URL: <https://docs.microsoft.com/ru-ru/windows/uwp/enterprise/wip-hub> (дата обращения: 15.06.2018).
3. Обзор возможностей System Center Configuration Manager (SCCM), URL: <https://www.youtube.com/watch?v=I5tsGH6W6MU>; История версий и функциональные возможности, URL: <https://ru.wikipedia.org/wiki/System_Center_Configuration_Manager>; Документация System Center Configuration Manager, URL: <https://technet.microsoft.com/ru-ru/library/mt346023.aspx> (дата обращения: 15.06.2018).
4. Установка и базовая настройка System Center Configuration Manager. URL: <https://www.youtube.com/watch?v=WUbX3HaI924>, SCCM Current Branch установка пакетов и азы работы с контентом. URL: <https://www.youtube.com/watch?v=3URpErD0F9E&t=136sm> (дата обращения: 15.06.2018).
5. Установка домена Active Directory в Windows Server 2016. URL: <https://vmblog.ru/ustanovka-domena-active-directory-v-windows-server-2016/>, <https://www.youtube.com/watch?v=CCiGnwSbX3I>, <https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/deploy/install-a-new-windows-server-2012-active-directory-forest--level-200-> (дата обращения: 15.06.2018).
6. Схема Active Directory. URL: <http://winintro.ru/schmmgmt.ru/html/b2df785e-69ad-4c2c-b3c4-c260b890ac04.htm>, <http://windata.ru/windows-world/lokalnaya-set/active-directory-osnastka-sxema/> (дата обращения: 15.06.2018).
7. Установка административных разрешений в оснастке «Схема Active Directory». URL: <http://winintro.ru/schmmgmt.ru/html/aa55c3f0-1f54-47a3-a3fd-118ad7de562a.htm> (дата обращения: 15.06.2018).
8. Документация «Prepare Windows Servers to support System Center Configuration Manager». URL: <https://docs.microsoft.com/en-us/sccm/core/plan-design/network/prepare-windows-servers> (дата обращения: 15.06.2018).
9. Windows ADK. URL: <https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install> (дата обращения: 15.06.2018).
10. SCCM 1606: Step by Step Walk-through Setup, URL: <https://social.technet.microsoft.com/wiki/contents/articles/36614.sccm-1606-step-by-step-walk-through-setup.aspx>; SCCM 2016 – Install System Center Configuration Manager 2016, URL: <https://harmikbatth.com/2017/02/02/sccm-2016-install-system-center-configuration-manager-2016/>; SCCM 1606-1702 Step by Step Installation Guide, URL: <http://eddiejackson.net/web_documents/SCCM_2016_Setup_Created_by_Eddie.pdf>; Configuring WSUS with SCCM Current Branch (Server 2016) (Parts 1-3), URL: <https://everythingsccm.com/2017/03/27/configuring-wsus-with-sccm-current-branch-server-2016-part-i/>, <https://everythingsccm.com/2017/08/04/configuring-wsus-with-sccm-current-branch-server-2016-part-ii-adrs-baselines/>, <https://everythingsccm.com/2018/03/21/configuring-wsus-with-sccm-current-branch-server-2016-part-iii/>; Развёртывание System Center Configuration Manager 1702 (8 частей), URL: <https://itblog.ru.net/sc/sccm/sccm-deployment-part1/> (дата обращения: 15.06.2018).
11. SCCM Upgrade Stuck Checking Prerequisites, URL: <https://www.andersrodland.com/sccm-upgrade-stuck-checking-prerequisites/>, <https://www.youtube.com/watch?v=9fcTRblyLTc>; SCCM Hotfix Stuck on “Prerequisite Check Passed”, URL: <https://emeneye.wordpress.com/2016/08/01/sccm-1602-hotfix-stuck-on-prerequisite-check-passed/> (дата обращения: 15.06.2018).
12. Configuration Manager Client Upgrade Package Distribution Failed. URL: <http://www.kwokhau.com/2014/04/configuration-manager-client-upgrade.html> (дата обращения: 15.06.2018).
13. Создание и проверка сертификата агента восстановления данных (DRA) шифрованной файловой системы (EFS). URL: <https://docs.microsoft.com/ru-ru/windows/security/information-protection/windows-information-protection/create-and-verify-an-efs-dra-certificate> (дата обращения: 15.06.2018).
14. Создание и развертывание политики Windows Information Protection (WIP) с помощью System Center Configuration Manager. URL: <https://docs.microsoft.com/ru-ru/windows/security/information-protection/windows-information-protection/create-wip-policy-using-sccm> (дата обращения: 15.06.2018).
15. Об утверждении Концепции кибербезопасности («Киберщит Казахстан»). Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. URL: <http://mdai.gov.kz/sites/default/files/pages/koncepciya_kibershchit.rus__0.pdf> (дата обращения: 15.06.2018).