УДК 004.65; 681.3.068

Щебланін Ю. М., к.т.н.; **Пелешенко А. В.,** студентка
(Державний університет телекомунікацій. +380 (97) 311 67 12. sheblanin@ukr.net. kuzzya.ap@gmail.com)

БЕЗПЕЧНЕ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА ПРИКЛАДІ MICROSOFT SHAREPOINT 2010

Щебланін Ю. М., Пелешенко А. В. Безпечне функціонування електронного документообігу на прикладі Microsoft Sharepoint 2010. Розглядається питання реалізації безпечного функціонування електронного документообігу в межах підприємства на прикладі безкоштовного рішення Microsoft Sharepoint Foundation 2010. Визначені питання державного врегулювання захисту інформації, що зберігається і передається за допомогою електронного документообігу. Особливу увагу приділено забезпеченню безпеки і захисту Sharepoint. Наведена логічна ієрархія для базового розуміння структури Sharepoint. Розглянуті питання безпеки на рівнях ферми, додатків, облікових записів та операційної системи. Описані стандартні групи користувачів та їх права в системі. Зроблено висновок з приводу того, що вимоги кожного підприємства до функціональних можливостей електронного документообігу і до інформаційної безпеки є специфічними, тому Sharepoint досить вдала реалізація і, доцільно, що увага приділена саме захисту системи Sharepoint.

Ключові слова: електронний документообіг, Microsoft Sharepoint, захист інформації

Щебланин Ю. Н., Пелешенко А. В. Безопасное функционирование электронного документооборота на примере Microsoft Sharepoint 2010. Рассматривается вопрос реализации безопасного функционирования электронного документооборота в рамках предприятия на примере бесплатного решение Microsoft Sharepoint Foundation 2010. Выделены вопросы государственного урегулирования защиты информации, которая хранится и передается с помощью электронного документооборота. Особое внимание уделено обеспечению безопасности и защиты Sharepoint. Приведена логическая иерархия для базового понимания структуры Sharepoint. Рассмотрены вопросы безопасности на уровнях фермы, приложений, учетных записей и операционной системы. Описаны стандартные группы пользователей и их права в системе. В конце статьи сделан вывод по поводу того, что требования каждого предприятия к функциональным возможностям электронного документооборота и к информационной безопасности являются специфическими, поэтому Sharepoint довольно уместная реализация и, целесообразно, что внимание уделено именно защите системы Sharepoint.

Ключевые слова: электронный документооборот, Microsoft Sharepoint, защита информации

Shcheblanin Yu. M., Peleshenko A. V. Secure performance of the electronic document management using the Microsoft Sharepoint 2010 example. The article addresses a matter related to the secure performance of the electronic document management within the enterprise using the example of Microsoft Sharepoint Foundation 2010 free solution. It highlights the matters related to national regulation for the protection of information stored and transmitted using the electronic document management tool. Much attention is given to the Sharepoint safety and security provision. The article provides a logical hierarchy for a basic understanding of the Sharepoint structure, and the security items are examined at the frame, applications and accounts and operating system levels. It gives a description of the default user groups and their rights within the system. At the end of the article the conclusions are drawn that the requirements of each enterprise to the performance of the electronic document management and information security are specific, so Sharepoint is well-becoming implementation, and there is a good reason that attention is given to the Sharepoint system protection.

Keywords : electronic document , Microsoft Sharepoint, system protection, permission, implication, anonymous access, user groups, rights , ports

Постановка проблеми. Одним із найбільш розповсюджених напрямів використання Microsoft Sharepoint є електронний документообіг (ЕДО). Кількість документів, які використовують підприємства у своєму внутрішньому документообігу, постійно зростає. Основною задачею ЕДО є забезпечення цілісності, доступності та конфіденційності інформації. Але, незважаючи на всі переваги використання Sharepoint, існує багато проблем забезпечення захищеності даних, які у ньому обробляються. У більшості організацій прийнято приділяти найсерйознішу увагу питанням безпеки і збереження вмісту Microsoft Sharepoint. Залежно від галузі це може бути пов'язано із законодавчими обмеженнями, що вимагають забезпечення захисту та аудиту доступу до певного контенту.

Зазвичай, система безпеки – це велика тема, яка охоплює не тільки адміністраторів ферми Sharepoint, а й адміністраторів серверів, мережевої інфраструктури і баз даних. Крім делегування управління адміністраторам колекцій сайтів і власникам сайтів в бізнес-

підрозділах, система безпеки також включає щоденне обслуговування кінцевих користувачів. З метою оптимізації роботи інформаційних служб необхідна кооперація адміністраторів інформаційних систем.

Для ефективного застосування орієнтованих на бізнес політик управління інформацією необхідна також тісна співпраця з бізнесом. Для задоволення запитів більшого числа зацікавлених сторін Sharepoint 2010 пропонує гнучку модель безпеки, що підтримує кілька типів перевірки на автентичність і рівнів авторизації дозволів. Однак ця гнучкість має і зворотну сторону: без зрозумілої опублікованої стратегії управління дозволами в організації хаос з питань безпеки може зробити повсякденну роботу дуже складною. Враховуючи всі складові, не дивно, що система безпеки може виявитися складною. Проте, якщо запастися чітким розумінням вимог безпеки, набором технічних інструкцій і здоровим глуздом, цілком можливо побудувати модель безпеки, яка буде і ефективною, і стійкою.

Аналіз останніх досліджень і публікацій. Законом України «Про електронні документи та електронний документообіг» від 22.05.2003 [1] регулюються організаційно-правові основи використання електронних документів (ЕД) у всіх сферах економіки.

Порядок ЕДО визначається державними органами, органами місцевого самоврядування, підприємствами, установами й організаціями усіх форм власності відповідно до законодавства. Суб'єкти ЕДО, які здійснюють його, самостійно визначають режим доступу до ЕД, що містять конфіденційну інформацію, та встановлюють для них систему дозволів.

В інформаційно-телекомунікаційних системах, які забезпечують обмін ЕД, що містять інформацію, яка є власністю держави, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства. А саме Законом України «Про інформацію» [2], Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [3], Законом України «Про державну таємницю» [4]. В публікації [5] зазначено, що нормативно-правові акти вимагають подальшого удосконалення в зв'язку зі слабкою опрацьованістю більшості питань. В той же час специфічні ризики в галузі ЕДО можливо страхувати, що дозволить уникнути наявності нічого не гарантуючих інститутів державного ліцензування і сертифікації.

У публікації [6] розглянуті проблеми зберігання і захисту ЕД на прикладі досвіду ФРН. Наведені вимоги для тривалого зберігання ЕД, стратегії збереження і забезпечення доступності архівної електронної інформації. Особливу увагу приділено проблемі безпеки даних. Виділені загальні та специфічні фактори ризику.

Не вирішена раніше частина загальної проблеми. На сьогодні питання щодо захисту інформації, яка зберігається і передається за допомогою ЕДО досить неврегульоване з законодавчої сторони. У Законі України «Про електронні документи та електронний документообіг» не виділені чіткі вимоги до захисту саме ЕД. Лише у Законі України «Про інформацію» висвітлені поняття захисту інформації, вимоги забезпечення інформаційної безпеки України, що транслюються на порядок ЕДО. Доцільно виділити і економічне питання: для функціонування ЕДО більшість програмного забезпечення (ПЗ), що здатне забезпечити безпеку і захист електронних документів, є пропрієтарним і досить коштовним. Тому окрему увагу приділено застосуванню Microsoft Sharepoint 2010 в якості ПЗ, оскільки у ньому присутня безкоштовна версія Sharepoint Foundation 2010, що призначена для невеликих організацій, яким потрібне безпечне функціонування ЕДО.

Метою статті є розробка рекомендацій щодо забезпечення безпеки і підвищення рівня захисту ЕД на прикладі застосування безкоштовної версії ПЗ Sharepoint Foundation 2010.

Виклад основного матеріалу. Останнім часом, у зв'язку з бурхливим розвитком комп'ютерної техніки і комп'ютерних мереж загального доступу, виникла можливість перенесення частини діяльності господарюючих суб'єктів і державних органів управління в так званий "кіберпростір", під яким слід розуміти циркуляцію вмісту локальних і глобальних мереж, об'єднаних Інтернетом.

Слід відзначити, що у сучасній вітчизняній науковій юридичній літературі відсутні комплексні роботи з питань правового регулювання електронної комерції та ЕДО. Існуючий стан дуже далекий від ідеального і не відповідає інтересам ні держави, ні самих учасників електронної комерції, що також обумовлює актуальність дослідження. Таким чином, комплексне теоретичне дослідження аспектів електронної комерції, а також тісно пов'язаного з нею процесу ЕДО, є доцільним та актуальним.

Основні рішення щодо забезпечення інформаційної безпеки підприємства під час користування ЕДО такі: *аутентифікація* користувачів системи; *розмежування* прав доступу для користувачів; *шифрування* листів і документів; *ведення* історії і статистики роботи з документами; аудит роботи користувачів в системі.

Більшість систем для організації ЕДО мають у собі наступні функції: *реєстрація, обробка і зберігання* документів; *управління* передачею документів між виконавцями; *контроль* виконання; *пошук документів* за атрибутам та повнотекстовий пошук; *робота* із зв'язаними документами; *регламентування* прав доступів; *інтеграція* з зовнішніми системами електронної пошти та інше.

Розглянемо реалізацію ЕДО на прикладі Sharepoint в якості засобу для організації централізованого зберігання документів в електронному вигляді, картотеки документів, що зберігаються на паперових носіях, управління доступом до документів, контролю версій і інші стандартні завдання документообігу. Виділемо основні методи та засоби забезпечення безпеки і захисту самої системи.

Логічна ієрархія Sharepoint. Розглянемо базову термінологію середовища Sharepoint. Поняття «ферма Sharepoint» відноситься до всіх серверів (тобто до зовнішніх веб-серверів, серверів додатків і серверів баз даних), які працюють разом для надання клієнтам сервісів Sharepoint. У межах ферми Sharepoint організація контенту виконана за ієрархічною структурою, що зображена на Рис. 1. Метою цієї ієрархії є організація та захист великої кількості контенту всередині Sharepoint [7].

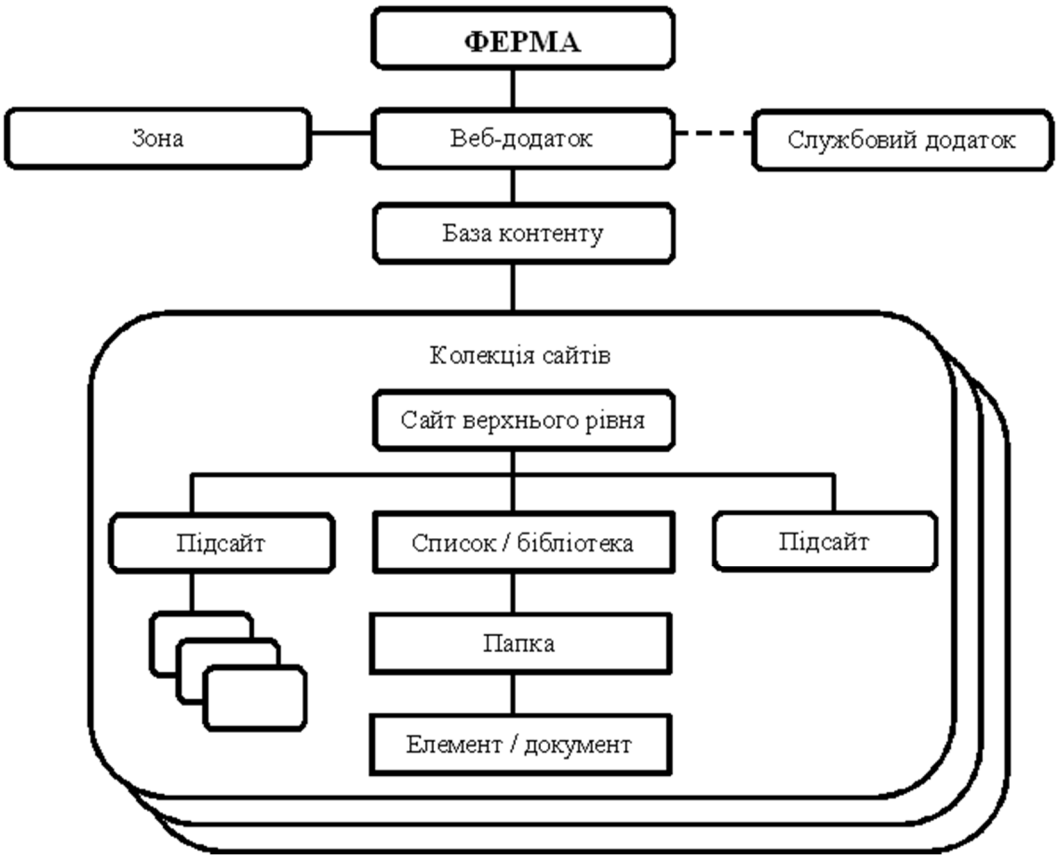

Рис. 1. Логічна ієрархія ферми Sharepoint.

Захист інформації ферми –- процес не дуже складний. Дозволи часто виконуються за принципом "все або нічого": або ви адміністратор ферми, або ні. У адміністратора ферми є права абсолютного контролю, включаючи управління веб-додатками, запуск або зупинку сервісів, резервне копіювання або відновлення ферми. Практично будь-яке завдання можна знайти в Central Administration у веб-інтерфейсі адміністрування Sharepoint. Адміністратор може кожному надати доступ до контенту всередині Sharepoint. Таким чином, адміністратор ферми – фігура вельми могутня, і слід з великою обережністю давати такий рівень доступу.

Щоб виконати певні адміністративні завдання, такі як створення веб-додатків, також необхідно бути локальним адміністратором Windows на веб-сервері або серверах, які запускають веб-додаток Central Administration [9].

Захист веб-додатків. Веб-додаток є точкою входу користувача Sharepoint. Як правило, він складається з одного або декількох веб-сайтів Microsoft Internet Information Server (IIS), які контролюють процес аутентифікації користувачів. При наданні дозволів на доступ до веб-додатків єдина мета – відстежувати, хто має доступ до контенту всередині сайту, який асоціюються з веб-додатками. Цей дозвіл можна надати тільки адміністраторам ферми, і у них повинен бути адміністративний контроль над усіма веб-додатками.

Захист колекції сайтів. Користувачі аутентифікуються на рівні веб-додатків, а авторизація зазвичай виконується на рівні колекції сайтів. Іншими словами, при постійному щоденному управлінні потрібно призначення дозволів через колекції сайтів.

За замовчуванням дозволи наслідуються або передаються послідовно усім веб-сайтам, спискам, бібліотекам, папкам і елементам в ієрархії колекції сайтів. Таким чином, дозволи, які надаються сайту верхнього рівня, також застосовуються до документа, що розташований в глибині колекції сайтів.

Розмежування дозволів. За замовчуванням дозволи встановлюються для сайту верхнього рівня всередині колекції сайтів і застосовуються до всього контенту в ієрархії колекції. Ця концепція допомагає спростити процес управління дозволами.

Доступ до вмісту надається за допомогою рівнів дозволів. Рівні дозволів представляють собою прості в застосуванні поєднання індивідуальних дозволів. Прикладом вбудованого рівня дозволів може служити рівень Contribute, який означає, що користувач має дозвіл на доступ з правом переглядати вміст, додавати, оновлювати і видаляти його.

Звичайно, всередині Sharepoint можна зупинити наслідування дозволів і встановити унікальний ACL, який буде послідовно скидати його нижнім рівнями, на чотирьох об'єктах усередині колекції сайтів: списки або бібліотеки, папки і елементи. Це дає унікальну гнучкість для формування спеціального набору дозволів навколо контенту. Однак, чим більше зупиняти наслідування, тим складнішим стає процес управління дозволами [10].

Як правило, блокування наслідування має застосовуватися тільки у вигляді виключення, і для цього буде потрібно відповідно будувати структуру вузлів, бібліотек і папок.

Анонімний доступ дозволяє неаутентифікованим користувачам отримати доступ до веб-додатків Sharepoint. Анонімний доступ широко використовується для сайтів Інтернету, але його можна застосовувати і у внутрішніх мережах.

Треба відзначити, що за замовчуванням у анонімних користувачів немає доступу до колекцій сайтів до тих пір, поки їм не надано цей дозвіл. Таким чином, після активації анонімного доступу необхідно визначити, які дозволи є у анонімних користувачів.

У Windows Sharepoint Services підтримується 21 право, які використовуються в п'яти групах користувачів вузла за замовчуванням. Ці п'ять стандартних груп користувальницьких прав – «Гість», «Читач», «Співробітник», «Веб-дизайнер» і «Адміністратор».

У Табл. 1 перераховані права користувачів, які за умовчанням включаються в кожну з цих груп [11]. Права, призначені групам вузла «Гість» і « Адміністратор», не можуть бути змінені. Права ж, що включаються в групи «Читач», «Співробітник» і «Веб-дизайнер», можна налаштувати, залишивши в кожній з них лише необхідні. Можна додавати нові групи вузла, комбінуючи різні набори прав, змінювати права, що призначені будь-якій групі, і видаляти групи, що не використовуються. Користувачів не можна включати безпосередньо

до групи «Гість»: у неї автоматично додаються користувачі, яким надано доступ до списків або бібліотек документів на основі дозволів для списків. Група вузла «Гість» не може бути налаштована або видалена. Управляти групами вузла та дозволами на доступ можна на сторінках HTML-адміністрування або за допомогою засобу командного рядка Stsadm.exe. Для виконання завдань управління безпосередньо в коді можна використовувати об'єктну модель Windows Sharepoint Services.

Стандартні групи вузлів Windows Sharepoint і їх права за замовчуванням Табл.1

Ім'я групи вузла	Права користувачів
Гість	Немає.
Читач	*Використання* для самостійного створення вузлів; *перегляд* сторінок; Перегляд елементів
Співробітник	Усі права групи «Читач», плюс: додавання елементів, додавання і видалення особистих веб-частин, перегляд каталогів, створення міжвузлових груп, видалення елементів, зміна елементів, управління власними поданнями, оновлення персональних веб-частин
Веб-дизайнер	Усі права групи «Співробітник», плюс: додавання і налаштування сторінок, застосування тем і границь, відміна вилучань, управління списками
Адміністратор	Усі права групи «Веб-дизайнер», плюс: створення дочірніх вузлів, управління дозволами списку, управління групами вузла, перегляд відомостей про використання

Безпека на рівні системи. Платформа Sharepoint може продемонструвати свої магічні можливості лише за участю широкого кола "дійових осіб", включаючи ОС Microsoft Windows, Microsoft IIS, Microsoft SQL Server і Active Directory (AD). Кожна з цих дійових осіб відіграє важливу роль, але якщо безпека будь-якої з них буде під загрозою, в масштабах ферми Sharepoint може вибухнути справжня катастрофа. Тому забезпечення інформаційної безпеки згаданих компонентів теж входить в коло обов'язків адміністратора Sharepoint.

Windows Update – важливий механізм оновлення серверів, проте застосовувати його до серверів Sharepoint потрібно з обережністю. Цей центр оновлює не тільки систему Windows, а й, в ряді випадків, Sharepoint. Необхідно з уважністю підходити до аналізу кожного оновлення. Наприклад, перед установленням модуля корекції для Microsoft SQL Server необхідно перевірити, чи не призведе ця процедура до порушень в роботі Sharepoint [9]. Установка пакетів оновлень – важлива міра посилення захисту сервера, але застосовувати її слід з дотриманням запобіжних заходів. Зокрема, корисно організувати тестове середовище. Зрозуміло, що тестове середовище ніколи не буде точною копією, але слід подбати про максимальну схожість: застосовувати одні і ті ж версії Windows і Sharepoint, а в процесі налаштування тестового середовища використовувати однакові налаштування.

Ще один спосіб підвищення рівня захисту сервера Sharepoint полягає в блокуванні портів, що не використовуються платформою [8]. Тим самим це зменшує ймовірність того, що зловмисники зможуть зламати сервер за допомогою першої ліпшої шкідливої програми, що використовує уразливість системи. У Табл. 2 представлені деякі порти, часто використовувані серверами Sharepoint для прийому запитів від Інтернет-клієнтів.

До складу пакетів Windows 2008 і Windows 2008 R2 входить майстер налаштування безпеки Security Configuration Wizard (SCW). Майстер налаштування безпеки допоможе визначити, які ролі виконує сервер в даний час і які порти він при цьому використовує. Програму SCW потрібно запускати по завершенні встановлення і налаштування Sharepoint. SCW представить профіль безпеки, який можна застосувати до сервера. Це відносно простий спосіб блокування сервера, але слід бути обережними: можна вимкнути його «назавжди». Треба переконатися, що є чітке уявлення про те, як скасовується будь-яка зміна, внесена майстром SCW. Запускати SCW найкраще в періоди запланованого простою [7].

Висновки. Вимоги кожного підприємства як до функціональних можливостей електронного документообігу, так і до інформаційної безпеки є специфічними і за важливістю не поступаються одна одній. У електронному документообігу опрацьовуються декілька видів інформації - метадані, дані про бізнес-процеси і контент, який потрібно по-

різному захищати. Електронний документообіг – один із елементів інформаційної інфраструктури, який захищається згідно з єдиною політикою забезпечення інформаційної безпеки підприємства, що може грунтуватися на одному чи декількох поширених у світі стандартах. Захищеність визначається рівнем захисту всієї інфраструктури.

Порти, що часто використовуються для входу **Табл. 2**

Порт	Для чого його використовує Sharepoint
TCP 80, TCP 443	Центральний адміністративний порт і будь-який порт, що налаштовується, на якому публікується вміст веб-з'єднання
TCP 32843, TCP 32844, TCP 32845	Взаємодія з додатками сервісів
TCP 32846	Використовується сервісом User Code (рішення типу "пісочниця")
TCP/UDP 445, TCP 137, UDP 138, TCP/UDP 139	Сервіси файлів і друку, що використовуються сервісом Search
TCP/UDP 88, UDP 464	Потрібні, якщо Sharepoint використовує засоби аутентифікації Kerberos
TCP 5725, TCP/UDP 389, UDP 464, TCP/UDP 88, TCP/UDP 53	Використовується додатками сервісу User Profile
UDP 1434, TCP 1433	Застосовані за замовчуванням порти для MS SQL Server; рекомендовано розглянути можливість виконання системи з використанням нестандартних портів і блокування портів за замовчуванням
TCP 25	SMTP, якщо використовується вхідна електронна пошта
TCP 3389	RDP, якщо цей протокол застосовується для доступа до сервера

Реалізація електронного документообігу на прикладі Sharepoint дозволяє досить гнучко підійти до питання забезпечення інформаційної безпеки за рахунок гнучкої моделі системи безпеки, оскільки підтримує кілька типів аутентифікації і рівнів авторизації дозволів.

Загальні рекомендації по забезпеченню достатнього рівня захисту Sharepoint полягають у свідомому розумінні принципів чіткого розмежування дозволів на усіх рівнях системи, обов'язковому ознайомленні з рекомендованою літературою [1, 2, 4]. Також, необхідне регулярне, але й обачне встановлення оновлень, що пов'язані з безпекою.

Література

1. Про електронні документи та електронний документообіг. Закон України від 22.05. 2003 р. № 851-IV [Електронний ресурс] // – Режим доступу: http://zakon1.rada.gov.ua/laws/

2. Про інформацію. Закон України від 2.10.1992 р. № 2657-XII [Електронний ресурс]. // – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12

3. Про захист інформації в інформаційно-телекомунікаційних системах.: Закон України від 5.07.1994 р. № 80/94-ВР [Електронний ресурс] //– Режим доступу: http://zakon4.rada.gov.ua

4. Про державну таємницю. Закон України від 21.01.1994 р. № 3855-XII [Електронний ресурс] // – Режим доступу: http://zakon4.rada.gov.ua/laws/show/3855-12

5. М. Дутов Правові проблеми електронного документообігу // Право України. – 2002. – № 6. С. 122-124.

6. Рудюк В. Проблеми зберігання і захисту електронних документів: досвід ФРН / В. Рудюк // Бібліотечна планета. – 2006. – № 4. – С. 17-21.

7. Основы безопасности Sharepoint [Електронний ресурс] // – Режим доступу: http://www.osp.ru/

8. Руководство по развертыванию Microsoft Sharepoint Server 2010 [Електронний ресурс] // – Режим доступу: http://www.microsoft.com/ru-ru/download/details.aspx?id=10009

9. Руководство по управлению Microsoft Sharepoint Server 2010 [Електронний ресурс] // –Режим доступу: http://www.microsoft.com/ru-ru/download/details.aspx?id=25201

10. Майкл Ноэл, Колин Спенс. «Microsoft Sharepoint 2010. Полное руководство». – Вильямс, 2011. – 880с

11. Архитектура безопасности в продуктах и технологиях Sharepoint [Електронний ресурс] // – Режим доступу: http://www.oszone.net/4632/Sharepoint