УДК 004.056

Ю.В. Борсуковський, В.Ю. Борсуковська

РЕКОМЕНДАЦІЇ ПО КАТЕГОРІЮВАННЮ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

В даній статті проведено детальний аналіз вимог щодо категоріювання інформації з обмеженим доступом для корпоративних користувачів. Сформульовані базові вимоги та рекомендації щодо структури та змісту політики категоріювання інформації з обмеженим доступом з врахуванням досвіду впровадження систем запобігання витокам інформації.

Ключові слова: категоріювання, класифікація, доступ, політика, кібербезпека

Вступ і постановка задачі

Категоріювання інформації в корпоративних інформаційних ресурсах є ключовою функцією забезпечення інформаційної безпеки [3,4,5]. Дане завдання в тому чи іншому вигляді вирішується в кожній інформаційній системі організацій державного та приватного сектору.

Завдяки процесу зіставлення категорій інформації і прав користувачів формалізується та забезпечується процес захисту інформації з обмеженим доступом від несанкціонованого використання [1,2].

У корпоративної мережі кожної організації зберігається і обробляється інформація, яка є життєво важливою для ведення бізнесу, відноситься законодавством України до комерційної та службової таємниці, інформація щодо персональних даних співробітників та інша інформація, доступ до якої може обмежуватися її власником.

З метою забезпечення захисту інформаційних ресурсів від їх незаконного використання, повинна бути розроблена політика доступу до інформації з обмеженим доступом (ІзОД) і встановлений єдиний для всіх користувачів порядок надання, зміни та скасування доступу до ІзОД у відповідності до встановлених політик і який є обов'язковим для виконання всіма без виключення користувачами.

Нижченаведені рекомендації розроблені з метою демонстрації підходу до забезпечення безпеки інформаційних активів, що беруть участь в бізнес-процесах державного і приватного секторів і проведення їх категоріювання.

Рекомендації спрямовані на забезпечення проведення наступних робіт:

- Формування реєстру інформаційних активів;
- Формування системи управління інформаційними активами;
- Розгортання системи протидії витокам інформації.

Зрозуміло, що у роботах з категоріювання інформаційних активів і забезпечення управління ними повинні брати участь усі керівники структурних підрозділів або особи, уповноважені ними, співробітники підрозділів ІТ - адміністратори серверів, на яких розміщуються інформаційні активи, а також фахівці з інформаційної безпеки (ІБ). В процесі виконання рекомендацій повинно бути визначено структурний підрозділ, який управляє і є власником перерахованих нижче процесів.

Терміни та визначення

Для однозначної трактовки термінів їх визначення наведені в таблиці 1.

Таблиця 1

Терміни та визначення

Термін		Визначення
Інформаційний актив	-	Матеріальний або нематеріальний об'єкт, який: є інформацією або містить інформацію, служить для обробки, зберігання або передачі інформації, має цінність для організації.
Інформація з обмеженим доступом (ІзОД)	-	Відомості про осіб, предмети, факти, події, явища і процеси, незалежно від форми їх подання, що є конфіденційною

		інформацією, комерційною таємницею, персональними даними, даними для внутрішнього користування або іншими відомостями, які охороняються відповідно до чинного законодавства України, а також нормативними актами і регламентуючими документами організації.
Підрозділ	-	Відокремлений підрозділ, субхолдинг, акціонерне товариство, компанія, завод, представництво, департамент, управління, відділ, служба чи інша організаційна одиниця, що розробляє конфіденційний документ або курирує його розробку силами сторонньої організації.
Керівники підрозділів	-	Керівники відокремлених підрозділів, субхолдингів, акціонерних товариств, заводів, філій, департаментів, управлінь, служб, відділів чи інших організаційних одиниць, а також їх заступники.
Комерційна таємниця		Інформація з обмеженим доступом, що дозволяє її власникові при існуючих або можливих обставин збільшити доходи, уникнути невиправданих витрат, зберегти положення на ринку товарів, робіт, послуг або отримати іншу комерційну вигоду.
Інформація, що становить комерційну таємницю	-	Науково-технічна, технологічна, інвестиційна, виробнича, фінансово-економічна або інша інформація (в тому числі складова секретів виробництва (ноу-хау), яка має дійсну або потенційну комерційну цінність в силу невідомості її третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим обмеженого доступу до інформації.
Захист інформації		Діяльність щодо запобігання витоку інформації, що захищається, а також несанкціонованих і ненавмисних дій на інформацію, що захищається.
Режим обмеженого доступу до інформації		Правові, організаційні, технічні та інші заходи, які приймаються власником відомостей, що становлять інформацію з обмеженим доступом, з охорони їх конфіденційності.
Категорія ІзОД		Застосовувані класи відомостей для категоріювання інформації за ступенем обмеження доступу.
Категорія ІзОД: строго конфіденційно (СК)		Клас відомостей, що становлять конфіденційну інформацію зі строго регламентованим доступом і захистом – строго конфіденційна інформація.
Категорія ІзОД: комерційна таємниця (КТ)		Клас відомостей, що становлять комерційну таємницю.
Категорія ІзОД: персональні дані (ПДн)		Клас відомостей, що становлять персональні дані співробітників.
Категорія ІзОД: для службового (внутрішнього) користування (ДСК)		Клас відомостей, що містять інші відомості, що містять інформацію з обмеженим доступом - для службового користування.
Категорія ІзОД: публічна (ПБ)		Клас відомостей, що не містять інформацію з відкритим доступом - публічна інформація.
Гриф ІзОД		Застосовувані обмежувальні грифи для маркування інформації за ступенем обмеження доступу: СК, КТ, ПДн, ДСК, ПБ (див. категорії ІзОД).

Виклад основного матеріалу дослідження

Зважаючи на ріст рівня інформаційних та кіберзагроз для організацій державного та корпоративного сектору, варто виокремити декілька основних тверджень щодо підходу до категоріювання інформації з обмеженим доступом.

Твердження 1. Формування реєстру інформаційних активів

Для формування реєстру інформаційних активів необхідно визначити:

1) Перелік інформаційних активів, що обробляються кожним підрозділом, і провести їх категоріювання (визначити клас ІзОД);

2) Перелік інформаційних систем, в яких обробляються та зберігаються інформаційні активи;

3) Перелік місць зберігання носіїв, що містять інформаційні активи (електронні та паперові);

4) Власника інформаційного активу та перелік підрозділів, доступ яким необхідний до активу для виконання співробітниками службових обов'язків.

Прикладами інформаційних активів можуть бути: договір з клієнтами, фінансова звітність, технологічна карта, журнал реєстрації листів, проекти нових продуктів або послуг, ноутбук з інформацією про фінансовий стан підприємства, сервер з інформацією про клієнтів, архів (приміщення) з паперовими справами співробітників підприємства, планшет керівника підприємства з планом перспективної та оперативної діяльності.

Інформаційні активи володіють основними властивостями фінансових та матеріальних активів підприємства: вартість, вартість для організації, можливість накопичення, можливість трансформації в інші активи.

Дуже часто цінність інформаційного активу підприємства може перевершувати цінність всіх фінансових активів. Прикладом такого активу може бути імідж підприємства.

Приклад шаблону реєстру інформаційних активів представлений в Таблиці 1.

Формування реєстру здійснюється шляхом отримання інформації від керівників структурних підрозділів, що обробляють інформаційні активи. При цьому керівники структурних підрозділів або уповноважені ним особи повинні надавати інформацію про всі види інформаційних активів, що отримуються, створюються і передаються в ході реалізації бізнес-процесів співробітниками їх підрозділів.

Твердження 2. Інформаційне наповнення реєстру

Реєстр повинен містити наступну інформацію:

1) Назва інформаційного активу;

2) Місце обробки інформаційного активу (інформаційна система, називання БД, файловий ресурс, обробка в паперовому вигляді і т.д.);

3) Критичність інформаційного активу[1] - конфіденційність, цілісність, доступність;

4) Опис активу - характеристика оброблюваної інформації, опис типових форм і документів (наприклад, картка Т2, форма договору, анкета);

5) Термін зберігання інформаційного активу;

6) Доступ до інформаційного активу - перелік ролей[2] і їх прав.

Примітка - будь-які додаткові відомості про інформаційні активи (порядок отримання активу, порядок передачі всередині організації, передаються чи активи третім особам і т.д.).

Для спрощення процедури збору інформації про інформаційні активи пропонується розробити та впровадити типові форми опитування.

---

[1] Критичність інформаційного активу визначається відповідно до «Керівництва по інвентаризації і оцінці критичності інформаційних активів організації: рівень критичності по конфіденційності, цілісності та доступності».

[2] У разі якщо в організації не реалізована рольова модель доступу і не створена матриця доступу, необхідно надати інформацію про підрозділи, співробітники яких мають доступ до кожного конкретного інформаційного активу.

При цьому керівник структурного підрозділу буде власником інформаційного активу. Надалі, надання доступу до інформаційного активу в обов'язковому порядку повинен узгоджуватися з його власником.

За результатами отримання інформації від керівників структурних підрозділів представляється можливим заповнити частину граф реєстру інформаційних активів (див. Таблиця 1).

Керівники структурних підрозділів на підставі «Переліку відомостей, що становить інформацію з обмеженим доступом» визначають для кожного інформаційного активу його категорію. Ми будем розглядати п’ять типових класів активів: публічна інформація, інформація для внутрішнього (службового) користування, персональні дані, комерційна таємниця, суворо конфіденційна інформація (див. як приклад таблицю 2).

Результати класифікації вписуються в графу 6 реєстру інформаційних активів.

Реєстр інформаційних активів пропонується вести в електронному вигляді і підтримувати в актуальному стані.

Повинні бути визначені власник, місце зберігання і обов'язки з ведення реєстру інформаційних активів.

Твердження 3. Управління інформаційними активами

Для забезпечення безпеки інформаційних активів необхідно документувати і впровадити такі процеси:

1) Надання доступу до інформаційних активів;
2) Забезпечення безпеки носіїв;
3) Структурування інформаційних активів на файлових ресурсах;
4) Повідомлення працівників про правила використання корпоративних ресурсів;
5) Контроль за дотриманням вимог розміщення інформаційних активів.

Твердження 4. Надання доступу до інформаційних активів

Для управління доступом до інформаційних активів доцільно розробити рольову модель, яка включає в себе структуру прав доступу користувачів до інформаційних активів.

Надання доступу до інформаційних активів доцільно здійснювати за заявкою від керівника підрозділу, якому належить співробітник з обов'язковим погодженням доступу з власником інформаційного активу і СлІБ.

Надання доступу має ґрунтуватися на принципі «need to know», тобто співробітники повинні мати доступ тільки до тих активів (даними), які необхідні їм для виконання їх посадових обов'язків, і вони (співробітники) повинні володіти мінімально необхідними привілеями.

Оригінали узгоджених заявок повинні зберігатися в ДІТ. Копії погоджених заявок повинні передаватися в електронному вигляді в СлІБ.

Періодично необхідно проводити інвентаризацію облікових записів, що підтверджує що:

1) Для всіх активних облікових записів існують узгоджені заявки;
2) Усі облікові записи звільнених співробітників заблоковані;
3) Неперсоніфіковані, колективні, групові облікові записи не використовуються для цілей адміністрування;
4) Всі тестові облікові записи активні тільки на час проведення робіт.

Результати інвентаризації повинні оформлятися у вигляді акту, що описує результати перевірки.

Всі знайдені невідповідності реальних прав доступу наявними заявками повинні бути усунені.

Твердження 5. Забезпечення безпеки носіїв

Носії інформаційних активів необхідно захищати. Для цього доцільно:

1) Промаркувати носії інформації;
2) Регулярно проводити інвентаризацію носіїв інформації;
3) Забезпечити їх фізичну безпеку;
4) Визначити порядок доступу до носіїв інформації.

Таблиця 2

ПЕРЕЛІК ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ ІНФОРМАЦІЮ З ОБМЕЖЕНИМ ДОСТУПОМ

А1. СУВОРО КОНФІДЕНЦІЙНІ ВІДОМОСТІ

А1.1. Відомості про структуру організації та її власників

№ зп	Перелік відомостей	Гриф
1	Відомості про корпоративну структуру організації	СК
…	……	СК
n	Відомості про плани зміни структури акціонерного капіталу.	СК

А1.2. Відомості щодо забезпечення загальної безпеки

№ зп	Перелік відомостей	Гриф
1	Відомості про діяльність, структуру, штат департаменту з питань безпеки та служби інформаційної безпеки.	СК
…	……	СК
n	Відомості, що розкривають об'єкти зацікавленості департаменту з питань безпеки та служби інформаційної безпеки.	СК

А2. ВІДОМОСТІ, ЩО СКЛАДАЮТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ

А2.1. Відомості фінансового і економічного характеру

№ зп	Перелік відомостей	Гриф
1	Відомості, що розкривають порядок і строки забезпечення фінансовими засобами.	КТ
…	……	КТ
n	Відомості, що містяться в регістрах бухгалтерського обліку, бухгалтерські звіти (крім тих, які опубліковані).	КТ

А2.2. Відомості про системи автоматизації, зв'язку і технічних засобах

№ зп	Перелік відомостей	Гриф
1	Зведені відомості про використовувані засоби зв'язку і автоматизації, їх стан і плани щодо їх модернізації.	КТ
…	……	КТ
n	Відомості, що містяться в базах даних, що належать організації та / або використовуються ним.	КТ

А2.3. Відомості що представляють собою «ноу-хау», стосуються технології виробництва продукції, проведення робіт і надання послуг

№ зп	Перелік відомостей	Гриф
1	Відомості з технічних розробок і проектів, що містить оригінальні рішення (know-how).	КТ
…	…..	КТ
n	Відомості про програми перспективних досліджень і розробок, їх цілі та завдання.	КТ

А2.4. Відомості по зовнішньої діяльності та взаємовідносинам

№ зп	Перелік відомостей	Гриф
1	Відомості, що розкривають зміст матеріалів обстежень замовників, що включають інформацію з обмеженим доступом.	КТ
…	……	КТ
n	Відомості, що розкривають зміст комерційних пропозицій клієнтам, в тому числі конкурсних пропозицій.	КТ

А2.5. Відомості про виробничі процеси

№ зп	Перелік відомостей	Гриф
1	Відомості про результати внутрішніх перевірок та звіти про стан виробництва.	КТ
…	……	КТ
n	Відомості про інвестиційні плани і техніко-економічних обґрунтуваннях таких планів.	КТ

А3. ВІДОМОСТІ ДЛЯ СЛУЖБОВОГО КОРИСТУВАННЯ

А3.1. Відомості з організаційно-штатних питань

№ зп	Перелік відомостей	Гриф
1	Відомості, що стосуються допуску до конфіденційної інформації працівників.	ДСК
…	…..	ДСК
n	Відомості, що містять персональні дані працівників.	ПДн

А3.2. Відомості про виробничі процеси

№ зп	Перелік відомостей	Гриф
1	Відомості про порядок формування виробничих програм, нормативів витрачання сировини, матеріалів та енергоресурсів.	ДСК
…	…..	ДСК
n	Відомості про порядок організації технологічних процесів виробництва продукції, а також відомості про затвердженій номенклатурі, обсяг і якість продукції.	ДСК

А3.3. Відомості про забезпечення охорони об'єктів

№ зп	Перелік відомостей	Гриф
1	Відомості, що розкривають порядок пропускного режиму на об'єктах організації, заходи, що його забезпечують.	ДСК
…	……	ДСК
n	Інструкції служби безпеки.	ДСК

А3.4. Відомості щодо забезпечення інформаційної безпеки

№ зп	Перелік відомостей	Гриф
1	Відомості, що розкривають значення діючих кодів, паролів, які використовуються для підтвердження повноважень при встановленні зв'язку і доступу до інформаційних систем організації.	ДСК
…	……	ДСК
n	Відомості про грубі порушення вимог інформаційної та кібернетичної безпеки.	ДСК

А3.5. Відомості щодо …

	==========	

Носії інформації рекомендується промаркувати наклейками, що містять обліковий номер і найменування класу активу. При цьому носії інформації доцільно враховувати у відповідних журналах і проводити регулярну інвентаризацію носіїв (рекомендується проводити інвентаризацію не менше, ніж раз на рік).

Для забезпечення фізичної безпеки носіїв інформаційних активів рекомендується обмежити доступ в приміщення, де здійснюється їх обробка та зберігання. Носії, на яких зберігається і / або обробляється строго конфіденційна інформація, комерційна таємниця або інформація для внутрішнього користування, доцільно зберігати в приміщеннях, обладнаних системою контролю доступу.

Матеріальні носії доцільно зберігати в сейфах або шафах, що замикаються.

ISSN 2409-7292

Таблиця 3

Шаблон реєстру інформаційних активів

ID активу	Назва активу	Місце розміщення [3]	Власник активу	Контактна інформація власника активу	Клас активу	Критичність активу (К, Ц, Д)	Короткий опис активу	Термін зберігання інформації	Доступ до активу	Дата занесення в реєстр	Примітка
1	2	3	4	5	6	7	8	9	10	11	12
010101	*Звіт щодо аналізу ризиків*	*SRVVM01/Risk*	*Керівник відділу аналізу ризиків*	*392-29-29*	*Строго конфіденційний*	*К4 Ц4 Д2*	Підсумкові звіти щодо аналізу ризиків	*3 роки*	Відділ аналізу ризиків - повний доступ	*21.12.2017*	Дані не можуть бути передані стороннім організаціям.
020101	*Трудовий договір*	*SRVVM01/OK/ LaborContract*	*Керівник відділу кадрів*	*392-23-23*	*Для службового користування*	*К2 Ц4 Д2*	Документ, що містить ПДн працівників: ПІБ, посада, паспортні дані, адреса проживання	По досягненню мети обробки ПДн	Відділ кадрів - повний доступ	*21.12.2017*	Дані не можуть бути передані стороннім організаціям.
020201	*Резюме співробітників*	*SRVVM01/OK/ Resume*	*Керівник відділу кадрів*	*392-23-23*	*Персональні данні*	*К2 Ц4 Д2*	Документ, що містить ПДн працівників: ПІБ, освіту, досвід роботи	По досягненню мети обробки ПДн	Відділ кадрів - повний доступ, HR - відділ - читання	*21.12.2017*	Документи надходять безпосередньо від кандидатів на працевлаштування на e-mail співробітникам відділу кадрів.
030101	Маркетингові матеріали	*SRVVM03/Mark/* Marketing*Pictures*	*Керівник відділу маркетингу*	*392-23-32*	*Публічний*	*К1 Ц4 Д2*	Рисунки для створення внутрішніх презентацій, документів та ін.	*Не обмежено*	Відділ маркетингу - повний доступ, Решта підрозділів - читання, запуск	*07.03.2015*	Дані можуть бути передані стороннім організаціям по узгодженню з керівником відділу маркетингу.
...	...	...	...	...	...	...	...	...	...	...	...
091956	*Звіт щодо аналізу вразливостей IT систем*	*SRVVM03/CISO/* VulnerabilityIT	*Керівник СлІБ*	*392-09-11*	*Строго конфіденційний*	*К4 Ц4 Д2*	Підсумкові звіти щодо аналізу вразливостей IT систем організації	*6 міс.*	СлІБ та ДІТ	*01.08.2017*	Дані не можуть бути передані стороннім організаціям.
091957	*Політики безпеки*	*SRVVM03/CISO/* PolitikIS&IT	*Керівник СлІБ*	*392-09-11*	*Для службового використання*	*К2 Ц4 Д2*	Політики безпеки організації	*Не обмежено*	СлІБ	*01.01.2010*	Дані не можуть бути передані стороннім організаціям.

[3] Точне місце розміщення інформаційного активу: інформаційна система, шлях до директорії на файловому сервері, місце зберігання носіїв - паперових і електронних

Доступ до носіїв, які містять інформаційні активи, необхідно надавати відповідно з виробничою необхідністю, в рамках виконання співробітниками своїх посадових обов'язків.

Твердження 6. Структурування інформаційних активів на файлових ресурсах

Пропонується упорядкувати інформаційні активи, що розміщуються на файлових ресурсах. Для цього ДІТ з урахуванням інформації, документованої в реєстрі інформаційних активів, формує архітектуру каталогів.

Орієнтовна структура каталогів представлена на Рис. 1.

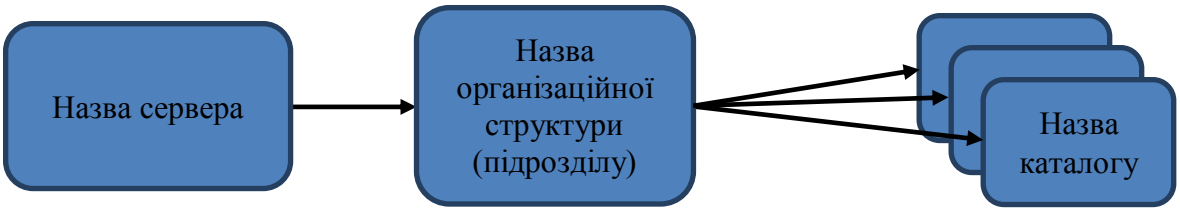

Рис. 1. Пропонована структура каталогів

Наприклад, для резюме, доступ до яких мають працівники відділу кадрів і розміщених на сервері SRVVM01, допустимо наступне назва каталогу: SRVVM01/OK/Resume.

Назви каталогів доцільно узгодити з керівниками структурних підрозділів - власниками активів. За результатами узгодження коригується графа 3 реєстру інформаційних активів.

ІТ фахівці - адміністратори серверів формують нову структуру каталогів і розмежовують права доступу до нових папок відповідно до графи 10 реєстру інформаційних активів. ІТ фахівці також визначають максимальний розмір дискового простору каталогів верхнього рівня.

Після завершення процесу створення структури каталогів, керівники структурних підрозділів або уповноважені особи все дані, що зберігаються на корпоративних ресурсах, переглядають і переносять (копіюють) їх відповідно до виділених каталогів. При цьому всіх користувачів даних інформаційних ресурсів необхідно повідомити про процес перенесення даних і представити їм опис нової структури зберігання інформаційних активів.

Після цього рекомендується застосування автоматизованих кошти інтелектуального аналізу файлових сховищ, використання яких дозволяє підвищити ефективність управління файловими сховищами.

Твердження 7. Повідомлення працівників про правила використання корпоративних ресурсів

Пропонується по електронній пошті провести розсилку внутрішнім адресатам з визначенням вимог щодо розміщення документів на корпоративних ресурсах. Вимоги щодо розміщення документів пропонується оформити окремим документом - «Правила розміщення інформаційних активів на корпоративних ресурсах».

До складу правил пропонується включити:

Вимоги по необхідності зберігання документів тільки відповідно до прийнятої структури;

Перелік категорій інформації, доступної для розміщення на корпоративних ресурсах (наприклад, документи, призначені для роботи);

Перелік інформації, розміщення якої заборонено на корпоративних ресурсах (наприклад, інформація особистого характеру, відеофільми, фотографії та ін.);

Вимога своєчасно видаляти інформацію, яка не потрібна для виконання бізнес-процесів і цілі обробки якої, досягнуті.

Будь-яку іншу інформацію, що стосується підвищення корпоративної культури роботи з файловими сховищами.

У внутрішні документи організації доцільно прописати відповідальність працівників за дотримання поточних вимог.

Твердження 8. Контроль за дотриманням вимог розміщення інформаційних активів

Контроль за дотриманням вимог щодо розміщення інформаційних активів здійснюють власники інформаційних активів. З періодичністю не рідше одного разу на півроку-рік власник інформаційного активу повинен переглядати дані в каталогах на предмет виконання вимог щодо їх розміщення.

Висновок

Питання організації безпеки інформації з обмеженим доступом, а зокрема управління зберіганням та наданням прав доступу до неї, на даний час досить гостро стоїть у цілому світі. Особливо це актуально для організацій, що починають впроваджувати автоматизовані DLP-системи (системи запобігання витокам інформації) Проаналізовані і сформовані рекомендації та вимоги щодо категоріювання ІзОД для організацій різних форм власності можуть допомогти суттєво зменшити ризики пов'язані з несанкціонованим доступом до конфіденційної інформації, втратою інформаційних ресурсів, компрометації інформаційних ресурсів організацій і т.п. Подальші дослідження варто зосередити на створенні та впровадженні типового положення про інформацію з обмеженим доступом та захисту інформаційних активів організацій державного та корпоративного сектору економіки, навчанні та тренінгам персоналу правилам класифікації інформації.

Список використаної літератури

1. Управління доступом. TechNet - Microsoft (https://technet.microsoft.com/ru-ru/library/cc770749(v=ws.11).aspx)
2. Рольове управління доступом для IBM Systems Director Console (*http://www.ibm.com/support/knowledgecenter/ru/ssw_aix_71/com.ibm.aix.sysdircon/rbac_main.htm*)
3. Левкин Р. Внедрение DLP-системы на предприятии (https://www.anti-malware.ru/analytics/Technology_Analysis/introduction_DLP_system_enterprise)
4. Защита от потери данных – Microsoft (*https://technet.microsoft.com/ru-ru/library/jj150527(v=exchg.150).aspx*)
5. Практические аспекты внедрения системы защиты от утечек данных. (*http://old.s-director.ru/443cb001c138b2561a0d90720d6ce111/fe5d43d94d46a8221baaec6d2141bf0d/magazineclause.pdf*)

Надійшла: 11.09.2015 Рецензент: к.т.н., доц. Курченко О.А.