УДК 004.4

М.В. ФЕНЮК

АНАЛІЗ НЕДОЛІКІВ СИСТЕМ АВТОМАТИЗОВАНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА МЕТОДІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ, ЯКІ В НИХ ВИКОРИСТОВУЮТЬСЯ

Анотація. *У статті розглядаються різноманітні системи захисту інформації з використанням біометрії, їхні недоліки, які створюють проблеми при роботі автоматизованих систем. Розглядаються методи, що дозволяють усувати недоліки та використовувати їх у боротьбі із зловмисниками.*
Ключові слова: *захист інформації, IDS-системи, міжмережеві екрани, інформаційна безпека, інсайдери, антивіруси, DLP-системи.*

Аннотация. *В статье рассматриваются различные системы защиты информации с использованием биометрии, их недостатки, создающие проблемы при работе автоматизированных систем. Рассматриваются методы, которые позволяют устранять недостатки и использовать их в борьбе со злоумышленниками.*
Ключевые слова: *защита информации, IDS-системы, межсетевые экраны, информационная безопасность, инсайдеры, антивирусы, DLP-системы.*

Abstract. *This article discusses a variety of information security systems using biometrics, their disadvantages that cause problems in automated systems running. Methods that allow eradicating disadvantages and using them to combat attackers are regarded in the paper.*
Keywords: *information protection, IDS-systems, firewalls, information security, insiders, antiviruses, DLP-systems.*

1. Вступ

При створенні системи захисту інформації враховуються фактори, які можуть понести за собою втрату інформації. До них відносяться і моделі загроз, що представляють собою вхідну інформацію для проектування системи захисту, механізми моніторингу коректності доступу до інформації, автентифікація користувача тощо.

Проектування систем захисту потребує попереднього аналізу діючих систем, виявлення їх достоїнств та недоліків. Отже, розглянемо особливості деяких систем, які забезпечують захист інформації, та їх недоліки.

2. Система виявлення атак (IDS)

Розпочнемо з систем виявлення атак (intrusion detection Systems – IDS). Такі системи використовують для моніторингу та знаходження вторгнень у локальну мережу [1]. Системи прекрасно себе зарекомендували при виявленні атак. Основні особливості таких систем – це те, що вони дозволяють виявляти загрози при спробі злому, автоматично можуть блокувати атаки та повідомляти, на якому сегменті є загроза. Також вони забезпечують документацію усіх загроз, які можуть бути у мережі, та забезпечують контроль за якістю розробки й адміністрування нових систем захисту інформації [2].

Але у них є ряд недоліків, які не дають повністю використати свій потенціал для роботи:

1. IDS-системи можуть хибно спрацювати, тобто спрацювати на дії, які не є загрозою, але для IDS вони можуть здаватися загрозливими, що компрометує систему та може призвести до відмови від неї [3].

2. Атаки, які здійснюються на низькому рівні, по моделі OSI залишаються не поміченими. Зловмисник може використати внутрішню фізичну мережу для отримання

важливої для нього інформації. Це може бути комутаційне обладнання підприємства або установи [3].

3. Якщо використовувати усі механізми аудиту такої системи, то можуть знадобитися ще й додаткові ресурси, що створює незручності у роботі. У час інформаційних технологій немає проблеми для того, щоб збільшити апаратну спроможність для систем, які захищають дані, але проблеми можуть виникнути тоді, коли для IDS та інших систем використовується один сервер на всіх [3].

4. Ще один великий мінус таких систем – це те, що вони не повністю можуть виявити атаки на маршрутизатори. Якщо атака іде ззовні, тоді така система не завжди визначить атаку, так як зловмисник може використати дані співробітників, які мають доступ до офісної робочої станції ззовні [3].

5. Дані, які надаються цим системам, можуть бути не повні. Так як багато з них працюють по сигнатурах і реагують чітко на прописані правила, то деякі атаки вони можуть пропустити. Адміністратор, який відповідає за захист інформації, не завжди може вчасно відреагувати на загрози, що виникають. Для цього йому необхідно проаналізувати загрози, які з'являються і які можуть бути використані проти системи. IDC призначена для того, щоб попереджати про загрози. Але якщо вона не знає, що така загроза існує, тоді вона не може допомогти в її виявленні [3].

6. IDS не може виявити атаки на мережу при максимальних навантаженнях на дану мережу. Причиною цього є повне навантаження на сервери збоку клієнтів чи працівників, і тоді IDS не може відрізнити пакети зловмисника та клієнта. У такому випадку вона може заблокувати усіх або пропустити усі пакети.

Системи IDS прекрасно працюють та дають хороші результати для захисту мережі, але як і будь-який програмний продукт, що розвивається, він має свої недоліки.

3. Міжмережеві екрани

Розглянемо міжмережеві екрани, які використовуються для захисту локальної мережі. Це вдале рішення для того, щоб захистити своїх користувачів від спроб несанкціонованого доступу до мережі ззовні.

Так, як і у IDS, у міжмережевих екранах є недоліки, що можуть скомпрометувати роботу мережі. Основною проблемою, яка не робить міжмережевий екран повністю безпечним для роботи, є те, що його роботу можуть порушити авторизовані користувачі [4]. Він не дозволяє захистити дані від копіювання на змінний носій. Також немає захисту від нестандартних рішень та нових мережевих сервісів, які можуть додаватися до мережі, що теж створює незручності в роботі та налагодженні системи [4]. Ще однією проблемою міжмережевих екранів є продуктивність роботи. При максимальних навантаженнях на мережу та на сам міжмережевий екран продуктивність системи, на яку встановлений екран, дуже знижується, що створює незручності та небезпеку. Адже це може зупинити роботу усієї мережі. Також іноді існують топології мереж, які дуже складно захищати за допомогою міжмережевих екранів.

Ще одна проблема, яка виникає при роботі з міжмережевим екраном, коли у корпоративній мережі використовуються протоколи PPP та застосовуються VPN-з'єднання. Тоді виникає проблема з тим, що дані можуть через ці канали зв'язку передаватися у незахищені сегменти як локальної мережі, так і у відкриту мережу. Небезпечними для міжмережевих екранів є Java, ActiveX-сервіси, які зараз дуже поширені у мережі. Такі сервіси можуть нести загрозу, тому адміністратори часто просто блокують їх, що теж може спричинити незручності в роботі. Однак треба зауважити, що не завжди заблоковані сервіси не несуть загрози для мережі. Треба враховувати той факт, що правильно написаний код для аплету чи сервісу, призначеного для обходу міжмережевого екрана, буде повністю не помітний у мережі.

Віруси, які є уже в середині мережі, та атаки із середини мережі створюють чимало проблем. Системи типу Firewall не можуть захистити мережу, так як не мають засобів захисту від останніх. Виробники намагаються постачати міжмережеві екрани базовими антивірусами, але вони не дуже допомагають, бо завжди працюють з базою сигнатур.

4. Антивіруси

Антивірусні системи [5] базуються на двох методах, за допомогою яких вони проводять пошук вірусів:

1. База уже існуючих вірусів та їх сигнатур. Пошук здійснюється у коді файла та звіряється з даними з бази.

2. Відслідковувати дії програм та виявити дії, які подібні на дії заражених програм.

Дані методи дозволяють знайти та знешкодити вірусну небезпеку, але у двох цих методах є недоліки.

У методі з сигнатурами виникають проблеми, коли база антивірусу не поновлена або з'явився вірус, який ще не потрапив до цієї бази. Це призводить до неправильної роботи як антивірусу,так і усієї операційній системі (ОС). Враховуючи швидкість Інтернету і те, які засоби для передачі даних використовуються в сучасному світі, віруси, черв'яки та трояни досить часто передаються на flash-накопичувачах, через електронну пошту та мережу Інтернету, що теж створює великі проблеми для антивірусів, які можуть не зреагувати на вірус.

У методі 2 антивірус перевіряє дії програм і знаходить аномалії в їх поведінці, також не завжди точно визначає появу вірусу, так як ґрунтується на певній базі подій, що відбуваються. Іноді повністю легальне програмне забезпечення, яке проводить оновлення через Інтернет, сприймається антивірусом як файл, заражений вірусом, що спричиняє незручності в роботі.

Іноді необхідно відключати антивірус для того, щоб провести оновлення або встановити зв'язок з деякими службами, а це вже порушує політику безпеки. У більшості випадків такі дії виконує міжмережевий екран, але все частіше в антивірусні пакети включають міжмережеві екрани.

Однією з основних проблем, яка існує на даний момент, є методи шифрування та дешифрування коду вірусів. Антивіруси не можуть визначити, чи це є програма шифрування, чи вірус, чи робоча програма. Більшість антивірусів мають можливість визначати такі програми, але при написанні вірусів можуть використовуватися зовсім інші методи шифрування та дешифрування. Сам антивірус може генерувати програмний код з сміттям, що не дає змоги антивірусу визначити його присутність. Навіть сильні методи евристики не дозволяють знайти такі віруси. Подібні віруси ще називаються віруси-мутанти або поліморфними. Антивіруси, які не мають якісних евристичних методів для боротьби з ними, не можуть визначити вірусну присутність.

З усього сказаного можна зробити висновки, що системи захисту не мають ефективності поодинці, а в сукупності іноді можуть створювати проблеми в роботі як користувача, так і усієї структури, яку захищають. Немає єдиного центру керування захистом і єдиної політики безпеки усієї мережі.

Враховуючи розвиток ІТ-технологій, не можна встигнути за всіма загрозами, які виникають у світі. Навіть правильно розроблена політика безпеки мережі може бути уже недосконалою через рік і її треба переглядати та вносити зміни в роботу мережі, а також змінювати налаштування усіх систем захисту інформації, що теж створює незручності. З впевненістю можна сказати, що єдина система захисту інформації на підприємстві, у державній установі зняла б деякі проблеми, але не всі. Централізований доступ та обслуговування таких систем дозволяють сподіватися на якісний захист і моніторинг [6].

5. Біометричні системи авторизації та автентифікації

Розглянемо біометричні системи авторизації та автентифікації, які покликані захистити користувачів від зломів систем, але не завжди стають тим захистом, що може забезпечити стабільну роботу. По-перше, ціна на такі засоби досить велика, а робота, наприклад, систем авторизації за відбитком пальця, може давати до 2% похибки, що не дуже надійно.

Автентифікацію [7] біометричних систем можна розбити на декілька категорій, в яких використовуються різні технології. Коротко опишемо кожну категорію:

1. Автентифікація за відбитком пальця – одна з найпопулярніших технологій і відносно не дорога. Популярною вона стала завдяки тому, що її легко використати та застосувати будь-де. Також вона не вимагає якихось особливих дій від користувача. Так як відбитки пальців на протязі життя не змінюються, то їх можна використати для автентифікації.

Виходячи з особливостей систем біометричної авторизації, можна навести і недоліки, які виникають при роботі з цією технологією. Одна з них: можна створити копію, використовуючи латекс або желатин. Дешеві аналоги не мають захисту від такого злому, більш дорогі уже набагато краще захищені, хоча теж не повністю забезпечують надійність. Також самі алгоритми, які використовуються, можуть неправильно вирахувати контрольну суму, що формується під час першої реєстрації користувача.

Інша проблема автентифікації за відбитком пальця в тому, що при передачі даних за межі сканера по незахищеному каналу можна втратити дані, так як їх можна перехопити. Канали шифруються, але чи допоможе це тоді, коли є відомості про шифрування та ключ шифрування?

Ще одна досить поширена проблема для дешевих сканерів у тому, що на сканері залишається відбиток пальця, який можна скопіювати прямо зі сканера та відтворити його.

2. Автентифікація по райдужці ока – одна із самих надійних на даний момент технологій, що використовується на великих підприємствах. Технологія досить дорога та вимоглива до користувачів.

При використанні автентифікації по райдужці ока можуть виникнути технічні проблеми, пов’язані зі скануванням сітківки ока. Іноді сканери неправильно сканують сітківку, що веде до неправильної обробки даних і може заблокувати доступ до ресурсів користувачеві. Основна проблема, яку описують усі спеціалісти, що займаються біометричними системами, це різноманітні муляжі для успішної авторизації. Хоча самі сканери і мають захист від таких речей, але можна використати контактні лінзи, на які наноситься рисунок райдужки ока користувача, що має авторизований доступ до інформації. Це єдина проблема, з якою стикаються розробники подібних систем. Захисту від таких дій не існує, хоча дістати копію райдужки ока складно, але можливо.

На даний час великою проблемою є інсайдери. Це люди, які, працюючи в організації, мають доступ до певної інформації, що може бути конфіденційною, персональною, секретною, а також можуть використовувати її у своїх цілях [8]. Дивлячись на стрімке збільшення атак на різноманітні ресурси та успішні зломи систем, які вважалися захищеними, виникає думка, що щось сталося у всій системі захисту, хоча витік інформації здійснювався саме через інсайдерів, а також через неуважність співробітників.

Розглянемо системи, які забезпечують захист від інсайдерів.

6. Системи запобігання витоків інформації (Data leak prevention – DLP)

Системи для запобігання витоків інформації (Data leak prevention – DLP) [9] призначені для захисту конфіденційної інформації від внутрішніх загроз. Основною метою таких систем є захист від дій інсайдерів та некомпетентних дій працівників, що може призвести до витоку конфіденційної інформації. Одним з представників таких систем є Zecurion DLP

[10]. Системи прекрасно справляються з цією задачею, але, враховуючи різноманітні режими роботи, DLP теж мають недоліки.

Для початку розглянемо два методи роботи системи:

1. Лінгвістичні методи, які ґрунтуються на лінгвістичному аналізі документів і визначені грифами секретності у документі, а також проводять аналіз текстів, які передаються всередині локальної або корпоративної мережі. Лінгвістичні методи аналізу тексту допомагають визначити, до якої категорії відноситься документ, надати йому гриф секретності й відправити у відповідну категорію.

2. Статичні методи аналізують посимвольні дані будь-яких файлів що дозволяє їх використовувати, у порівнянні з лінгвістичним методом, набагато ефективніше при роботі з медіафайлами.

Майже у всіх DLP-систем ці два методи використовуються паралельно, що забезпечує надійність у роботі.

Розглянемо недоліки даних систем. Недоліками їх є те, що перший метод може працювати тільки з файлами мови, яку він розуміє. Враховуючи, що на ринку України працює багато корпорацій з інших країн, то їхні методи можуть не працювати з документами на українській мові. Російські компанії, які розробляють аналогічні системи, краще обізнані з особливостями української мови, так як російська та українська мають спільні корені. Хоча дії і таких лінгвістичних методів не завжди є успішними. Також лінгвістичні методи не можуть успішно опрацьовувати медіафайли та інженерні креслення, які є інтелектуальною власністю. Також не всі продукти можуть аналізувати скановані документи. Основною проблемою для DLP-систем є визначення, до якого каталогу відноситься той чи інший документ. При обробленні тексту у файлах іноді виникає невизначеність, і документ, який має мати гриф секретність, може бути визначений як публічний. У системах використовуються аналоги спам-фільтрів, хоча і допрацьовані.

Якщо взяти статичний метод, то він прекрасно справляється з медіафайлами та файлами, які немає необхідності відкривати, а тільки слід перевірити хеш-ключі, які можуть сказати: чи інформація є однаковою. І інформація повторюється в обох файлах, якщо іде перевірка таких файлів.

Недоліком цього методу є те, що визначення секретності файла покладається на працівника, а це може порушити конфіденційність файлів, якщо працівник не відмітив правильно статус документа (це може бути зроблено навмисне або просто через халатність працівника). Ще одна проблема методу складається в тому, що фізичний відбиток, який має файл, може змінюватися, і коли йде перевірка на наявність змін та створення нового відбитку, це може зайняти багато часу при обробці даних по мережі. Для файлів це не так критично, як для баз даних, що змінюються декілька раз на секунду.

Загальною проблемою DLP-систем є те, що вони не можуть контролювати запис файлів на змінні носії, а це робить таку систему повністю не потрібною, так як вона не може контролювати робочу станцію. Вирішенням даних ситуацій є тільки встановлення бездискових станцій та робота виключно в термінальному режимі, що також навантажує мережу й створює незручності.

7. Система управління доступом до інформації

Розглянувши DLP-системи, перейдемо до розгляду систем управління правами (Documetation Information Rights management-DIRM-системи), які призначені для захисту документообігу [11].

DIRM-системи подібні до DLP-систем. Іноді їх так і називають, але у них немає нічого спільного [11].

DIRM-системи розроблялися як системи для захисту документообігу у корпоративній мережі. Основна задача даних систем – це шифрувати документи, які є

конфіденційними, і права до них надаються централізовано і через асиметричне шифрування.

Звичайно у таких систем є свої недоліки:

1. У них існує ризик того, що система не авторизує людину, яка має права доступу до документів, і це може скомпрометувати систему.

2. Також система не зможе зберегти дані у цілісності, якщо конфіденційною інформацією необхідно буде обмінюватися між різними організаціями, які не мають спільного зв'язку між собою. Тоді система змушена буде розшифрувати дані та передавати їх у незашифрованому вигляді.

3. IRM не може розпізнати декілька однакових копій документів, якщо вони не мають свого грифу. Це може призвести до втрати цінної інформації. Також такі системи не можуть класифікувати документи. Якщо на документи не поширюється політика безпеки системи, тоді це призводить до незахищеності документів.

Основною проблемою DIRM є те, що організація чи підприємство повинні повністю довіряти співробітникам, які виставляють грифи документам, які вони обробляють або створюють. Це викликає великі проблеми при створенні розподіленого доступу до документів та надаванні прав на файли для користувачів.

Враховуючи той факт, що дві системи конкурують між собою, вони дуже злагоджено працюють разом і доповнюють одна одну. Таким чином, при правильному підході до реалізації захисту в середині мережі можна досягнути досить хороших результатів, хоча й не завжди.

8. Системи розподіленого доступу

Системи розподіленого доступу покликані до того, щоб відокремити певні групи від інформації, яка може бути критичною для організації , але також такі системи іноді можуть не дозволити виконати роботу іншим службам, так як людина, що повинна надати інформацію, необхідну іншим службам, може бути відсутня. Це спричиняє незручності в роботі та може скомпрометувати таку систему. У розподілених системах немає повної гнучкості для роботи з даними у критичні моменти часу.

Для демонстрації того, що це означає, наведемо приклад.

Припустимо, що організація продає зброю. Для укладання договору замовнику необхідно переглянути технічні характеристики систем, які вони хочуть купити, та порівняти їх з товаром конкурентів.

Начальника відділу, який володіє такою інформацією, відправили у відрядження, а доступ до цієї інформації є тільки в нього. Тобто авторизацію та ідентифікацію [12] особи на персональному комп’ютері може пройти тільки він, а необхідні для цього файли є тільки в нього в комп'ютері. Інші люди не мають доступу до його комп’ютера. Навіть системний адміністратор не може взяти ці дані, так як вони ще й зашифровані, а ключ шифрування знає тільки начальник відділу. Звичайно він приїде з відрядження й покаже інформацію замовнику, але вона може бути уже не актуальною.

Тут якраз спрацював розподілений доступ. Тут також можна успішно використати комплексний захист інформації [13]. З цієї ситуації є багато виходів, але чи є довіра до людей?

На нашу думку, основною проблемою систем захисту інформації є те, що розробники не хочуть визнати своїх помилок при проектуванні таких систем, а керівництво не хоче визнати, що у них можуть працювати недобросовісні працівники.

Усі атаки, які відбувалися у 2011 році в мережі Інтернет, були успішними тільки тоді, коли в середині організації був інсайдер (юридична або фізична особа, яка має доступ до конфіденційної інформації про справи банку завдяки своєму службовому становищу, участі в капіталі банку, родинним зв'язкам і має можливість використовувати своє

становище у власних інтересах) або людина, яка не була до кінця проінформована, як необхідно реагувати на невідому пошту або невідомий ресурс, на який пропонують зайти.

Тут також є помилка і служб, які займаються безпекою. Їхня провина в тому, що вони, по-перше, не змогли виявити загрозу, по-друге, не проінформували про можливі проблеми керівництво та не організували брифінг для співробітників для проведення тренінгів. Також розробники чітко визначають правила, які діють у системах захисту інформації для кожного користувача. Іноді це не гнучко і заважає роботі, так як один користувач має особливий рід робіт, а робота його колеги перетинається з деякими об'єктами роботи свого співробітника. При виникненні необхідності зміни у цьому перетині, зміни може зробити тільки користувач, який працює в цьому напрямі, а користувач, який працює з даними, не може змінити їх, а може тільки переглянути необхідні йому дані. Така побудова задачі створює незручність і не гнучка, так як при відсутності першого користувача інший не здатний змінити. Таким чином, робота може зупинитися. У більшості випадків дублюють користувача з такими даними, але це не завжди допомагає.

9. Висновки

Напевно, основний технічний недолік будь-якої системи захисту інформації не у ній самій, а у системі, на якій вона встановлена, тобто в ОС.

Будь-яка ОС має багато «дірок», які можна використати для злому її та й усіх встановлених на ній систем захисту інформації.

Одні системи покликані захистити ОС, інші – захистити користувача від можливих спроб злому як ззовні, так і в середині мережі. Але іноді причини витоку конфіденційної інформації настільки банальні, що вся робота по захисту їх зводиться нанівець. Елементарний приклад – це виток даних, записаних на флешку.

Флешку можна згубити, її можна викрасти, а там є важливі конфіденційні документи, що призводить до витоку інформації.

Підведемо підсумки. Що ж робити з усіма проблемами, пов'язаними з системами, які забезпечують захист інформації та захист від вірусної активності? Перш за все необхідно визначити пріоритети, що є основним, які ресурси необхідно захистити. Зовнішні атаки досить просто заблокувати. Слід правильно налаштувати міжмережеві екрани та не випускати назовні непотрібні служби, чітко прописати обов'язки в політиці безпеки локальної мережі організації. Де необхідно встановити біометричне обладнання та обмежити доступ до нього.

Відносно інсайдерів. Можна встановити тотальний контроль та чіткий розподілений доступ, що може спровокувати невдоволення, а краще проробити для кожного працівника, включаючи адміністраторів, бази знань щодо їх прямих та непрямих обов'язків. Автоматизувати процес контролю за працівниками, давши можливість самій системі визначати доступ до інформації, керуючись базою знань, яка накоплюється. Адміністратори будуть мати обмежений доступ, а дозвіл на збільшення привілеїв чи їх зменшення має приймати як мінімум 2 особи. При умові, що доступ необхідний негайно і оператор не має змоги надати такі права, система сама визначає таке право та надає на певний короткий час доступ до необхідної інформації. Приблизно таким чином можна забезпечити певний захист та мінімізувати ризик. Від інсайдерських атак немає технічних рішень, які можуть гарантувати повну безпеку. Вони можуть мінімізувати ризик витоку інформації та дати змогу проаналізувати сегменти мережі, де є проблеми. Також надати певну характеристику працівників, але тотальний контроль не можна вводити. Він тільки зашкодить роботі працівників та знизить їх працездатність.

Помилки, які є в ПЗ (програмне забезпечення), призначеному для захисту інформації, будуть завжди. Іноді вони допомагають знайти проблеми у роботі інших

системних служб та виправити їх, тому немає необхідності задаватися питанням, як зберегти свою інформацію. Необхідно пам'ятати, що інформація може бути актуальною, але з часом вона втрачає свою актуальність.

Переглянемо усі записи щодо активності у напрямі захисту інформації та зробимо певні висновки. А саме, це те, що усі помилки, «дірки» та неправильна робота ПЗ були описані уже давно. Так, наприклад, популярний зараз міжсайтовий скріптинг був озвучений тоді, коли такі мови програмування, як PHP, тільки почали виникати. Популярні Ddos-атаки дійшли до нас, ще коли канали зв'язку могли передавати тільки малі об'єми даних і їх можна було перезавантажити дуже просто. Так, зараз канали зв'язку дуже добре захищені, але що змінилося? Нічого. Помилки в ОС, які були виявлені в 2011 році, також існували там від початку їх створення. Новітні технології розвиваються, але помилки, допущені при розробці технологій, залишаються. Основним завданням необхідно зробити пошук та закриття помилок, напрацьованих протягом років.

СПИСОК ЛІТЕРАТУРИ

1. http://www.internet-technologies.ru/articles/article_223.html.
2. http://kiev-security.org.ua/box/12/141.shtml#AEN482.
3. Жабин С.Ф. Исследование систем обнаружения вторжений операционного уровня информационных систем / С.Ф. Жабин, А.Е. Захаров // Тезисы научно-технического семинара «Координационный совет по информатизации Владимирской области». – 2008.
4. http://citforum.ru/security/internet/fw_pan.shtml.
5. http://bug.kpi.ua/uk/2009-07-15-13-45-05.
6. http://uk.wikipedia.org/wiki/Моніторинг.
7. http://uk.wikipedia.org/wiki/Автентифікація.
8. http://uk.wikipedia.org/wiki/Інсайдер.
9. http://ru.wikipedia.org/wiki/Предотвращение_утечек.
10. http://www.bytemag.ru/articles/detail.php?ID=13844.
11. http://www.securit.ru/solutions/data-loss-prevention.
12. http://uk.wikipedia.org/wiki/Ідентифікація_(інформаційна безпека)#cite_note-pravyla-0.
13.http://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації.

Стаття надійшла до редакції 05.03.2012