УДК 004.9

В.М. Чаплига, О.А. Нємкова

Львівський інститут банківської справи Університету банківської справи НБУ, Львів

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ КОНТУРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ SEARCHINFORM

Розглянуто питання щодо особливостей впровадження контуру інформаційної безпеки фірми SearchInform в навчальний процес вищих навчальних закладів для виконання практичних робіт в рамках дисциплін, пов'язаних із захистом конфіденційної інформації.

Ключові слова: *виток конфіденційної інформації, контур інформаційної безпеки, аналіз перехоплених документів, цифровий відбиток, фразовий пошук, повнотекстовий пошук.*

Вступ

Питання інформаційної безпеки в наш час, коли фактично жодна обробка даних не відбувається без участі комп'ютерів, постають практично перед будь якою фірмою, не залежно від форми її власності та роду занять. Відкритість сучасних комп'ютерних систем, їх складність, а також загальна комп'ютерна грамотність ще більш загострюють ці питання.

Банки є найбільш вразливими до такого виду загроз, як виток інформації, тому питання захисту конфіденційної інформації останнім часом набувають особливої актуальності. Усе це викликає необхідність перегляду підходів до забезпечення безпеки інформації банку, та передбачає необхідність створення відповідних систем захисту [1].

Найчастіше різноманітні фірми потерпають від інсайдерів, що підтверджується статистикою [2 – 4]. За даними компанії InfoWatch, експерта в області систем забезпечення інформаційної безпеки та захисту даних від витоку, приблизно 60% співробітників, що звільнюються, залишають в себе цінні дані підприємства [5]. Основний обсяг витоку інформації найбільш важливих та цінних активів компаній припадає на фінансову кризу 2008-2009 років. За прогнозами економістів Всесвітнього банку та провідних банків України ризик нової кризи призведе до скорочень штату і як наслідок, до потенційного витоку інформації.

Важливі питання для власників успішного бізнесу: «Як захистити свій бізнес? Як захиститись від витоку найбільш важливої комерційної інформації? Кому довіряти?» були, є та будуть поставати з часом все гостріше. Тому створити систему інформаційної безпеки або покращити вже існуючу завжди вигідно і ніколи не пізно.

Системи, що запобігають витоку конфіденційної інформації, в англомовній літературі отримали назву DLP-системи (Data Leakage Prevention). Дани системи знаходять та блокують несанкціоноване передавання (витік) конфіденційної інформації по будь-якому каналу з використанням інформаційної інфраструктури підприємства. Вони мінімізують ризик витоку або знищення даних, саботажу, промислового шпигунства та інших необережних та неправомірних дій співробітників по відношенню до корпоративної інформації. На ринку країн СНД подібні системи називаються «Контур Інформаційної Безпеки» (КІБ, Контур).

Всі ці системи розрізняються за багатьма факторами: технологіями детектування, системними вимогами, позіціонуванням на ринку, контрольованими каналами передачи даних, можливостями контролю зовнішних пристроїв, моніторінгу агентів та їх захисту, управлінням системою та обробкою інцидентів.

Як показує статистика, найчастіше втрати відбуваються через неакуратне ставлення персоналу до інформації, а цей фактор не так легко усунути. До того ж, більшість людей є беззахисними проти методів соціальної інженерії, яка маніпулює або людскою недбалістю, а частіше – їх прагненням зробіти як краще, непомітно порушуючи при цьому посадові інструкції. Тому впровадження КІБ для багатьох підприємств, особливо банків та інших фінансових установ, є виходом з положення для запобігання витоку конфіденційної інформації.

Впровадження системи КІБ в навчальний процес

Все більше фірм цікавляться установкою КІБ у себе [6]. Спеціалісти, що вміють користуватись такими системами, будуть потрібними у все більшій кількості комерційних установ. Для банків це питання стає особливо актуальним з позицій вимог настанови НБУ [1]. Тому доцільно ввести вивчення КІБ у навчальний процес спеціальностей, що пов'язані із безпекою інформаційних систем, банківською діяльністю, економічною кібернетикою.

У Львівському інституті банківської справи (ЛІБС) КІБ вивчають студенти спеціальності Економічна кібернетика в рамках магістерської програми в межах дисципліни «Захист інформації у комер-

ційних установах». Паралельно їм читається курс «Аудит інформаційних систем», оскільки при вивченні Контуру мова йде фактично про внутрішній аудит інформаційної системи установи. Тому багато питань даних дисциплін тісно пов'язані між собою.

Відмітимо, що перед тим як починати вивчати контур, студентам доцільно прослухати дисципліни, що вводять їх у коло питань інформаційної безпеки, знайомлять з базовими поняттями цієї галузі, пояснюють різноманітні види небезпеки, можливі канали витоку інформації, роз'яснюють міри запобігання проявам інцидентів, знайомлять із законодавчою базою. В ЛІБС це дисципліна «Безпека банківської діяльності». Фактично, щоб користуватись певним механізмом захисту, потрібно володіти знаннями і про інші способи захисту, розуміти їх можливості та обмеження. Для розуміння можливостей контуру, способах пошуку інцидентів доцільно прослухати курс «Безпека інформаційних систем».

Також студенти повинні мати чітке уявлення про конфіденційний документообіг на підприємстві, обробку персональних даних, напрями інформаційних потоків. Тобто перед початком ознайомлення з КІБ у студентів повинні бути чітко сформовані погляди на захист інформації в установі.

Для того, щоб обґрунтувати технічні та організаційні вимоги при впровадженні КІБ в навчальній лабораторії закладу, необхідно зробити огляд його функціональних можливостей.

Контур інформаційної безпеки від компанії СофтІнформ - одне з найбільш універсальних і практичних рішень з контролю за інформаційними потоками підприємства на всіх рівнях - від комп'ютера кожного окремого користувача до серверів локальної мережі [6]. Також контролюються усі дані, що йдуть в Інтернет. Контур має модульну структуру, тобто замовник може за власним вибором встановити тільки частину компонентів.

У число модулів контуру входять:

- DataCenter - центр управління всіма індексами (допоміжними файлами, що полегшують та пришвидшують пошук), створеними компонентами контуру інформаційної безпеки. DataCenter дозволяє розбивати індекси на частини, збільшуючи продуктивність пошуку інформації; задавати правила створення нових індексів за певний інтервал часу. Це дозволить відстежувати інформацію тільки за необхідні періоди часу, а також слідкувати за станом роботи всіх компонентів КІБ і відсилати повідомлення на e-mail при будь яких інцидентах.
- Сервер індексації робочих станцій дозволяє в режимі реального часу відслідковувати появу конфіденційної інформації на комп'ютерах користувачів і в інших місцях, для цього не призначених (загальнодоступні мережеві ресурси).
- PrintSniffer дозволяє перехоплювати вміст документів, відправлених користувачем на друк.
- DeviceSniffer перехоплює інформацію, яка записується на різні зовнішні пристрої (наприклад USB-флешки, CD/DVD диски).
- MailSniffer перехоплює всю вхідну і вихідну електронну пошту.
- SkypeSniffer перехоплює голосові та текстові повідомлення Skype.
- IMSniffer перехоплює повідомлення інтернет-пейджерів (ICQ, QIP та інші).
- HTTPSniffer дозволяє перехоплювати інформацію, що відправляється в Інтернет-форуми, блоги та інші web-сервіси.
- AlertCenter - це «мозковий центр» всієї системи безпеки. AlertCenter - самостійний додаток, що опитує всі перераховані модулі і при наявності в перехопленій інформації певних ключових слів, фраз або фрагментів тексту, негайно сповіщає офіцера безпеки - співробітника, відповідального за інформаційну безпеку.

Компоненти Контура інформаційної безпеки перехоплюють документи користувачів. Перехоплення даних здійснюється або сервером NetworkSniffer, або агентами, встановленими на цільові робочі станції користувачів:

- сервер NetworkSniffer слухає мережевий трафік і перехоплює документи користувачів на рівні мережного адаптера. Така схема реалізована для компонентів MailSniffer, IMSniffer, HTTPSniffer;
- агенти встановлюються на робочі станції користувачів і перехоплюють документи користувачів безпосередньо на робочих станціях. Така схема роботи застосовується для компонентів SkypeSniffer, DeviceSniffer, PrintSniffer, Сервер індексації робочих станцій.

У загальному випадку, перехоплена інформація міститься в базах даних SQL-типу:

- сервер NetworkSniffer (компоненти MailSniffer, IMSniffer, HTTPSniffer) поміщає перехоплені повідомлення та файли безпосередньо в бази даних;
- агенти передають дані не безпосередньо в базу, а через сервери керування (Компоненти SkypeSniffer, PrintSniffer і DeviceSniffer);
- окремий випадок - компонент Сервер індексації робочих станцій (сервер IPC). Агенти IPC не поміщають документи в базу даних, а ведуть локальні протоколи файлової системи на робочих станціях користувачів.

Відзначимо, що перевірка перехоплених даних автоматизується за допомогою клієнт-серверного компонента AlertCenter, який дозволяє:

- налаштовувати і зберігати пошукові запити, які використовуються для визначення і містять конфіденційну інформацію документів;
- налаштовувати розклад, за яким відбувається пошук конфіденційних документів;

- отримувати повідомлення, якщо по використовуваним запитам знайдено конфіденційні документи.

Серверний модуль перевіряє перехоплені документи, ідентифікує конфіденційні документи і відправляє оповіщення офіцеру безпеки. Клієнтський модуль використовується для налаштування правил перевірки перехоплених документів.

Налаштування AlertCenter (правила перевірки) і журнал інцидентів зберігаються в базі даних під управлінням Microsoft SQL Server. Повідомлення містять посилання на перегляд перехоплених документів. Пошукові клієнти дозволяють переглянути всі перехоплені документи з можливістю зрізу по даті і користувачам домену. Схема розміщення компонентів КІБ та напрями інформаційних потоків наведено на рис. 1.

Умови лабораторії, де студенти повинні вивчати контур, повинні бути максимально наближені до реальних. Повинний бути організований вихід в Інтернет, щоб можна було користуватись електронною поштою, скайпом, мессенджерами. Бажано мати в аудиторії підключений мережевий принтер. Для забезпечення необхідного обсягу документів, серед яких відбуватиметься пошук конфіденційної інформації, можна організувати в лабораторії заняття інших студентських груп. Учбову аудиторію, в якій планується розташувати лабораторію, доцільно відокремити від основної комп'ютерної мережі учбового закладу. Вихід в Інтернет відбуватиметься через окремий сервер, на ньому встановлюються необхідні компоненти контуру та поштовий сервер. Користування зовнішнім поштовим сервером втрачає сенс, тому що вся переписка при цьому шифрується.

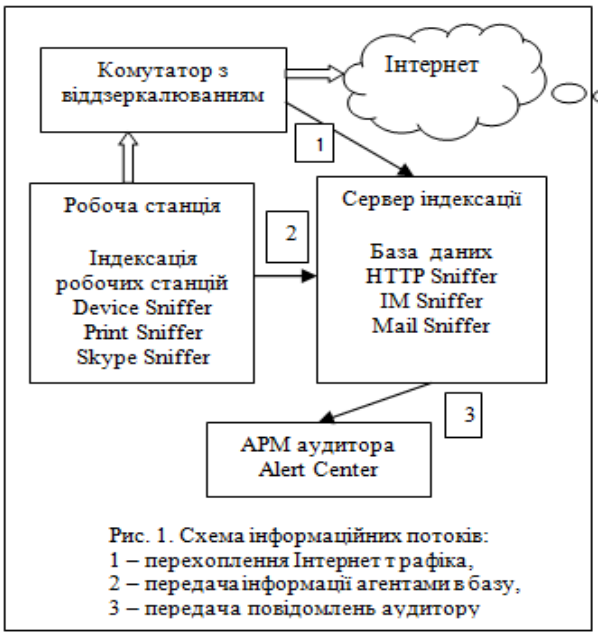

Рис. 1. Схема інформаційних потоків:
1 – перехоплення Інтернет трафіка,
2 – передача інформації агентами в базу,
3 – передача повідомлень аудитору

На кожному комп'ютері лабораторії встановлюються відповідні агенти робочих станцій, тобто кількість ліцензій, що надається при установці, співпадає з кількістю комп'ютерів. Вимоги до серверу такі самі, як до інших серверів мережі закладу, тим більш, що реально великих інформаційних потоків не очікується. Достатньо великим повинний бути жорсткий диск сервера, тому що на ньому має зберігатись база перехоплених документів. Його об'єм повинний складати не менш одного терабайта.

До суттєвих плюсів контуру слід віднести можливість його встановлення віддалено, що робить можливим швидке встановлення при мінімальній участі системного адміністратора закладу. Хоча агенти робочих станцій встановлюються на кожному комп'ютері, тим не менш слід організувати роботу таким чином, щоб була прив'язка до профілю користувача, а не до робочої станції. Кожному профілю виділяється певне місце на загальному диску сервера, в цієї директорії студенти мають змогу зберігати свої документи. Вочевидь, студент має змогу зайти у свій профіль з будь якої робочої станції.

Контур із захисту інформації від «СофтІнформ» комплектується дуже потужним пошуковим модулем. Наявність повнотекстового пошуку є однією з необхідних умов для аналізу інформації. Для більш якісного аналізу та виявлення фактів порушення політики безпеки компанії, продукти «СофтІнформ» надають користувачеві не простий пошук за словами і словосполученнями, а набагато більш інтелектуальні можливості.

Найбільш важливим компонентом будь-якої системи інформаційної безпеки є аналітичний модуль. Саме він дозволяє співробітникам служби інформаційної безпеки оперативно і точно приймати рішення про ступінь конфіденційності перехоплених даних. В КІБ від «СофтІнформ» реалізовані такі типи пошуку:

1. Пошук за словами з урахуванням морфології та синонімів. Це найпростіший вид пошуку, що дозволяє знаходити документи, які містять шукані слова, їх словоформи і синоніми, незалежно від того, в якому місці документа вони знаходяться.

2. Пошук за фразами з урахуванням порядку слів і відстані між ними. При пошуку інформації нерідко потрібно аналізувати документ не за окремими словами, а за словосполученнями (наприклад, прізвища-імені). У цьому випадку фразовий пошук має очевидні переваги, а саме можливість задати порядок слів і відстань між ними. Цей вид пошуку виключає варіант, при якому користувач отримує документ зі словами із запиту, розкиданими по всьому тексту.

3. Пошук регулярних виразів. Такий пошук дозволяє відстежити послідовності символів, характерні, скажімо, для персональних даних, фінансових документів або структурованих записів у базах даних. Наприклад, система відреагує на спробу відправки запису з такими персональними даними, як

прізвище людини, її день народження, номери кредитних карт, телефони та інше.

4. Пошук за цифровими відбитками. Цей вид пошуку передбачає визначення групи конфіденційних документів і зняття з них цифрових відбитків, за якими в подальшому і буде здійснюватися пошук. За допомогою цього методу можна швидко виявляти в інформаційних потоках документи, що містять великі фрагменти тексту з документів, що відносяться до конфіденційних. Основною перевагою методу є висока швидкість роботи, а до недоліків можна віднести його неефективність при внесенні в документ значущих змін і необхідність оперативного створення цифрових відбитків всіх нових документів для можливості їх пошуку.

5. Запатентований алгоритм «Пошук подібних». Інтелектуальні можливості цього типу пошуку дозволяють відстежувати відсилання конфіденційних документів навіть у тому випадку, якщо вони були попередньо відредаговані. У якості пошукового запиту використовуються як фрагменти документів, так і документи цілком. Результатом пошуку є документи, що або містять пошуковий запит цілком, або схожі на нього за змістом.

Студенти повинні засвоїти, що немає чітких правил для визначення способу пошуку в тих чи інших випадках. Мірою правильності вибору зробленого ними виду пошуку буде така характеристика, як ревалентність. Бажано відпрацювати зі студентами кожний вид пошуку окремо, щоб ознайомитись з особливостями кожного з них. Наприклад, коли використовують пошук за словами, необхідно скласти список стоп-слів – таких, що не є ознакою конфіденційності. Тому при застосуванні іншого виду пошуку, наприклад, пошуку за фразами, останній не спрацює, якщо у контрольному виразі зустрічається стоп-слово.

Отже, якщо на початковому етапі студенти мають ознайомитись з можливостями контуру та навчитись елементарним діям з ним, то наступним етапом буде робота над різними варіантами типу «чому в даному випадку пошук не відбувся, хоча мав би відбутись» та навпаки. Чим більше таких варіантів буде опрацьовано, тим більш впевнено буде почуватись майбутній аудитор безпеки.

Якщо доводиться працювати з цифровими відбитками, то тут студенти стикаються з необхідністю весь час поповнювати базу документів, з яких вже знято цифрові відбитки, тому що на практиці маємо постійне оновлення конфіденційних документів установи.

Наступним важливим питанням, яке потрібно відпрацювати зі студентами, є захист самого Контуру. Для захисту робочих станцій від вірусів, троянських програм та іншого зловмисного програмного забезпечення доцільно використати антивірусну програму, що є достатньо простою, наприклад – Avira. Більш потужні антивірусні програми можуть вступати у конфлікт з пошуковими агентами Контуру, які по суті представляють собою сніффери, тому реакція на них в того ж AVK буде однозначною.

Якщо компоненти КІБ включені в загальну локальну мережу, то потрібно використовувати вбудовані засоби захисту самого Контуру. Відразу після встановлення і налаштування компонентів КІБ потрібно провести наступні операції:

- змінити паролі доступу до консолів серверів NetworkSniffer, NSA, DeviceSniffer,SoftInformSearch. Після зміни паролів, доступом до серверних консолів зможе скористатися тільки аудитор служби безпеки і тільки він зможе змінювати налаштування перехоплення даних;
- змінити пароль доступу до клієнта AlertCenter і базі правил перевірки AlertCenter. Після призначення пароля, підключитися до бази правил перевірки AlertCenter зможе тільки аудитор служби безпеки;
- призначити права доступу до індексів. Після цього доступ до проіндексованих даних не під обліковим записом аудитора буде заборонений.

Слід відмітити деякі особливості роботи зі студентською аудиторією. Хоча робота з контуром ставить студентів у положення аудиторів, тобто у майбутньому офіцерів безпеки, тим не менш основні паролі при входженні в контур викладач повинен набирати самостійно. Повідомляти повністю всі паролі для роботи з контуром студентам категорично не рекомендується.

Більш високий рівень захисту забезпечує робота КІБ в ізольованій підмережі. Тому за наявності такої можливості ці заходи рекомендується доповнити організацією ізольованою підмережі і включенням в неї компонентів КІБ.

Доступ до ізольованої підмережі обмежений її співробітниками. Сполучною ланкою між підмережею і основною користувальницької мережею буде сервер з встановленими серверними модулями NetworkSniffer, IPC, DeviceLock. Наприклад, на даний сервер можуть бути встановлені дві мережеві карти, одна з яких буде здійснювати зв'язок з призначеним для користувача доменом, а друга - зв'язок з власною підмережею служи безпеки.

Для перехоплення імен користувачів сервер NetworkSniffer, IPC, DeviceLock повинен працювати під обліковим записом користувача домену. Відповідно до серверних модулів може підключитися користувач з правами адміністратора в основному користувальницькому домені.

Для отримання імен користувачів домену, служба перехоплення NetworkSniffer повинна працювати під доменним обліковим записом з правами читання журналів безпеки. Установка агентів Device-

Lock і керування ними повинно проводитися під доменним обліковим записом з правами адміністратора домену. Сервер індексації робочих станцій також повинен працювати під обліковим записом адміністратора домену. Інші компоненти підмережі повинні працювати під обліковими записами робочої групи.

Якщо підмережа служби безпеки виокремлена в окремий домен, останній повинен бути пов'язаний довірчими відносинами з доменом або доменами, в яких працюють користувачі мережі. Це дозволить серверам NetworkSniffer, IPC і DeviceLock працювати в мережі основного користувача домену під обліковим записом окремого домену служби безпеки, дана схема роботи дозволить захистити всі компоненти КІБ від стороннього доступу.

В багатьох організаціях є користувачі, документи яких повинні бути виключені з перехоплення. Такими користувачами можуть бути: генеральний директор, головний бухгалтер та інші відповідальні працівники. Фільтри обмежень з перехоплення можна задати за допомогою серверних консолей NetworkSniffer, NSA і DeviceLock.

Для цього передбачені наступні можливості AlertCenter: «Білі списки» для користувача атрибутів, а також складні запити з обмеженням по атрибутам документів.

Після вивчення особливостей підключення КІБ та можливих варіантів пошуку слід опрацювати зі студентами створення індексів, призначення розкладу перевірок, створення політик, а також підключення індексів до політик та виконання перевірок.

Висновки

Фінансові установи для впровадження контуру інформаційної безпеки повинні мати чітко розроблену політику безпеки, суттєвою складовою якої є класифікація всієї документації установи на конфіденційну інформацію та інформацію з відкритим доступом.

Впровадження КІБ в навчальний процес, як показує досвід, є можливим та доцільним для всіх спеціальностей, що пов’язані із захистом інформації.

Використання КІБ доцільно не тільки у фінансових установах, а також в компаніях, що працюють з персональними даними (медичними закладами, пенсійними фондами, фірмами мобільного зв’язку, податкової служби), або є власниками цінної технологічної інформації (фармацевтичні фірми, будівельні компанії, фірми що пов’язані з технологіями виробництва харчової продукції).

Розглянутий КІБ має широкій спектр запобіжних дій по відношенню до витоку конфіденційної інформації. Функціонал контуру є ретельно продуманим, вимоги до «заліза» не є дуже високими і по силах майже всім установам, що турбуються про власний захист.

Список літератури

1. Постанова НБУ від 28.10.2010 г. №474. Вимоги до системи управління інформаційною безпекою.СОУ Н НБУ 65.1 СУІБ 1.0:2010, СОУ Н НБУ 65.1 СУІБ 2.0:2010.

2. Скиба В.Ю., Курбатов В.А.- Руководство по защите от внутренних угроз информационной безопасности – СПб.: Питер, 2008. – 320 с.

3. ЄпіфановА.О., ШкольникІ.О., РайхлінгП - Базель II: проблеми та перспективи використання в національних банківських системах - Суми:ДВНЗ «УАБС НБУ», 2011.-261 с.

4. Зубок М. І. - Безпека банківської діяльності - К.: КНЕУ, 2003. — 156 с.

5. www.infowatch.ru

6. Контур информационной безопасности. Руководство аудитора безопасности //www.SearchInform.com

Надійшла до редколегії 26.03.2012

Рецензент: д-р техн. наук, проф. А. П. Бондарєв, Національний університет «Львівська політехніка», Львів.

ОСОБЕННОСТИ ВНЕДРЕНИЯ КОНТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SEARCHINFORM

В.М. Чаплыга, Е.А. Немкова

Рассмотрены особенности внедрения контура информационной безопасности фирмы SearchInform в учебный процесс высших учебных заведений для выполнения практических работ в рамках дисциплин, связанных с защитой конфиденциальной информации.

Ключевые слова: *виток конфиденциальной информации, контур информационной безопасности, анализ перехваченных документов, цифровой отпечаток, фразовый поиск, повнотекстовий поиск.*

FEATURES OF THE CIRCUIT IMPLEMENTATION OF INFORMATION SECURITY SEARCHINFORM

Chaplyga V.M., Nemkova H.A.

There are considered the characteristics of the circuit implementation security of firm SearchInform in the educational process of higher education institutions to carry out practical work in the disciplines related to the protection of confidential information.

Keywords: *coil of confidential information, contour of informative safety, analysis of the intercepted documents, digital imprint, phrase search, search.*