УДК 004.056

С.Т. Іванишин[1]

[1]*Університет банківської справи (м. Київ) Національного банку України*

МЕНЕДЖМЕНТ БЕЗПЕКИ ІТ КОМПЛЕКСНОЇ АВТОМАТИЗАЦІЇ У ТЕРІТОРІАЛЬНО РОЗНЕСЕНИХ ВІДДІЛЕННЯХ БАНКУ

Розглянуто питання інформаційної безпеки при проведенні віддаленого внутрішнього аудиту в банку. Обґрунтована необхідність автоматизації безпеки при проведенні внутрішнього аудиту віддалено через агресивне середовище – Інтернет. Для віддаленого проведення внутрішнього аудиту визначено можливі канали витоку інформації, режими захисту, рівні контролю. Побудована автоматизована модель захисту інформації банку. Надано практичні рекомендації щодо впровадження існуючих систем захисту від витоку.

Ключові слова: внутрішній аудит в банку, захист каналу, захист периметру, контент-контроль, автоматизація безпеки.

Вступ

Актуальний практичний досвід з основних тем менеджменту якості в сучасному банку потребує викладення згідно інтерпретації вимог стандарту ISO 9001:2008. Впровадження системи управління якістю забезпечує високоякісне обслуговування клієнтів банку, економічний ефект систем менеджменту якості (СМЯ), програмні продукти бізнес-моделювання, успішні практики та багато іншого [1].

Керування якістю у банках стосується безпосередньо проведення внутрішнього аудиту [2]. Факт дистанційної роботи внутрішнього аудитора значно ускладнює ситуацію, адже доступ до банківської інформації (конфіденційної, таємної) відбувається через агресивне середовище – Інтернет. Внутрішній аудитор має доступ до різноманітної банківської інформації, він контролює всі банківські процеси. З точки зору забезпечення банківської безпеки окремої уваги потребує діяльність внутрішнього аудитора, адже існує варіант спотворення інформації, переадресації, несанкціонованого її знищення та фальсифікації, хибної авторизації платіжних документів.

Інформаційна безпека в роботі будь якого банку базується на конфіденційності, цілісності та доступності. Для вибору системи захисту цих трьох постулатів банк повинен проаналізувати канали витоку інформації, визначити рівні контролю та режими захисту та обрати один з двох варіантів захисту: захист каналу або захист периметру. При віддаленій роботі внутрішнього аудитора система інформаційного захисту повинна надати йому доступ до будь якої інформації ззовні та забезпечити захист при віддаленому доступі. При цьому може виникнути конфлікт між вимогами систем захисту периметру або каналу з необхідністю передавання даних для роботи аудитора. Для усунення конфлікту потрібно розробити модель безпеки доступу при віддаленому проведенні внутрішнього аудиту в банку. Це питання обговорюється та вирішуються у даній роботі.

Питання безпеки при проведенні внутрішнього аудиту

Процес внутрішнього аудиту можна розділити на п'ять видів аудиту (під процесів) [3].

1. Аудит документації системи управління якістю банку. Проводиться аудиторами дистанційно. Документи представлені в електронному вигляді. Включає перевірку складу та змісту нормативних документів та записів. Основні записи, що розглядаються у стандарті ISO 9001, перевіряються повністю, записи, що стосуються бізнес-процесів, стандартів процесів, посадових інструкцій – вибірково. На основі звітів по бізнес-процесах проводиться оцінка відхилень показників якості.

По суті даний під процес працює з конфіденційною інформацією кількох основних процесів, доступ до неї повинен бути організований дистанційно. Відповідальність за безпеку несуть одночасно аудитор та офіцер безпеки банку (власник бізнес-процесу інформаційної безпеки банку).

2. Вибірковий аудит персоналу та підрозділів. (опитування та інтерв'ю). Проводиться на території банку и охоплює дві категорії співробітників: відповідальних за виконання вимог стандарту ISO 9001; представників керівництва та рядових співробітників. Вибірково по окремих співробітниках перевіряється знання основної документації, знання інструкцій, відповідність до кваліфікаційних вимог, наявність документації на місцях та доступ до всіх необхідних електронних документів.

На даному етапі є небезпека незаконного вибіркового копіювання при доступі до електронних документів. Відповідальними за безпеку під процесу є також аудитор та офіцер безпеки.

3. Вибірковий аудит бізнес-процесів. Проводиться на території банку. Включає спостереження та опитування персоналу на відповідність регламенту бізнес-процесів їх реальному виконанню у банку, перевірку наявності ресурсів та інфраструктури для бізнес-процесів та відповідності електронних документів їх завіреним печаткою версіям.

Небезпека полягає у тому, що аудитор може скопіювати дані на свій робочий ноутбук для детальної перевірки у більш спокійній обстановці. Існує небезпека втрати такого ноутбука, або копіювання з нього даних зацікавленими особами. Відповідальними за безпеку під процесу є аудитор та офіцер безпеки.

4. Аудит задоволення потреб клієнтів. Проводиться на території банку та на базі каналів зворотного зв'язку через опитування.

Присутня небезпека незаконного копіювання персональних даних, а також навмисної та ненавмисної фальсифікації. Відповідальними за безпеку слід вважати аудитора та офіцера безпеки.

5. Аудит якості обслуговування в операційних офісах зазвичай за методикою Mystery Shopper.

При проведенні внутрішнього аудиту слід прийняти до уваги, що аудитор працює зі всіма інформаційними технологіями та системами банку. До основних систем відносяться:

- автоматизована банківська система та допоміжні системи по автоматизації бізнес-процесів;
- програмний продукт бізнес-моделювання;
- CRM-система (Customer Relationship Management) — управління взаємовідносинами та взаємодіями з клієнтами;
- система електронного документообігу;
- канали самообслуговування.

Відповідальним за надійність функціонування таких систем є начальник IT служби, хоча сучасні банки додатково використовують спеціалістів із захисту інформації для обслуговування цих систем саме для забезпечення безпеки інформаційних потоків та даних. Якщо банк купує та встановлює в себе програмний комплекс для забезпечення безпеки, постає питання інтеграції рішення по безпеці з переліченими системами [4].

Для захисту від ненавмисного та навмисного деструктивного втручання доцільно включити ще одну систему, що запобігає витоку інформації, повідомляє про порушення

політики безпеки, контролює всі втручання в інші інформаційні системи і може вважатись запорукою інформаційної безпеки у банку. Однією з таких систем є контур інформаційної безпеки SearchInform. Застосування контуру вирішило б багато питань, що пов'язані з особливостями проведення внутрішнього аудиту, тому що могло б забезпечити канальний захист інформації банку.

Рівні контролю при віддаленому доступі

При віддаленому доступі система контролю за витоком інформації сприйме роботу аудитора як порушення безпеки, якщо не вжити спеціальних допоміжних заходів. Розглянемо це питання більш детально.

Основною задачею захисту від витоку є визначення каналу витоку. У подальшому під такими каналами будуть вважатись електронна пошта, доступ до Інтернету, друк на локальному чи мережевому принтері та змінні носії інформації. Можливі три рівні контролю каналів: первинний, вторинний та третинний [5]. На першому рівні використовується принцип: не дати доступу зовсім, надати тільки в одну сторону, надати в обидві сторони. Як правило, на цьому рівні забезпечується контроль над змінними носіями – флеш-пам'ять, компакт-диск. Цей рівень вважається самим неефективним. Програми, що надають такий сервіс, не вміють розрізняти конфіденційну інформацію від публічних документів. Вони працюють у режимі надати\заборонити доступ. Користувач може або виконати операцію через порт, або не виконати. Не відбувається контроль за контентом. Наприклад, не можна заборонити записувати на флеш-пам'ять дані з конфіденційною інформацією та дозволити записувати публічну інформацію. Те саме відбувається на робочій станції. Якщо у працівника є дозвіл використовувати запис на флеш-пам'ять, він може копіювати все, що завгодно. Застосування спеціальних флеш-носіїв з дозволеною функцією копіювання не рішає проблеми.

Якщо всі файли, що записуються на флеш-пам'ять, архівуються системою у спеціальний архів для подальшого аналізу, то це називають тіньовим копіюванням. Як правило, тіньові архіви кожного користувача зберігаються просто на робочих станціях. Це не дозволяє ефективно перевіряти архіви та суттєво сповільнює роботу робочої станції. До того ж це не запобігає витоку інформації, а лише фіксує його.

Вторинний рівень контролю відповідає за нецільовий доступ до ресурсів зі сторони співробітників. Він використовується після того, коли у співробітника вже є легальний доступ до інформаційного каналу. Наприклад, квотування друкованих документів дозволяє відслідкувати друк сторонніх документів, який робить працівник у своїх інтересах. До вторинного рівня відноситься система білінгу, що контролює трафік. Тим не менш, дані функції не стосуються витоку інформації, хоча на будь якій фірмі чи державній установі вони є корисними.

На третинному рівні контролю перевіряються всі дані, що виходять за межі корпоративної мережі. Всі файли проходять контент – контроль, перевіряються атрибути файлів (ім'я, розмір, формат та ін.). Саме цей рівень контролю покликаний запобігати витоку інформації. Але насправді рівень сучасних систем корпоративної безпеки є далеким від ідеального. Про це говорить статистика: приблизно чверть від загальної кількості витоків не ідентифікована. Тобто виток відбувся, але способу ніхто не знає (звичайно, крім інсайдера).

Слід відмітити, що на вторинному та третинному рівнях можливі три режими роботи: архів, моніторинг та активний захист. Для архівування характерним є копіювання всієї інформації, що виходить за периметр корпоративної мережі, та відповідних атрибутів (час відправлення, дані про відправника, дані про мережу, в яку надіслана інформація). Перевірка архіву проводиться за регламентом.

Моніторинг представляє з себе архів, у якого є функція сигналізації про деякі події, їх ще називають інцидентами. Інформація перед відправкою в архів проходить перевірку контенту та атрибутів відповідно до заданих правил. Правила наперед задані офіцером безпеки виходячи з політики безпеки фірми чи установи. Якщо відбувається співпадіння контенту чи атрибутів на задані правила, тобто відбувається інцидент безпеки,

то офіцеру безпеки надсилається повідомлення. Як правило, це повідомлення приходить на визначену адресу електронної пошти (пошти офіцера безпеки), можна організувати інтернет-пейджер, SMS. Звичайно, моніторинг є кроком вперед порівняно з архівуванням, тому що дозволяє вирахувати інсайдера, але все рівно він не запобігає витоку.

Активний захист є самим сильним засобом проти інсайдерських атак. При виявленні переміщення конфіденційної інформації відбувається призупинення. Пересилання можливо тільки у випадку автоматичного підтвердження на відповідність правилам, що встановлені для даного відправника.

Робота на віддалі для внутрішнього аудитора характеризується двома протилежними тенденціями. З одного боку, аудитор має право доступу до будь-яких документів та даних банку. Це можна забезпечити, надавши йому право доступу до них. Наприклад, у системі запобігання витоку профіль аудитора отримує право доступу до всіх даних. З другого боку, перегляд тих файлів має відбуватись за межами корпоративної мережі. Таким чином, надавши повний доступ до файлів, вже не можна контролювати подальші дії аудитора, тому що системи контролю обмежуються локальною мережею. Пересилання відбувається через зовнішнє середовище, де може відбутись виток інформації.

Автоматизація безпеки роботи зовнішнього аудитора

Таким чином, безпечна робота внутрішнього аудитора зводиться до рішення трьох питань: по-перше, потрібно надати право перегляду будь якого документу зовнішньому користувачу з профілем аудитора; по-друге, захистити інформацію від читання при можливому перехопленні; по-третє, забезпечити захист від витока на комп'ютері аудитора. Дані задачі можуть бути вирішені в наступній моделі, рис.1.

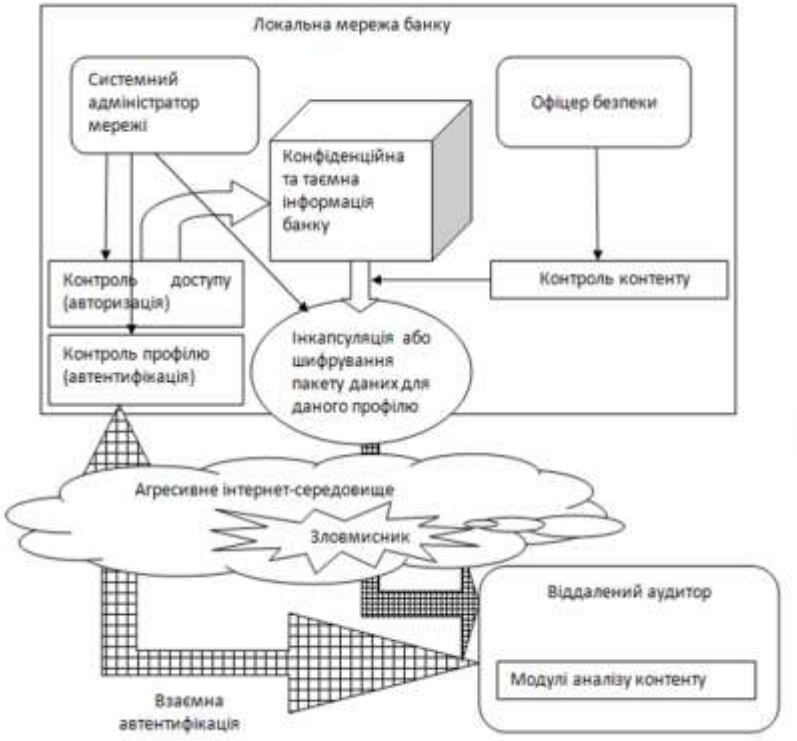

Рис.1. Модель автоматизації безпеки при віддаленому доступі.

Сеанс зв'язку віддаленого аудитора з локальною мережею починається з проходження взаємної автентифікації. При цьому локальна мережа переконується, що має справу з віддаленим аудитором, а аудитор переконується, що буде працювати з локаль-

ною мережею. Відмітимо, що в даній ситуації стороною, яка активізує процес, є віддалений аудитор. Тому для проходження автентифікації він має застосувати сувору автентифікацію, для чого можна використати електронний ключ – токен. Ніяка початкова інформація від аудитора не повинна виходити у відкритій формі, обов'язково потрібне шифрування. Тому слід наперед синхронізувати токен із системою контролю локальної мережі. Для цього можна застосувати набір спеціальних шифрувальних таблиць. Автентифікація відповідає первинному рівню контролю. На даному рівні варто проводити архівування журналу сеансів зв'язку. Відповідальним за первинний рівень є системний адміністратор. Після проходження первинного рівня аудитор отримує права загального користувача в локальній мережі банку.

На вторинному рівні відбувається авторизація віддаленого аудитора, надається доступ до ресурсів банку згідно статусу користувача - внутрішнього аудитора. Відповідальним за рівень є системний адміністратор. Він виконує стандартні операції білінгу, квотування за часом або за обсягом, збирає статистику. На даному рівні доцільним використовувати режим моніторингу.

Після того, як встановлено доступ до ресурсів локальної мережі банку, внутрішній аудитор починає свою роботу. Всі дані, перед тим як вийти з локальної мережі, повинні бути або зашифровані сеансовим ключем аудитора, або повинне бути застосовано VPN-з'єднання (віртуальна приватна мережа). Відповідальним за це є системний адміністратор мережі. За контроль контенту на третинному рівні відповідає офіцер безпеки. Для проведення операцій по аналізу контенту необхідно, щоб на ноутбуці аудитора були встановлені компоненти контуру інформаційної безпеки, їх набір такий самий, як для будь якої робочої станції локальної мережі. Вимога на обмін інформацією між модулями аналізу контенту на ноутбуці аудитора та центром безпеки, що знаходиться в локальній мережі, така сама, що для даних – інформація повинна або проходити шифрування, або використовуватись VPN-з'єднання. Для уніфікації процесу представляється більш правильним використання VPN-з'єднання. Таким чином з точки зору офіцера безпеки робота віддаленого аудитора нічим не відрізняється від роботи будь якого користувача локальної корпоративної мережі. Тому офіцер безпеки налаштовує модулі, що відповідають різним каналам передавання інформації: за e-mail, друк документів, копіювання на змінні носії, вихідні інтернет-повідомлення так саме, як би аудитор працював у середині корпоративної мережі. На даному рівні потрібно застосовувати самий жорсткий та ефективний режим захисту – активний захист, який зупиняє операцію переміщення інформації по каналу.

Висновки

Сучасні системи запобігання витоку інформації здатні забезпечити аналіз контенту при віддаленому режимі роботи внутрішнього аудитора. Для цього на комп'ютері аудитора мають бути встановлені спеціальні модулі – агенти безпеки каналів. Первинний та вторинний рівні контролю має забезпечувати системний адміністратор. Таким чином можлива повна автоматизація безпеки віддаленої роботи з функціями контролю всіх рівнів.

Література

1. Cobit 4.1 (повна версія)/ - [Електронний ресурс]. - Режим доступу : http://ea-banks.ucoz.ru/load3-1-0-3.
2. Закон України. Про банки і банківську діяльність. Стаття 45. Внутрішній аудит. - [Електронний ресурс]. - Режим доступу : http://kodeksy.com.ua /pro_banki_i_bankivs_ku_diyal_nist/statja-45.htm.
3. Исаев Р.А. "Типовая система менеджмента качества коммерческого банка и ее архитектура" часть 1 и часть 2 / Р.А.Исаев // "Методы менеджмента качества" № 11-12'2010 –

[Електронний ресурс]. - Режим доступу : *http://www.businessstudio.ru/buy/modelshop/nm_bank2*.
4. Стандарти Національного банку України: СОУ Н НБУ 65.1 СУІБ 1.0:2010 "Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги" (ISO/IES 27001:2005, MOD); СОУ Н НБУ 65.1 СУІБ 2.0:2010 "Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою" (ISO/IES 27002:2005, MOD). - [Електронний ресурс]. - Режим доступу : *http://bank.gov.ua/B_zakon/Acts/2010/28102010_474.pdf*
5. Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности / В.А. Курбатов, В.Ю. Скиба // - СПб.: Питер, 2008. – 320 с.

Надійшла до редколегії 02.05.2013 р.

Рецензент: Бондарєв А.П., доктор технічних наук, професор кафедри ТРР Національного університету «Львівська політехніка», м. Львів

С.Т. Иванишин

МЕНЕДЖМЕНТ БЕЗОПАСНОСТИ ИТ КОМПЛЕКСНОЙ АВТОМАТИЗАЦИИ ТЕРРИТОРИАЛЬНО РАЗНЕСЕННЫХ ОТДЕЛЕНИЯХ БАНКА

Рассмотрены вопросы информационной безопасности при проведении удаленного внутреннего аудита в банке. Обоснована необходимость автоматизации безопасности при проведении внутреннего аудита удаленно через агрессивную среду - Интернет. Для удаленного проведения внутреннего аудита определены возможные каналы утечки информации, режимы защиты, уровне контроля. Построена автоматизированная модель защиты информации банка. Даны практические рекомендации по внедрению существую-щих систем защиты от утечки.

Ключевые слова: внутренний аудит в банке, защита канала, защита периметра, контент-контроль, автоматизация безопасности.

S.T. Ivanishin

MANAGEMENT OF SAFETY OF IT OF COMPLEX AUTOMATION TERRITORIALLY CARRIED OFFICES OF BANK

Questions of information security are considered when carrying out remote internal audit in bank. Need of automation of safety is proved when carrying out internal audit far off through hostile environment - the Internet. For remote carrying out internal audit possible channels of information leakage, protection modes, control level are defined. The automated model of information security of bank is constructed. Practical recommendations about introduction of existing systems of protection against leak are made.

Keywords: internal audit in bank, protection of the channel, protection of perimeter, content control, safety automation.