Klyuvak O. V.

The cryptographic strength of combinational hashing the authentication data in Internet-payment system

It is described the combinational hashing mechanism in Internet-payment system. It is tested the reliability of combinational hashing by means of the probability of hash collision.

Key words: *Internet payment-system, online transaction, banking payment card, authentication data, authentication, combinational hashing, OOC (online own code), cryptographic strength, collision.*

Клювак Оксана Володимирівна – фахівець 2-ї категорії наукового відділу Львівського інституту банківської справи Університету банківської справи Національного банку України (м. Київ).

УДК 004.056

С. Т. Іванишин

МОДЕЛЮВАННЯ АВТОМАТИЗАЦІЇ БЕЗПЕКИ ВНУТРІШНЬОГО АУДИТУ В БАНКУ

Розглянуто питання інформаційної безпеки при проведенні віддаленого внутрішнього аудиту в банку. Обґрунтовано 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. Побудовано автоматизовану модель захисту інформації банку. Надано практичні рекомендації щодо впровадження наявних систем захисту від витоку.

Ключові слова: *внутрішній аудит у банку, захист каналу, захист периметра, контент-контроль, автоматизація безпеки.*

Постановка проблеми. Сучасна система менеджменту в банку згідно з вимогами міжнародного стандарту ISO 9001 включає процес управління якістю. Упровадження системи управління якістю забезпечує банкові значний ефект шляхом економії коштів завдяки збільшенню обсягів продажу банківського продукту та комплексності обслуговування, а також зменшенню кількості клієнтських претензій, підвищенню якості обслуговування клієнтів, припливу нових клієнтів [1].

Процес управління якістю в банківських установах стосується безпосередньо проведення внутрішнього аудиту [2]. Ситуація значно ускладнюється завдяки факту дистанційної роботи внутрішнього аудитора, коли доступ до банківської інформації відбувається через агресивне середовище – Інтернет. Внутрішній аудитор повинен мати доступ практично до всієї банківської інформації, він контролює всі банківські процеси. Діяльність внутрішнього аудитора потребує окремої уваги щодо забезпечення банківської безпеки, тому що існує ймовірність викривлення інформації, її фальсифікації, переадресації, несанкціонованого знищення, 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 й обрати один із двох варіантів захисту: захист каналу або захист периметра. За віддаленої роботи внутрішнього аудитора система інформаційного захисту повинна надати йому доступ до будь-якої інформації ззовні та забезпечити захист за віддаленого доступу. При цьому може виникнути конфлікт між вимогами систем захисту периметра 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 опрацьовано і вирішено в цій 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. Проводять аудитори дистанційно. Документи представлені в електронному форматі. Включає перевірку складу і змісту нормативних документів та записів. Основні записи, що розглядаються у стандарті ISO 9001, перевіряють повністю, записи, що стосуються бізнес-процесів, стандартів процесів, посадових інструкцій – вибірково. На основі звітів про бізнес-процеси проводять оцінку відхилень показників якості.

По суті, цей підпроцес 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 і підрозділів (опитування та інтерв'ю). Проводять на території банку, він охоплює дві категорії співробітників: відповідальних за виконання вимог стандарту ISO 9001; представників керівництва і рядових співробітників. Вибірково щодо окремих співробітнків перевіряють знання основної документації, знання інструкцій, відповідність до кваліфікаційних вимог, наявність документації на місцях і доступ до всіх необхідних електронних документів.

На цьому етапі є небезпека незаконного вибіркового копіювання при доступі до електронних документів. Відповідальними за безпеку підпроцесу є також аудитор і офіцер безпеки.

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

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

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

Присутня небезпека незаконного копіювання персональних даних, а також навмисної і ненавмисної фальсифікації. Відповідальними за безпеку слід вважати аудитора і 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 з усіма інформаційними технологіями та системами банку. До основних систем відносять:

- автоматизовану банківську систему і допоміжні системи з автоматизації бізнес-процесів;
- програмний продукт бізнес-моделювання;
- CRM-систему (Customer Relationship Management) – управління взаємовідносинами і взаємодіями з клієнтами;
- систему 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 і встановлює в себе програмний комплекс для забезпечення безпеки, постає питання інтеграції рішення з безпеки з переліченими системами [4].

Для захисту від ненавмисного і 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 вважатися запорукою інформаційної безпеки в 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.

Основним завданням 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 один бік, надати в обидва боки. Як правило, на цьому рівні забезпечується контроль над змінними носіями – флеш-пам'ять, компакт-диск. Цей рівень вважається найефективнішим. 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 із дозволеною функцією копіювання не вирішує проблеми.

Якщо всі файли, які записують 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 і 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 з боку 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 належить 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 перевіряють усі дані, що виходять за межі корпоративної мережі. Усі 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 і 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 – це архів, у якого є функція сигналізації про деякі події, їх ще називають інцидентами. Інформація перед відправленням в архів проходить перевірку контенту та атрибутів відповідно до заданих правил. Правила наперед задає офіцер безпеки, виходячи з політики безпеки фірми чи установи. Якщо відбувається збіг контенту чи атрибутів на задані правила, тобто відбувається інцидент безпеки, то офіцерові безпеки надсилають повідомлення. Як правило, це повідомлення приходить на визначену адресу електронної пошти (пошти офіцера безпеки), можна організувати інтернет-пейджер, SMS. Звичайно, моніторинг є кроком уперед порівняно з архівуванням, тому що дозволяє вирахувати інсайдера, але все одно він не запобігає витоку.

Активний захист є найсильнішим засобом проти інсайдерських атак. При виявленні переміщення конфіденційної інформації відбувається призупинення. Пересилання можливо тільки в разі автоматичного підтвердження на відповідність правилам, що встановлені для цього відправника.

Робота на віддалі для внутрішнього аудитора характеризується двома протилежними тенденціями. З одного боку, аудитор має право доступу до будь-яких документів і 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 відбуватися за межами корпоративної мережі. Таким чином, надавши повний доступ до файлів, уже не можна контролювати подальші дії аудитора, тому що системи контролю обмежуються локальною мережею. Пересилання відбувається через зовнішнє середовище, де може відбутися виток інформації.

Автоматизація безпеки роботи зовнішнього аудитора. Таким чином, безпечна робота внутрішнього аудитора зводиться до вирішення трьох питань: по-перше, потрібно надати право перегляду будь-якого документа зовнішньому користувачеві з профілем аудитора; по-друге, захистити інформацію від читання за можливого перехоплення; по-третє, забезпечити захист від

витоку на комп'ютері аудитора. Ці завдання можуть бути вирішені в моделі, відображеній на *рис.*

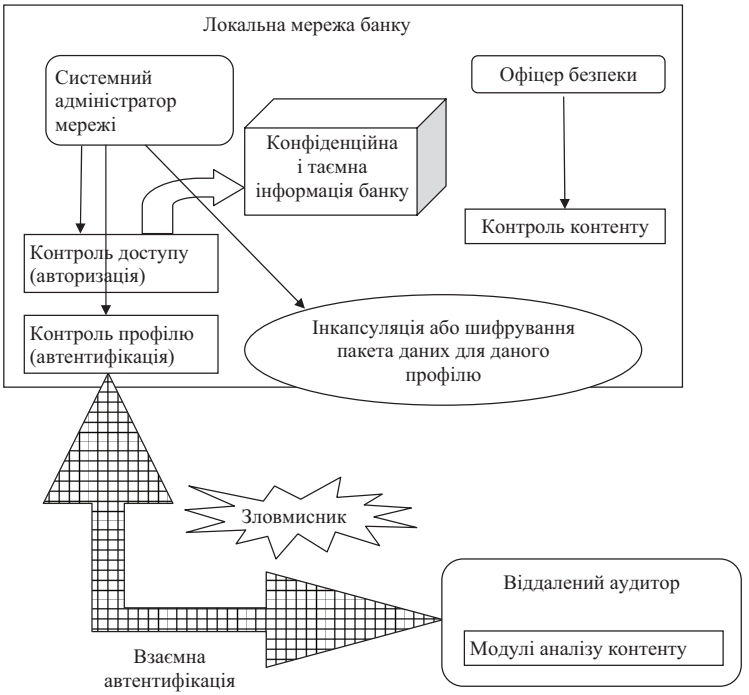

Рис. **Модель автоматизації безпеки за віддаленого доступу**

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 локальною мережею. Відмітимо, що в цій 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 цьому 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 зі статусом користувача – внутрішнього аудитора. Відповідальним за рівень є системний адміністратор. Він виконує стандартні операції біллінгу, квотування за часом або за обсягом, збирає статистику. На цьому рівні доцільно використовувати режим моніторингу.

Після того, як установлено доступ до ресурсів локальної мережі банку, внутрішній аудитор починає свою роботу. Усі 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 з аналізу контенту потрібно, 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 і центром безпеки, що є в локальній мережі, така сама, що й для даних – інформація повинна або проходити шифрування, або використовуватись *VPN*-з'єднання. Для уніфікації процесу є більш правильним використання *VPN*-з'єднання. Таким чином, з позиції 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 само, як би аудитор працював усередині корпоративної мережі. На цьому рівні потрібно застосовувати найсуворіший і найефективніший режим захисту – активний захист, який зупиняє операцію переміщення інформації по каналу.

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

Список використаних джерел

1. Cobit 4.1 (повная 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 [Электронный ресурс] / Р. А. Исаев. – Ч. 1 и 2 // Методы менеджмента качества. – 2010. – № 11–12. – Режим доступа : 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.

Иванишин С. Т.

Моделирование автоматизации безопасности внутреннего аудита в банке

Рассмотрены вопросы информационной безопасности при проведении внутреннего аудита в банке удаленно. Обоснована необходимость автоматизации безопасности при отдаленном проведении внутреннего аудита через агрессивную среду – Интернет. Для отдаленного проведения внутреннего аудита определены возможные каналы утечки информации, режимы защиты, уровни контроля. Построена автоматизированная модель защиты информации банка. Даны практические рекомендации относительно существующих систем защиты от утечек.

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

Ivanyshyn S. T.

Automation's design of security for internal audit in bank

The article deals with the question of information security during remote internal audit in the bank. The necessity of automating security for internal audit remotely via aggressive environment – the Internet. For remote internal audit identified potential information leakage, security mode, level control. Build an automated model of information security bank. Practical recommendations on the implementation of existing anti-leakage.

Key words: *internal audit of the bank, channel's protection, perimeter's protection, content-control, automation of security.*

Іванишин Сергій Теодорович – аспірант Університету банківської справи Національного банку України (м. Київ).