УДК 621.301.001.18 **Кравченко А.М., Орєхов А.А., Гаркунов А.Г.**

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ У БАНКІВСЬКИХ УСТАНОВАХ

Необхідною умовою побудови та функціонування банківської системи є всебічне забезпечення безпеки у всіх сферах банківської діяльності, важливою складовою якої є безпека економічної інформації. В статті розглядаються особливості захисту інформаційних систем у банківських установах.

Ключові слова: інформаційна безпека, система захисту, інфраструктура, конфіденціальність.

В умовах реформування української економіки значення та роль банківського сектору в забезпеченні економічної стабілізації та безпеки країни невпинно зростає.

Необхідною умовою побудови та функціонування банківської системи є всебічне забезпечення безпеки у всіх сферах банківської діяльності, важливою складовою якої є безпека економічної інформації.

Протягом минулих років банківська система пережила значні зміни, обумовленні глобалізацією фінансових ринків, розвитком інформаційних технологій, розширення асортименту банківських послуг, впровадження інноваційних технологій в управлінні банками. Це, у свою чергу, ще більше загострило ситуацію із забезпеченням надійного захисту інформації.

Питання, пов’язані з захистом економічної інформації банків, останнім часом набувають особливої актуальності, оскільки банки є найбільш вразливими до такого виду загроз, як наявність витоку інформації. Усе це викликає необхідність перегляду підходів до забезпечення безпеки інформації банку та передбачає необхідність створення відповідних систем її захисту.

Проблеми безпечного розвитку держави та її банківського сектора зокрема є предметом наукових досліджень як вітчизняних, так і зарубіжних вчених та практиків. Серед них: Арєфєєва О.В., Барановський О.І., Єрмошенко М.М., Клименко І.П., Зубок М.І., Козаченко І.П., Голубєв В.О., Никифоряк Д.Й., Костенко О.І. та інші.

Під інформаційною безпекою розуміється захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що її підтримує.

Банківська безпека – один з основних елементів менеджменту, має багатофункціональ-ний та комплексний характер.

Основними принципами забезпечення інформаційної безпеки банківських систем, є:

1. Постійний і всебічний аналіз інформаційної системи з метою виявлення уразливості інформаційних активів банку та підприємства.
2. Своєчасне виявлення проблем, потенційно здатних вплинути на інформаційну безпеку банку та підприємства, корегування моделей загроз і порушника.
3. Розробка і впровадження заходів захисту, адекватних характеру виявлених загроз, з урахуванням витрат на їх реалізацію і сумісності цих заходів з діючим банківським технологічним процесом. При цьому заходи, що приймаються для забезпечення інформаційної безпеки, не повинні ускладнювати досягнення статутних цілей банку та підприємства, а також підвищувати трудомісткість технологічних процесів обробки інформації і створювати додаткові складності для клієнтів.
4. Контроль ефективності впроваджених заходів захисту.
5. Персоніфікація та розподіл ролей і відповідальності між користувачами інформаційної системи банку чи підприємства, виходячи з принципу персональної і одноосібної відповідальності за здійснені операції.
6. Принцип «чотирьох очей», коли критичні операції та дії здійснюються або підтверджуються мінімум двома уповноваженими особами.
7. Знання банком чи підприємством своїх клієнтів і персоналу.

Найбільш небезпечні загрози внутрішній інформаційній безпеці є:

- крадіжка обладнання;
- саботаж;

- шахрайство;
- викривлення інформації;
- збої в інформаційній системі;
- втрата інформації;
- порушення конфіденційності інформації та інші.

Самою небезпечною загрозою є порушення конфіденційності інформації та витік інформації, оскільки банки побоюються цього за двома причинами. По-перше, кожен витік конфіденційної інформації та персональних даних банку підриває його репутацію, так як в очах його партнерів, інвесторів і клієнтів банк набуває імідж організації, яка не в змозі навести порядок в своїх власних стінах. В результаті відбувається відтік інвестицій та міграція клієнтів та конкурентів. По друге, інциденти такого роду можуть призвести до втрати конкурентоздатності банку, якщо, наприклад, інтелектуальна власність або база клієнтів попадуть до конкурентів.

Отже, наслідком витоку конфіденційної інформації є втрата клієнтів, погіршення іміджу, зниження конкурентоздатності та прямі фінансові збитки банків. З проблемою витоку інформації можна боротись, але перемогти її повністю неможливо, оскільки ні апаратні, ні технічні засоби не можуть забезпечити необхідного захисту, бо техніка безсила проти витонченого розуму людини.

Одна з систем, що забезпечує захист інформації - це DLP (Data Loss Prevention) – система та інші засоби, що захищають від витоків, перекривають або контролюють ті чи інші канали, по яким інформація може покинути інформаційну систему, такі як мережеві з'єднання по різних протоколах, відчужувані носії інформації, мобільні комп'ютери, принтери і т.д.

Не завжди у банків вистачає коштів і умінь перекрити всі можливі канали. Ті носії, які залишаються без належного контролю, є провідниками відповідної частки випадкових витоків.

У відношенні умисних витоків ситуація значно гірша. Внутрішні зловмисники, знаючи, які саме канали контролюються, намагаються їх обійти і послати конфіденційні дані по вільному, незахищеному - каналу. Тому на ймовірність умисних витоків слабко впливає неповне перекриття параметра інформаційної системи. Щоб ефективно протидіяти як випадковим, так і умисним витокам, DLP-система (за підтримки організаційних заходів), зрозуміло, повинна охоплювати всі без винятку канали (носії).

Згідно глобального аналізу витоку інформації по всьому світу, здійсненого компанією Infowatch, розглянемо основні канали витоку інформації за допомогою таблиці 1.

Основні канали витоку інформації за 2011-2012 роки Таблиця 1

Канали витоку	**2011**		**2012**	
	Кількість	Відсотки	Кількість	Відсотки
Мобільний комп'ютер	49	11,9	40	10,5
Носії інформації (CD/DVD, флешносії)	23	5,6	32	8,4
Настільний комп'ютер, сервер, НЖМД	41	9,9	90	23,6
Інтернет (вкл. e-mail)	97	23,5	82	21,4
Паперовий документ	84	20,3	78	20,4
Архівний носій	48	11,6	6	1,6
Інший	36	8,7	25	6,5
Не встановлено	35	8,5	29	7,6

Як видно з таблиці 1, з відмінностей в першу чергу звертає на себе увагу категорія «настільні комп'ютери, сервери і жорсткі диски ». Число витоків у цієї категорії істотно зросла.

Витоку через мобільні комп'ютери і мобільні носії були надзвичайно популярні 2-3 роки тому і раніше. У минулому році число інцидентів з ними знизилося. У цьому році спостерігається незначне зростання, що знаходиться в межах статистичної похибки. Падіння числа витоків, пов'язаних з відчужуваними носіями, без сумніву, пояснюється впровадженням засобів шифрування. Зашифрований носій при втраті або крадіжці витоком не вважається. На жаль, впровадження засобів шифрування сповільнилося. Воно так і не

стало обов'язковим для службових ноутбуків, флеш-накопичувачів і компакт-дисків. На наш погляд, шифрування впровадили лише «Свідомі» працівники і очолювані ними підрозділи. Інші ж нехтують цією мірою захисту, оскільки не можуть наочно уявити собі наслідків витоку, та й самий витік теж. Воно повністю рятує від неприємних наслідків при втраті ноутбука або мобільного носія. Всі знають, що ці наслідки неприємні (особливо в США і Великобританії). Але ймовірність інциденту мала, і пересічний громадянин не вірить, що це трапиться саме з ним. Тому впровадити шифрування носіїв можна лише шляхом примусу, встановивши покарання за відсутність шифрування всіх мобільних носіїв. Поки що така практика введена лише на невеликій кількості банків. У тому числі, і держоргани нехтують шифруванням, хоча на ноутбуках таких організацій часто зберігається державна і військова таємниця.

За оцінками аналітиків InfoWatch, впровадження шифрування мобільних носіїв буде продовжуватися, але дуже повільно. Все, що можна було запровадити «добровільно», вже зроблено. Подальше поширення шифрування можливо лише за рахунок адміністративного ресурсу – спочатку на корпоративному та галузевому рівнях, потім, можливо, на державному. Однак число використовуваних мобільних носіїв (ноутбуків і флеш-накопичувачів) постійно зростає. За рахунок цього частка «мобільних» витоків може знову вирости.

Щодо паперового документу, то проконтролювати його складніше, ніж електронний. Після виходу листа з принтера стежити за ним можна лише «вручну», за допомогою людей і організаційних процедур. Програмно-технічні методи захисту, які дешевше і звичніше, перестають працювати. В умовах відносної дешевизни технічних рішень і відносній дорожнечі робочої сили не дивно, що на Заході контроль за паперовими носіями слабкіше контролю за комп'ютерною інформацією. До того ж, багато недосконалі засоби захисту від витоків (назвати їх повноцінними DLP- системами ми не можемо) не контролюють такий канал, як відправка на друк. У цьому випадку конфіденційна інформація легко виходить з-під контролю. Типовий «паперовий» витік - це збій при автоматичній роздруківці листів, адресованих великому числу клієнтів. Як відомо, адреса на листі або на конверті друкується теж автоматично, часто і конверти заклеює автомат. Невелике зміщення - і адресати в листі і на конверті (в адресі) перестають збігатися, листи з чужими персональними даними йдуть стороннім людям. Щоб знизити число «паперових» витоків, необхідні два заходи. По-перше, потрібна DLP-система, яка блокує відправку на друк недозволеної інформації та перевіряє відповідність поштової адреси і адресата. По-друге, необхідний комплекс організаційних заходів щодо обліку руху паперових документів з конфіденційною інформацією. Заходи ці досить дорогі (особливо натлі низької вартості принтерів), тому число інцидентів з паперовими носіями буде знижуватися дуже повільно - в основному за рахунок відмови від використання паперу взагалі.

Отже, основні проблеми захисту банків від загроз зумовлені їх недостатньою увагою до власної безпеки економічної інформації. Реалізація зазначених заходів дозволить мінімізувати ризики витоку конфіденційних даних. Не втратити довіру клієнтів і не перетворитися на черговий об’єкт статистики інцидентів у сфері інформаційної безпеки.

ЛІТЕРАТУРА

1. Закон України «Про банки і банківську діяльність» від 17.01.2001 // Відомості Верховної Ради України. - 2001. - № 4.
2. Закон України «Про інформацію» // Ст. 30 «Інформація з обмеженим доступом».
3. Зубок М. І. Безпека банківської діяльності: навч. посіб. / М. І. Зубок. - К.: КНЕУ, 2009. - 190 с.
4. Аналітичні дані інформаційної безпеки - www.infowatch.ru

Надійшла: 28.02.2013 р.

Рецензент: д.т.н., проф. Єрохін В.Ф.