ІНФОРМАЦІЙНЕ ТА МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНИХ ПРОЦЕСІВ

INFORMATION AND MATHEMATICAL SUPPORT OF ECONOMIC PROCESSES

УДК 658.012.2

СУЧАСНІ ПРОБЛЕМИ ТА НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ БАНКІВ В УКРАЇНІ

З.М. Соколовська, д.е.н., професор;

П.Є. Марік

Одеський національний політехнічний університет, Одеса, Україна

Соколовська З.М., Марік П.Є. Сучасні проблеми та напрямки забезпечення фінансової безпеки банків в Україні.

Стаття присвячена розгляду проблем, існуючих у інформаційних банківських системах, та аналізу стратегій створення сучасних систем фінансової безпеки банків України. Стратегії забезпечення фінансової безпеки вітчизняних банків розглянуті на прикладі роботи Автоматизованої Банківської Системи «БАРС Millennium», яка використовується в системі Національного банку України, а також впроваджена в ряді фінансових установ.

Ключові слова: банк, автоматизована система, фінансова безпека, захист інформації

Соколовская З.Н., Марик П.Е. Современные проблемы и направления обеспечения финансовой безопасности банков в Украине.

Статья посвящена рассмотрению проблем, существующих в информационных банковских системах, и анализу стратегий создания современных систем финансовой безопасности банков Украины. Стратегии обеспечения финансовой безопасности отечественных банков рассмотрены на примере работы Автоматизированной Банковской Системы «БАРС Millennium», используемой в системе Национального банка Украины, а также внедренной в ряде финансовых организаций.

Ключевые слова: банк, автоматизированная система, финансовая безопасность, защита информации

Sokolovskaya Z.N., Marik P.E. Contemporary problems and the direction of providing financial safety of banks in the Ukraine.

Article is dedicated to the examination of the problems, which exist in the information banking systems and to the analysis of strategies of the creation contemporary the financial safety systems of the Ukraine banks. Strategies of providing financial safety of domestic banks are examined based on the example of the work of the automated banking system "BARS", of the utilized in the system of the national bank Ukraine, and also inculcated in the number financial organizations.

Keywords: bank, the automated system, financial safety, the protection of information

В результаті широкого розповсюдження на базі комп'ютерних мереж електронних платежів (з появою пластикових карт), об'єктами інформаційних атак стали безпосередньо грошові кошти як банків, так і їх клієнтів. Здійснити спробу крадіжки може будь-хто – необхідна лише наявність комп'ютеру, підключеного до Internet. Ця проблема сьогодні є актуальною й найменш дослідженою.

Аналіз останніх досліджень та публікацій

Щодо забезпечення фізичної та класичної інформаційної безпеки, то в тій сфері вже існують достатньо пророблені підходи, висвітлені у ряді літературних джерел [1–6] та ін. Але хоча і спостерігається їх розвиток, він ні йде ні в яке порівняння з частими радикальними змінами методів забезпечення безпеки автоматизованих систем обробки інформації банку (АСОІБ), що обумовлено постійним суттєвим оновленням комп'ютерних технологій.

Практика засвідчує, що не існує складних комп'ютерних систем, які б не помилялися. Згідно з цим, враховуючи регулярні зміни ідеології побудови складних АСОІБ, виправлення знайдених помилок та «вузьких місць» у системах безпеки вистачає ненадовго. Нова комп'ютерна система створює нові проблеми та робить нові помилки, що призводить до відповідної перебудови системи безпеки.

Стратегія системи безпеки типового підприємства базується на захисті його приватної інформації від конкурентів, а також від злочинців та, в деяких випадках – від податкових органів. Це сприяє зниженню вірогідності рекету та неконтрольованого зростання податкових виплат. Такі системи носять вузько спрямований характер.

Стратегія інформаційної безпеки банків значно відрізняється від аналогічних стратегій інших компаній та організацій. Це обумовлено специфічним характером загроз, а також публічним характером діяльності банків, які вимушені надавати легкий доступ до рахунків з метою забезпечення зручностей для клієнтів. Це потребує створення більш гнучких підходів до побудови систем безпеки банківської інформації.

Метою статті є огляд проблем, існуючих у інформаційних банківських системах, та аналіз стратегій створення сучасних систем фінансової безпеки банків України.

Виклад основного матеріалу дослідження

Багаторічний досвід функціонування банківської системи доводить, що інформаційна безпека банку повинна враховувати дію наступних специфічних факторів [1–8]:

— Інформація, яка зберігається та обробляється у банківських системах, представляє собою реальні гроші. Незаконна маніпуляція з такою інформацією може призвести до серйозних збитків. Ця особливість різко розширює коло саме «банківських» злочинців.
— Банківська інформація, як правило, конфіденціальна, що потребує забезпечення високого ступеня секретності.
— Конкурентоспроможність банку залежить від зручності користування клієнтами його послугами, зокрема, пов'язаними з віддаленим доступом. Але забезпечення легкості доступу клієнта до власних рахунків пов'язана з підвищенням ймовірності злочинного проникнення у банківські системи.
— Інформаційна безпека банку (на відміну від більшості компаній) повинна забезпечувати високу надійність роботи комп'ютерних систем навіть у позаштатних ситуаціях, коли банк несе відповідальність не тільки за власні кошти, але і за кошти клієнтів.
— Банк зберігає важливу інформацію про своїх клієнтів, що значно розширює коло потенційних злочинців, які зацікавлені у крадіжці або знешкодженні інформації.

У зв'язку з високим розвитком технологій, навіть максимально жорсткі організаційні заходи щодо впорядкування роботи з конфіденційною інформацією не захищають від її витоку по фізичним каналам.

Тому системний підхід до захисту інформації потребує, щоб засоби та дії, використані банком для забезпечення інформаційної безпеки (організаційні, фізичні та програмно-технічні), були розглянуті як єдиний комплекс взаємопов'язаних, взаємодоповнюючих та взаємодіючих заходів. Такий комплекс може бути націлений не тільки на захист інформації від несанкціонованого доступу, але і на попередження випадкового знищення, зміни або розголошення інформації. В якості головних підходів у забезпеченні безпеки програмно-технічного середовища можна виділити наступні [2; 8; 9]:

1) Ідентифікація (аутентифікація) і авторизація за допомогою паролів. Сутність підходу міститься у наступному. На кожному з вузлів створюється база даних користувачів, їх паролів та профілів доступу до локальних ресурсів обчислювальної системи. Задачу аутентифікації виконує незалежний (third-party) сервер, який містить паролі як для користувачів, так і для кінцевих серверів (у випадку групи серверів, базу даних паролів також містить тільки один (master) сервер аутентифікації; інші сервери – тільки періодично оновлені копії). Таким чином, використання мережевих послуг потребує двох паролів (хоча користувач повинен знати тільки один: інший надається йому «прозорим» образом).

«Вузьке місце» тієї системи – сервер. Безпеку всієї системи може порушити його «злом».

2) Інкапсуляція інформації, що передається, у спеціальних протоколах обміну. Використання подібних методів у комунікаціях засновано на алгоритмах шифрування з відкритим ключем. На етапі ініціалізації створюється пара ключів – відкритий та закритий. Останній зберігається у того, хто публікує відкритий ключ. Сутність алгоритмів шифрування з відкритим ключем у тому, що операції шифрування та дешифрування проводяться різними ключами (відкритим та закритим відповідно).

3) Обмеження інформаційних потоків. Це відомі технічні прийоми, які дозволяють розділяти локальну мережу на пов'язані підмережі та здійснювати контроль й обмеження передачі інформації між під мережами:

— 3.1. Firewalls (брандмауери). Метод передбачає створення між локальною мережею банку та іншими мережами спеціальних проміжних серверів, які здійснюють інспекцію, аналіз та фільтрацію усього потоку даних, що проходить через них (трафік мережевого/транспортного рівнів). Це дозволяє різко знизити загрозу несанкціонованого доступу зовні у корпоративні мережі, але не знімає загрозу повністю. Більш захищений різновид методу – це спосіб «маскараду» (masquerading): увесь трафік, що виходить з локальної мережі, посилається від імені firewall-сервера, роблячи закриту локальну мережу практично невидимою.
— 3.2. Proxy-servers. Даний метод передбачає жорсткі обмеження на правила передачі інформації у мережі: увесь трафік мережевого/транспортного рівнів між локальною та глобальною мережами забороняється повністю. Маршрутизація відсутня, а звернення з локальної мережі до глобальної здійснюються через спеціальні сервери-посередники. Очевидно, що за цим методом звернення з глобальної мережі до локальної стають неможливими у принципі. Також можна стверджувати, що цей метод не дає

достатнього захисту проти атак на більш високих рівнях, наприклад, на рівні програмного додатку.

4) Створення віртуальних приватних мереж (VPN), що дозволяє ефективно забезпечувати конфіденційність інформації, її захист від прослуховування та втручання в ході передачі даних. Цей підхід дозволяє встановити конфіденціальний захищений зв'язок у відкритій мережі (якою, зазвичай, є Internet) та розширити границі корпоративних мереж до віддалених офісів, мобільних користувачів, партнерів по бізнесу та ін. Технологія шифрування унеможливлює перехват повідомлень, що передаються по віртуальній приватній мережі, або їх прочитання особами, відмінними від авторизованих користувачів, за рахунок використання передових математичних алгоритмів шифрування та додатків до них. Концентратори серії Cisco VPN 3000 багатьма практиками признаються найліпшим у своїй категорії рішенням віддаленого доступу по віртуальним приватним мережам. Наведені концентратори з притаманними їм високою надійністю, унікальною цілеспрямованою архітектурою дозволяють корпораціям створювати інфраструктури віртуальних приватних мереж з високою віддачею, потужністю та можливим подальшим нарощуванням. Такі інфраструктури використовуються для підтримки відповідальних додатків віддаленого доступу. Мережеві об'єкти поєднуються за допомогою маршрутизаторів Cisco різних модифікацій – 800, 1700, 2600, 3600, 7100, 7200.

5) Використання систем знаходження вторгнень та сканерів уразнення, що створює додатковий рівень мережевої безпеки. Хоча між мережні екрани пропускають та затримують трафік в залежності від джерела, точки призначення, порту та інших критеріїв, вони фактично не аналізують трафік на атаки та не ведуть пошук вразливих місць в системі. Крім цього, між мережні екрани зазвичай не ведуть боротьбу з внутрішніми загрозами, які надходять від «своїх». Система знаходження вторгнень Cisco Intrusion Detection System (IDS) може захистити мережу по периметру, мережі взаємодії з бізнес-партнерами та вразливі внутрішні мережі в режимі реального часу. Система використовує агентів, в якості яких виступають мережеві прилади з високою віддачею, для аналізу окремих пакетів з метою знаходження джерел підозрілої активності. Якщо у потоці даних у мережі проявляється несанкціонована активність або мережева атака, агенти можуть знайти порушення у реальному часі, надіслати сигнали тривоги адміністратору та заблокувати доступ порушника до мережі. Окрім мережевих засобів знаходження вторгнень компанія Cisco також пропонує серверні системи знаходження вторгнень, які забезпечують ефективний захист конкретних серверів у мережі користувача, у першу чергу, серверів WEB і електронної комерції. Cisco Secure Scanner є програмним сканером промислового рівня, який дозволяє адміністратору виявляти та знищувати вразливості у мережевій безпеці перш, ніж їх знайдуть хакери.

У зв'язку з ростом та ускладненням мереж важливе значення набирає вимога наявності централізованих засобів управління політикою безпеки, які могли б управляти елементами безпеки.

Підвищення ефективності рішень в галузі мережевої безпеки знаходиться у сфері залучення інтелектуальних засобів, які визначатимуть стан безпеки, можуть управляти нею та виконувати загальний аудит системи. Наприклад, саме рішення Cisco реалізують стратегічний підхід до управління безпекою [9].

Cisco Secure Policy Manager (CSPM) підтримує елементи безпеки Cisco у корпоративних мережах, забезпечує комплексну та послідовну реалізацію політики безпеки. CSPM дає змогу клієнтам визначати відповідну політику безпеки, впроваджувати її й перевіряти відповідні принципи безпеки у роботі сотень між мережевих екранів Cisco Secure PIX, Cisco IOS Firewall Feature Set та агентів IDS. CSPM також підтримує стандарт IPsec для побудови віртуальних приватних мереж VPN. CSPM є складовою частиною розповсюдженої корпоративної системи управління CiscoWorks2000/VMS.

Резюмуючи наведені засоби, треба підкреслити, що розробка інформаційних систем потребує паралельної розробки технологій передачі та захисту інформації. Ці технології повинні забезпечити захист інформації, що передається, тобто забезпечити надійність мережі (мається на увазі логічний, інформаційний рівень).

Можна навести також ряд додаткових заходів, які реалізують наступні принципи: моніторинг процесів, дублювання технологій передачі та децентралізація.

Треба окремо підкреслити, що використання стандартизованих технологій обміну інформацією спостерігається у багатьох випадках як наслідок недостатньої потужності систем, які забезпечують процедури зв'язку. Одним з децентралізованих підходів є розповсюджена у системі Internet практика «дзеркал». Створення кількох ідентичних копій ресурсів може бути корисним у системах реального часу, у яких навіть короткочасні збої можуть мати серйозні наслідки.

Таким чином, захист банківської інформації – це комплексна задача, яка не може бути повністю вирішена тільки у рамках банківських програм. Ефективна реалізація захисту починається з вибору та конфігурування операційних систем та мережевих системних засобів, що підтримують функціонування банківських програм.

Серед дисциплінарних засобів забезпечення захисту, зазвичай, виділяють два напрямки:

— Достатня усвідомленість користувачів системи щодо особливостей її побудови.
— Наявність багаторівневих засобів ідентифікації користувачів та контролю їх прав.

На різних етапах свого розвитку автоматизовані банківські системи мали різні складові захисту. У вітчизняних умовах більшість банківських систем по рівню захисту можна віднести до систем першого та другого рівня складності, які характеризуються наступним:

— перший рівень – використанням програмних засобів, що надаються стандартними засобами операційних систем та мережевих програм;
— другий рівень – використання програмних засобів забезпечення, кодування інформації, кодування доступу, безпеки

Стратегії забезпечення фінансової безпеки вітчизняних банків розглянемо на прикладі роботи Автоматизованої Банківської Системи «БАРС Millennium» (далі АБС "BARS"), криптографічного шлюзу "BARS Gateway" та супутнього програмного забезпечення (ПЗ): «Обробки статистичної звітності» та ін.

Наведені програмні модулі обробки та захисту банківської інформації використовуються в системі Національного банку України, а також впроваджені в багатьох фінансових установах.

АБС "BARS" побудована на модульній основі, яка спирається на сучасну СУБД корпорації Oracle та інші продукти цієї корпорації [9]. АБС дозволяє реалізувати різнопрофільні рішення для різних фінансових сфер, зберігати й обробляти великі обсяги даних, проводити аналіз даних будь-якої складності і глибини. У алгоритми реалізації фінансових технологій закладаються сучасні принципи обробки, оригінальні рішення і перевірені досвідом підходи. Загальна архітектура системи наведена на рис. 1 [9, 10].

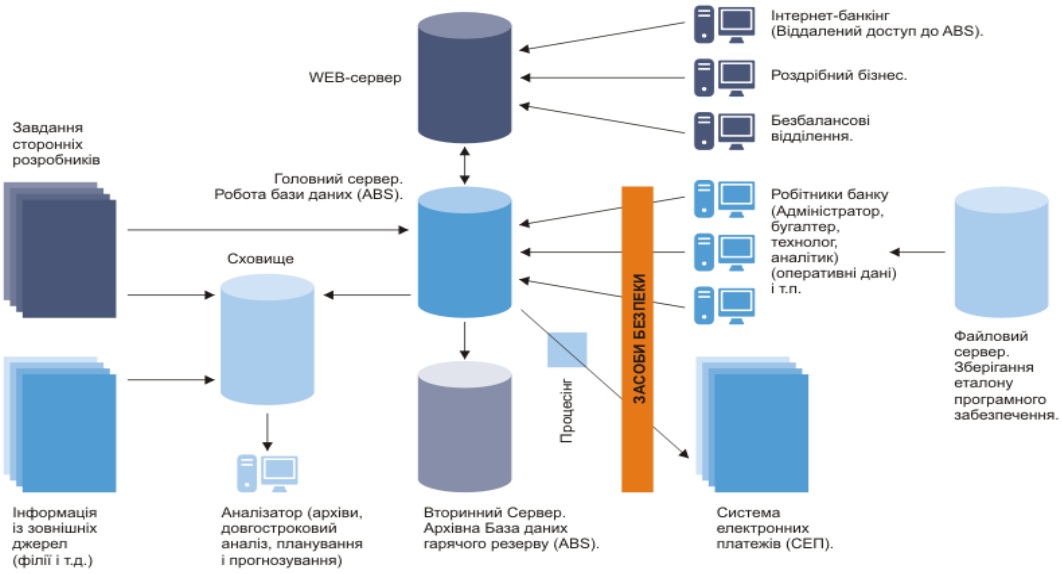

Рис. 1. Архітектура АБС «БАРС Millennium» [10]

Архітектура представленої автоматизованої банківської системи базується на двох рівнях доступу до даних (бізнес-логіка реалізується на рівні схем та процедур баз даних). Сьогодні це звичайна практика створення багаторівневих архітектур з використанням мережевих технологій та серверів додатків.

Система оснащена засобами параметричного настроювання, що надає змогу її впровадження із врахуванням особливостей конкретного банку. У АБС реалізовані система розмежування прав користувачів та захисту інформації, а також гнучкі засоби адміністрування. Фінансова безпека банку забезпечується комплексами фінансового візування й верифікації, а також роздільним доступом до фінансових ресурсів.

Відкрита API-технологія імпорту-експорту поряд з реалізацією взаємозв'язків з широким колом криптографічних засобів захисту надає можливості інтеграції у різноманітні комплексні рішення автоматизації.

Основоположними концепціями АБС є [9]:

— Орієнтація на промислові сервера баз даних Oracle.
— Використання архітектури «Клієнт-Сервер».
— Незалежність клієнтської частини від використовуваного сервера.
— Транзакційність.
— Підтримка цілісності на рівні СУБД.
— Набір внутрішніх обмежень цілісності і правил зберігання даних.
— Зберігання і обробка великих обсягів інформації.

Пристрій:

— Модульність.
— Мультивалютність.
— Багатонаціональність (переклад на різні мови).

— Можливість застосування різних офісних додатків для обробки інформації.
— Гнучка система адміністрування.
— Система захисту даних.
— Багаторівнева система візування.
— Багаторівнева система роздільного доступу до фінансових і технічних ресурсів банку.

«Засоби безпеки», наведені на рис. 1, представляє криптографічний шлюз BARS Gateway, властивості якого достатньо описані у керівництві користувача [9]. За описом системи [10], шлюз дозволяє встановлювати захищені (з криптуванням потоку даних) канали між декількома хостами, організовувати віртуальні приватні мережі (Virtual Private Network), а також має низьку ресурсоємкість і може працювати на всіх операційних системах сімейства Windows. Для захисту BARS Gateway використовує сертифіковані бібліотеки інших виробників.

Технічні характеристики системи [9]:
— Базовий протокол TCP/IP.
— Можливість застосування в будь-яких системах, що використовують, як транспорт, протокол TCP/IP або проколи, реалізовані поверх TCP/IP (HTTP, FTP та ін.).
— Гнучка багатониткова (multithreaded) архітектура. Як наслідок – низька ресурсоємкість.
— Підтримка різних криптографічних бібліотек.
— Централізоване управління клієнтськими з'єднаннями. Розширений моніторинг з'єднань. Статистика за трафіком для кожного клієнта.
— Розширена система протоколювання:
— 8-рівневий протокол.
— 4 протокольних вікна (повний протокол, повідомлення про помилки, попередження, інформаційні повідомлення).
— Захист протоколу від модифікації.
— Функції Firewall (брандмауера). Можливість фільтрувати клієнтські з'єднання за IP-адресами.
— Система звукового оповіщення адміністратора в разі помилок (спроба несанкціонованого доступу, розрив з'єднання і пр.).
— Додаткові можливості для управління таблицею відкритих ключів.

Окремо слід зазначити типове ПЗ «Обробки статистичної звітності», яке може мати різні найменування, але функціонал якого зводиться до одного – акумуляція статистичної звітності на містах з подальшим передавання до органів контролю (відповідні підрозділи Національного банку України).

У той чи інший спосіб усі програмні комплекси фінансової сфери банківської діяльності пов'язані з ПЗ «Оброки статистичної звітності», яка, у порівняні з зазначеними сучасними банківськими комплексами, являє собою застарілий алгоритм приймання-передавання, вводу – виводу та збереження у базі статистичної інформації для подальшої обробки. Враховуючи, що система працює у середині організації і не має зовнішніх виходів на інших учасників фінансових процесів з зовні банківської системи, програмне забезпечення не має ніяких механізмів сучасного програмного захисту.

Тривала експлуатація розглянутої системи дозволяє акцентувати увагу на її певних недоліках, а саме.

АБС "BARS" для забезпечення своєї універсальності реалізує усі методі на стороні клієнта. Тобто кожен раз, коли потрібно виконати дії, клієнт формує у відкритому вигляді запити до сервера.

Наприклад, вибрати інформацію за критерієм можливо через форму, де у звичному для SQL-запиту виді потрібно вказати («Крітерій 1») and («Крітерій 2»), що дозволяє виконати дуже простий механізм SQL ін'єкції та отримати інформацію з обмеженим доступом. Відсутність трирівневої системи на практиці дозволяє підключатись клієнтським містам напряму до бази даних, використовуючи для доступу тільки політики безпеки СУБД ORACLE. Остання має свої недоліки і вразливості, дозволяючи підвищувати привілеї користувачам (програмні виправлення для закриття вразливостей розробляються компанією ORACLE майже постійно).

Незважаючи на розвинуту систему доступу у самій АБС "BARS" адміністративні модулі дають змогу, при відсутності певних перешкод, пов'язаних с людським фактором, надати будь-кому усі можливі привілеї для виконання фінансових операцій або отримання конфіденційної інформації. Інакше, відсутній захист від інсайдерів.

Система крипто шлюзу "BARS Gateway" дозволяє використовувати вже створене, за допомогою зовнішніх систем захисту, захищене підключення для будь-яких цілей. Тобто разове «валідне» підключення може бути одночасно використано «Вірною програмою» та «Стороннім програмним кодом» зі сторони ініціатора. У випадку з АБС "BARS", підключившись до системи клієнтською частиною, можливо одночасно підключитись до СУБД ORACLE сторонніми програмними продуктами через створене захищене підключення "BARS Gateway". Режим посередника між клієнтом та сервером на практиці часто призводить до внутрішніх помилок, пов'язаних з затримкою передачі інформації про помилку на рівні мережевих протоколів, що призводить до зупинки роботи комплексу в цілому на невизначений час, а це є критично для передачі інформації в режимі online.

Як за перевагами, так і за недоліками ПЗ «Обробки статистичної звітності» не дуже виділяється серед зазначених комплексів. Але, нажаль, має один великий недолік. При передачі інформації не ведеться перевірка вмісту «посилки» на рівні байт-коду, що дає можливість, теоретично, завантажити у мережу певну виконуючу послідовність, що несе серйозну загрозу для системи в цілому. Також рівень побудови системи, нажаль, настільки складний, що під час помилки потрібно багато часу для відновлення роботи. А це також є критично для систем,

працюючих у рамках чіткого графіку формування інформації.

Висновки

Сучасні банківські та фінансові системи, на рівні інформаційних технологій, дають змогу виконувати весь спектр фінансових послуг на підставі чинної нормативної бази, забезпечують певний рівень захищеності інформації та не являються, у цілому, складними для розуміння і супроводження, але потребують постійної уваги з боку захисту інформації.

В останній час у вітчизняних банках спостерігається велика кількість випадків порушення рівня секретності. Як приклад – поява у вільному доступі різних баз даних на компакт-дисках стосовно комерційних компаній та приватних осіб. Хоча вітчизняна законодавча база стосовно захисту банківської інформації існує, її практичне використання має великі недоліки. Ілюстрація цього факту – відсутність прецедентів покарання банку або окремих копаній за, відповідно, спробу надання та спробу отримання конфіденційної інформації.

Забезпечення фінансової безпеки у банківській сфері передбачає не тільки захист документації та іншої виробничої інформації, але і мережевих настройок та параметрів функціонування мережі на комп'ютерах.

Таким чином, задача захисту банківської інформації постає більш жорстко, ніж у інших організаціях. Її розв'язання передбачає планування організаційних та системних заходів забезпечення безпеки. Однак, в ході планування захисту необхідно підтримувати його на такому рівні, який би не зашкоджував нормальній праці персоналу банку.

Постійні появи методів «обходу» будь-якої електронної системи захисту, вимагають від фахівців проведення постійного аналізу сучасних тенденцій розвитку світової інформаційної безпеки; розробку нових та вдосконалення існуючих механізмів захисту інформації.

Список літератури:

1. Гайкович Ю. Безопасность электронных банковских систем / Ю. Гайкович, А. Першин. – М.: Единая Европа, 2008. – 363 с.
2. Антонюк А. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / А. Антонюк, В. Жора. – Ірпінь : Національний університет ДПС України, 2010. – 310 с.
3. Голубєв В. Інформаційна безпека : проблеми боротьби з кіберзлочинами : монографія / В. Голубєв. – Запоріжжя : ГУ «ЗІДМУ», 2003 – 250 с.
4. Захист інформації в комп'ютерних системах та мережах : методична розробка / [уклад. : Б. Корнієнко, Л. Щербак]. – К. : НАУ, 2006. – 64 с.
5. Кавун С. Інформаційна безпека : підручник / С. Кавун. – Харків : Вид. ХНЕУ, 2009. – 368 с.
6. Курило А. Основы информационной безопасности автоматизированных банковских систем : учеб. пособ. / [Курило А., Милославская Н., Михайлов С., Толстой А.]. – М.: МИФИ, 2001. – 100 с.
7. Палюх Б. Надежность программных средств экономических информационных систем : учеб. пособ. / Палюх Б., Кемайкин В., Дорожкин А. – Тверь : Твер. гос. техн. ун-т, 2008. – 128 с.
8. Тютюнник А. Информационные технологии в банке / А. Тютюнник, А. Шевелев. – М. : БДЦ Пресс, 2003. – 368 с.
9. Автоматизированная банковская система «БАРС-Millennium» *[Электронный ресурс]*. – Режим доступа: – http://sdb.su/svalka/746-avtomatizirovannaya-bankovskaya-sistema-bars-millennium-rukovodstvo-polzovatelya-chast-1.html.
10. Автоматизированная банковская система «БАРС-Millennium» *[Электронный ресурс]*. – Режим доступа: – http://unity-bars.net/ua/produkti/abs-bars-millennium.

Надано до редакції 22.06.2014

Соколовська Зоя Миколаївна / Zoya N. Sokolovskaya
nadin@sky.od.ua

Марік Петро Євгенович / Peter E. Marik
m5_@mail.ru

Посилання на статтю / Reference a Journal Article:
Сучасні проблеми та напрямки забезпечення фінансової безпеки банків в Україні [Електронний ресурс] / З.М. Соколовська, П.Є. Марік // Економіка: реалії часу. Науковий журнал. – 2014. – № 5 (15). – С. 179-184. – Режим доступу до журн.: http://economics.opu.ua/files/archive/2014/n5.html