УДК 004.056.5

Сергій ЛУКЬЯНЧІКОВ
lsd57@ukr.net
ORCID: 0000-0002-6837-2930
Сергій ЄВДОКИМОВ
serge.evdokimov2015@gmail.com
м. Миколаїв

АКТУАЛЬНІ ПРОБЛЕМИ ТА ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АВТОМАТИЗОВАНОЇ БАНКІВСЬКОЇ СИСТЕМИ

У статті розглядаються і пропонуються нові підходи до інформаційної безпеки автоматизованих банківських систем (АБС) від сучасних загроз. Створення інформаційної безпеки – це одна з найбільш актуальних проблем для кожного банку. З метою запобігання злочинам пов'язаним з комп`ютерною інформацією постає необхідність правильно обирати засоби і заходи забезпечення захищеності інформації від несанкціонованого до неї доступу.

***Ключові слова**: автоматизована банківська система, кібербезпека, безпека даних, заходи безпеки інформації, цілісність інформації, криптографічний захист інформації, синергетичний підхід.*

Постановка проблеми

В даний час з більш ніж 90% усіх злочинів пов'язані з використанням автоматизованих систем обробки інформації банку. Щоденна діяльність автоматизованих банківських систем тісно пов'язана з використанням сучасних комп'ютерних технологій і перебуває в повній залежності від надійної та безперебійної роботи електронно-обчислювальних систем. Проблему кібербезпеки на сьогоднішній день вже непробачно ігнорувати. І в цьому недавня атака «PETYA.A» може стати в нагоді. Це пов'язано не тільки зі зберіганням в кредитних організаціях грошових коштів, але і з тим, що в банках важлива та найчастіше секретна інформація. Таким чином, вирішення питань безпеки транзакцій в АБС залишається актуальною і на сьогоднішній день. З метою опору злочинам у сфері комп`ютерної інформації або зменшення збитків постає необхідність правильно обирати засоби забезпечення захищеності інформації від проникнення та несанкціонованого до неї доступу [1].

Аналіз останніх досліджень і публікацій

Безпека даних – одна з головних завдач, що вирішуються IT-відділами компаній. Знайти універсальне рішення в даному питанні практично неможливо: неоднорідність сфер діяльності і структур організацій переводить завдання в категорію індивідуального підходу.

Постановка завдання

У сучасному взаємозв'язаному світі розвинені та високотехнологічні соціуми сильно залежать від роботи ряду служб, які в даний час стали життєво необхідними. У той же час, завдяки кіберзлочинності, банки втрачають мільярди доларів щорічно. Промислові мережі ставлять унікальні завдання перед фахівцями в області безпеки, оскільки вони мало схожі на традиційні IT-мережі. Однією з цілей функціонування АБС є обробка персональних даних співробітників та клієнтів банку, відповідно до вимог Закону України «Про захист персональних даних» [2]. На практиці побудувати складну систему, що задовольняє цьому принципові, неможливо, і не лише з огляду на ймовірність виникнення несправностей і помилок, але й через складність визначення і формулювання суперечливих очікувань проектувальника системи. Зараз банки активно співпрацюють з правоохоронними органами щодо попере-

© Сергій ЛУКЬЯНЧІКОВ, Сергій ЄВДОКИМОВ, 2018

дження злочинності, пов'язаної з втручанням в комп'ютерні системи, однак законодавство і практика свідчать про значні прогалини в цій сфері.

Виклад основного матеріалу

Під безпекою автоматизованих систем обробки інформації банку необхідно розуміти таку їх властивість, що полягає у спроможності протидіяти спробам завдання збитків власникам і користувачам системи, тобто захищеності від спроб розкрадання чи руйнування її компонентів [5]. Таким чином, головними завданнями будь-якої системи інформаційної безпеки є:

– забезпечення доступності даних для авторизованих користувачів – можливості оперативного отримання інформаційних послуг;

– гарантія цілісності інформації – її актуальності і захищеності від несанкціонованих змін або знищення;

– забезпечення конфіденційності відомостей.

Незважаючи на безліч можливостей витоку інформації, безпеку банківських даних та їх конфіденційність забезпечити цілком можливо. Існує досить велика кількість способів захисту комп'ютерів. Є методи, які ґрунтуються на застосуванні безпечних операційних систем та апаратного забезпечення, що здатне захистити комп'ютерну систему. Хоча під час проектування комп'ютерної системи необхідно взяти до уваги чимало характеристик. Безпека є серед них однією з найважливіших. Небезпечні програми деколи не правильно уподібнюються з комп'ютерними вірусами, тоді коли вірус – лише один із злочинних видів шкідливих програм.

В банківських автоматизованих системах вибір засобів захисту інформації – досить складна задача, а при її рішенні особливо необхідно врахувати можливість різних протиправних дій щодо порушення працездатності такої системи, вартість реалізації засобів захисту і наявність різних зацікавлених сторін [3]. Варто зазначити, що важливість забезпечення інформаційної безпеки оцінена і на державному рівні, що відбивається у вимогах нормативно-правових актів. Наприкінці 2017 року, Національний банк України встановив вимоги до кіберзахисту, які повинні впроваджуватися банками. Вимоги спрямовані на посилення захисту інформації у банківській системі з урахуванням актуальних кіберзагроз [3]. Заходи безпеки інформації включають:

1. Контроль доступу до ресурсів АБС (управління доступом)
2. Ідентифікація і аутентифікація АБС (користувачів процесів і т.д.)
3. Реєстрація та аналіз подій, що відбуваються в АБС.
4. Контроль цілісності об’єктів АБС.
5. Шифрування даних.
6. Резервування ресурсів і компонентів АБС.

Кожен напрямок включає кілька етапів роботи. Наприклад, контроль за доступом, тобто обмеження можливостей використання ресурсів системи програмами, процесами і користувачами згідно з політикою безпеки забезпечує захист не тільки від зовнішніх і внутрішніх зловмисників, але в тому числі дозволяє захиститися від помилок персоналу, що призводять до втрат еквівалентним реалізації атаки зловмисником. Управління доступу – захист інформації шляхом регулювання доступу до всіх ресурсів системи. Регламентуються порядок роботи користувачів і персоналу, право доступу до окремих файлів в базах даних і т.д.

Доступ до даних банку захищається за допомогою системи ідентифікації, тобто паролями або електронними ключами. Ідентифікація – це присвоєння коду кожному об'єкту персонального ідентифікатора. Аутентифікація – встановлення автентичності. Нові можливості дозволяють використовувати багатофакторну посилену ідентифікацію при авторизації в банківській системі. Така аутентифікація особливо актуальна в роботі співробітників, що мають права введення і підтвердження фінансових документів.

© Сергій ЛУКЬЯНЧІКОВ, Сергій ЄВДОКИМОВ, 2018

Для аналізу ефективності вжитих заходів необхідно вести облік або запис, які будуть відзначати працездатність й дієвість застосованих засобів захисту інформації в банку. Ці функції забезпечують отримання й аналіз інформації про стан ресурсів системи, реєстрацію дій, які можуть бути визначені як небезпечні ситуації, ведення журналу, який допоможе оперативно зафіксувати події, що відбуваються в системі. Аналіз журналу, якщо його вести належним чином, може допомогти у визначенні засобів, які використовував зловмисник під час порушення системи захисту, у визначенні реального стану системи, у виборі способів розслідування в разі порушення і підказати шляхи виправлення ситуації.

Контроль за цілісністю, тобто захист від несанкціонованої модифікації суб'єктів системи. Це фактично – контроль за цілісністю атрибутів суб'єкта, контроль за послідовністю і повнотою процесів та режимів їх виконання. Механізм контролю цілісності здійснює стеження за незмінністю контрольованих об'єктів, захист від шкідливого коду. При несанкціонованому знищенні, додаванні зайвих елементів та модифікації даних, зміну порядку розташування даних, формуванні фальсифікованих платіжних документів у відповідь на законні запити, активної ретрансляції повідомлень з їх затримкою. Цілісність порушується при, викраденні або незаконної зміні алгоритмів роботи. Забезпечення цілісності – частина комплексу заходів по досягненню безпеки інформації. Загрози, що відносяться до можливостей несанкціонованої модифікації інформації, є загрозами цілісності. Загрози, що відносяться до можливостей несанкціонованого ознайомлення з інформацією є загрозами конфіденційності. В загальному випадку вважається, що для захисту інформації повинні бути створені механізми захисту. Це управління доступом до ресурсів, включаючи доступ до паролей, надання рівнів доступу до об’єктів, ідентифікація, реєстрація та облік роботи користувачів. Порушення цілісності може статись в наслідок наступних причин:

1. Помилки користувачів, які викликають викривлення чи втрату інформації.
2. Навмисні дії осіб, які не мають прав доступу до системи.
3. Збої обладнання, які викликають викривлення чи втрату інформації.
4. Фізичний вплив на носії інформації.
5. Вірусні впливи.

Одним з дієвих методів реалізації вимог цілісності інформації є криптографічний захист інформації (шифрування, хешування, електронний цифровий підпис). При комплексному підході до захисту АБС, напрям забезпечення цілісності та доступності інформації переростає в план заходів, що спрямовані на забезпечення безперервності роботи АБС. Система шифрування даних забезпечує безпеку при обміні інформацією, тому всі дані, передані в банк або прийняті від банку, шифруються спеціальним методом згідно стандартів ISO 8730 та ISO 8731. Засоби шифрування доволі надійно захищають комп'ютерну інформацію від кіберзагроз. Кодування тексту за допомогою складних математичних алгоритмів, отримує все більшу популярність. Звичайно, що не один з алгоритмів шифрування не дає стовідсоткової гарантії захисту від зловмисників, але все ж, деякі методи шифрування досить складні, щоб дати змогу ознайомитися з повідомленнями зашифрованого змісту. Досить дієвим та потужним є застосування для захисту інформації криптозахисту, тобто систем, які дозволяють зашифрувати та дешифрувати інформаційні потоки.

RSA (абревіатура від англ. прізвищ Rivest, Shamir та Adleman) – це один із поширених методів шифрування на сьогодні. Алгоритм, в основі якого кожен учасник процесу має власний таємний ключ та відкритий ключ, який не має бути секретним, за допомогою нього проводиться обмін повідомленнями. Електронний цифровий підпис (ЕЦП) – це модель власно дію-

© Сергій ЛУКЬЯНЧІКОВ, Сергій ЄВДОКИМОВ, 2018

чого підпису в електронному вигляді певної посадової особи. Криптографічні методи широко застосовуються у АБС та мають реалізацію у вигляді програмних, апаратних чи програмно-апаратних методів захисту інформації. Криптографія є провідним засобом забезпечення конфіденційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, що є фундаментом реалізації багатьох з них і останньою захисною межею [6].

Строгий облік каналів та серверів, а також заходи, що забезпечують технічний захист інформації і безпеку банку мають на увазі захист резервних копій, забезпечення безперебійного живлення устаткування, що містить цінну інформацію, обмежений доступ до сейфів та захист від витоку інформації акустичним способом. Резервування ресурсів та абонентів АБС передбачає: організацію регулярних процедур порятунку і резервного зберігання критичних даних, періодичну перевірку резервних пристроїв обробки даних, підготовку фахівців, здатних замінити адміністраторів систем, реєстрацію систем та зберігання носіїв інформації в строго визначених місцях, видачу їх уповноваженим особам з необхідними відмітками в реєстраційних документах.

Безпека банкоматів та платіжних терміналів повинна забезпечуватися з використанням традиційних засобів – антивірусного захисту. В той же час специфіка таких пристроїв вимагає застосування додаткових засобів захисту. Створення «замкнутого програмно-апаратного середовища», повністю виключає установку любого стороннього програмного забезпечення і підключення зовнішніх пристроїв [3].

Система безпеки в цілому – це безперервний процес ідентифікації, аналізу та контролю. Оскільки інформація, що знаходиться в базі даних банків являє собою реальну матеріальну цінність, то вимоги до зберігання та обробки цієї інформації завжди будуть підвищеними.

Уточнення і доповнення безлічі актуальних загроз безпеки банківської інформації, безпека інформації і кібербезпека в банківському секторі, це основа для створення нового синергетичного підходу в області інформаційної безпеки АБС. Для аналізу основних видів загроз безпеки банківської інформації використовується відома модель безпеки – тріада CIA (Confidentiality, Integrity, Availability) в трьох сферах безпеки: інформаційної безпеки, безпеки інформації та кібернетичної безпеки (рис. 1).

Рис. 1. Модель тріади CIA
для комплексних АБС

У даній моделі під «інформаційною безпекою» розуміється процес забезпечення конфіденційності, цілісності і доступності інформації клієнтами банку. У моделі «конфіденційність» – забезпечення доступу до інформації тільки авторизованим користувачам, «цілісність» – забезпечення достовірності і повноти інформації, «доступність» – забезпечення доступу до інформації [7].

Модель синергетичного підходу – оцінка безпеки банківських систем. В процесі аналізу ризиків інформаційної безпеки можуть використовуватися спеціалізовані програмні комплекси, що дозволяють автоматизувати процес аналізу вихідних даних та розрахунку значень ризику. Прикладом такого комплексу є «АванГард» Ціллю інформаційної безпеки є забезпечення трьох найважливіших сервісів безпеки. Відповідно моделі безпеки інформа-

© Сергій ЛУКЬЯНЧІКОВ, Сергій ЄВДОКИМОВ, 2018

ції включають: конфіденційність, цілісність і доступність. Слід зазначити ключову особливість, характерну тільки пропонованому синергетичному підходу до безпеки банківської інформації. Основна мета запропонованого підходу - це порушення в системі забезпечення банківської інформації керованих емерджентних властивостей, спрямованих на отримання синергетичного ефекту, який досягається завдяки якісно новому підходу до безпеки. Таким чином, виходячи із потреби дотримання правила триєдиної позиції до забезпечення безпеки банківської інформації в рамках синергетичного підходу при взаємодії вибраних профілів безпеки і з метою підвищення рівня її захищеності є оцінювання величини ризику аналогічного грошового капіталу. Сенс запропонованого підходу може бути представлений в вигляді деякої умовної фігури [4]. Дані методи дозволять, визначити і класифікувати загрози і, відповідно до вірогідності наступу негативних наслідків та їх можливої тяжкості для Банку, організувати систему захисту.

Висновки і перспективи досліджень

У висновку потрібно зауважити, що високоякісний підхід до створення системи захисту інформації в АБС має на увазі конкретну оцінку імовірності появи кожної загрози. Таким чином, сучасні світові тенденції вимагають від банків бути готовими до зустрічі з ризиками інформаційної системи. Реалізація таких ризиків може завдати значних збитків банкові, так як практично вся діяльність банківської установи залежить від інформаційних систем. Тому, потрібно знайти принципово нові підходи для розробки та впровадження відносно надійних систем захисту банківської діяльності від комп'ютерних злочинів. Існує багато шляхів захисту комп'ютерів. Серед них методи, що ґрунтуються на використанні безпечних операційних систем та апаратного забезпечення, здатного захистити комп'ютерну систему. Вирішення полягає в захисті від сучасних небезпек і спрямованих атак, який також повинен дозволити виявити незвичайну або підозрілу поведінку. Такі засоби повинні забезпечувати ідентифікацію та аутентифікацію користувачів, розподіл повноважень доступу до системи, реєстрацію та облік спроб несанкціонованого доступу. Перспективним напрямком подальших досліджень є обробка сутності та змісту профілів безпеки, що входять до складу системи захисту банківської інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cybersecurity: Understanding the Online Threat, published on 2013/12/17, Sam Musa | Cyber Security Adjunct Professor, University of Maryland University College [Електронний ресурс].
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VII [Текст].
3. Голубєв, В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів [Текст] / В.О. Голубєв. – З.: Павел, 1998. – 144 с.
4. Куранов, А.И. Безопасность банковской информации [Текст] / А.И. Куранов //Системы безопасности. – 1995, № 4.
5. Стрельбицька, Л.М. Банківське безпекознавство: навч. посібник [Текст] / Л.М. Стрельбицька, М.П. Стрельбицький, В.К. Гіжевський. – К.: Кондор, 2007. – 602 с.
6. Олійник, А.В. Інформаційні системи і технології у фінансових установах: навч. посібник [Текст] / А.В. Олійник, В.М. Шацька. – Львів: "Новий Світ-2000", 2006 – 436 с.
7. Евсеїв, С.П. Синергетический подход к оценке безопасности банковских систем [Текст] / С.П. Евсеїв // Збірник наукових праць «Системи обробки інформації»: Т. 2 – Харьков, ХНЭУ им. С. Кузнеца, 2016. Вип. 4 (141). – 104 с.

© Сергій ЛУКЬЯНЧІКОВ, Сергій ЄВДОКИМОВ, 2018

Serhiy LUKIANCHIKOV, Serhiy EVDOKIMOV
Mykolayiv

ACTUAL PROBLEMS AND APPROACHES TO PROVIDE CIBBERBEEPING OF AUTOMATIC BANKING SYSTEM

The article deals with and proposes new approaches to information security of automated banking systems (ABS) from modern threats. Creating information security is one of the most pressing issues for each bank. In order to prevent computer-related crimes, it becomes necessary to choose the right means and measures to ensure the security of information from unauthorized access to it.

Keywords*: automated banking system, cybersecurity, data security, information security measures, integrity of information, cryptographic information protection, synergistic approach.*

Сергей ЛУКЬЯНЧИКОВ, Сергей ЕВДОКИМОВ
Николаев

АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПОДХОДЫ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ БАНКОВСКОЙ СИСТЕМЫ

В статье рассматриваются и предлагаются новые подходы к информационной безопасности автоматизированных банковских систем от современных угроз. Создание информационной безопасности - это одна из наиболее актуальных проблем для каждого банка. С целью предотвращения преступлений связанных с компьютерной информацией возникает необходимость правильно выбирать средства и меры обеспечения защищенности информации от несанкционированного к ней доступа.

Ключевые слова*: автоматизированная банковская система, кибербезопасность, безопасность данных, меры безопасности информации, целостность информации, криптографическая защита информации, синергетический подход.*

Стаття надійшла до редколегії 30.03.2018

© Сергій ЛУКЬЯНЧІКОВ, Сергій ЄВДОКИМОВ, 2018