**УДК 004.41-42**

**О.А. Курченко, А. В. Головатенко, Л.Ю. Карасевич**

# ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ БАНКУ

Розглядається проблема підвищення ефективності системи управління захистом персональних даних клієнтів банку. Проаналізовано і досліджено останні публікації, як в Україні, так і за її межами. Висвітлена невирішена раніше частина загальної проблеми. Також, в даній статті розкриваються існуючі системи управління захистом персональних даних та можливі шляхи покращення діяльності системи управління захистом персональних даних клієнтів банку для захисту від несанкціонованого доступу та інших зловмисних дій зовнішнього і внутрішнього характеру. Особливо наголошується на необхідності використання відповідних нормативних актів, які дозволяють визначати основні дії відносно захисту персональних даних, та сучасних системних продуктів захисту. Тому основна увага робиться на використанні комплексного захисту персональних даних клієнтів банку. Наприкінці статті зроблений висновок, в якому описаний необхідний перелік заходів, які необхідно застосувати для підвищення ефективності системи управління захистом.

**Ключові слова:** банк, клієнт банку, персональні дані, система захисту, інформаційна безпека банку.

**Постановка проблеми.** В сучасному інформаційному суспільстві захист персональних даних клієнтів банку – це вкрай важлива необхідність для успішного функціонування банку в конкурентному середовищі і роботи з клієнтами. Тому для успішного вирішення цього завдання банкам потрібно завжди бути в курсі останніх новинок захисту (як технічних, так і законодавчих) своїх даних і персональних даних своїх клієнтів, оскільки останнім часом атаки на банки для заволодіння базами даних стають все більш небезпечними.

В наш час в банках і банківській сфері чільне місце в захисті приділяється підтриманню на належному рівні, оптимізації та безперервному покращенні системи управління захистом персональних даних клієнтів банку. Банківська інформація, в тому числі персональні дані клієнтів банку, є основним об’єктом оперування, тому вона вимагає належного захисту на законодавчому, технологічному та управлінському рівнях.

На сьогоднішній день саме питання захисту персональних даних в банківській сфері, особливо після прийняття Закону України «Про захист персональних данних», стало досить актуальним. Мета прийняття закону «Про захист персональних данних» №2297-17 від 02.06.2010 [1] – створення правової бази державного регулювання суспільних відносин, встановлення прав, гарантій, обов’язків і відповідальності всіх суб’єктів діяльності, пов’язаної із захистом персональних даних. Одним із головних факторів розробки прийняття даного закону є розвиток взаємин та подальша плідна співпраця з Євросоюзом. Тому виникла нагальна необхідність у вирішенні питань захисту персональних даних клієнтів банку, тобто у банківській сфері, в державі згідно з принципами європейських стандартів. Проте теоретичні і практичні питання щодо підвищення ефективності системи управління захистом персональних данних клієнтів банку в Україні, на жаль, залишалися поза увагою вчених та інших представників науки.

**Аналіз останніх досліджень і публікацій**. Сама система управління захистом персональних даних клієнтів банку в Україні в правовому полі регулюється на основі національних законодавчих актів, серед яких є: Закони України «Про захист персональних данних», «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних данних» [2], «Про інформацію»[3], «Про банки і банківську діяльність»[4] та інших нормативних актів та рекомендацій Національного банку України і Державної служби України з питань захисту персональних даних. Проте, на сьогоднішній день проблематика питання щодо підвищення та оптимізації ефективності системи управління захистом персональних даних клієнтів банку повністю і досконало не вирішена. Основну увагу у вирішені цієї проблеми в Україні приділяють такі вчені: В.В. Домарєв, А.С.Савченко (директор департаменту інформатизації), В.А. Швець, В.В. Шестаков та інші. Швець у своїй книжці «Організаційне забезпечення захисту інформації з обмеженим доступом» [5] на основі аналізу та узагальнення матеріалу нормативних і законодавчих актів висвітлює питання організації та діяльності підрозділу захисту інформації, порядок здійснення захисту інформації на об’єктах інформаційної діяльності підприємства.

А вже інший відомий вчений Домарев В.В. у своїй праці «Управління інформаційною безпекою в банківських установах (теорія і практика впровадження стандартів серії ISO 27k)» [6] на прикладі банківських інформаційних технологій розглянув практичні і теоретичні питання впровадження вимог міжнародних стандартів управління інформаційною безпекою серії ISO 27k, і надав практичні і

методичні рекомендації щодо організації захисту інформації. Також в книжці є розділ про банківське шахрайство і зловживання службовим становищем працівників банків, де проводиться детальний аналіз цих загроз і передумови їх виникнення.

**Не вирішена раніше частина загальної проблеми**. На сьогодні механізм захисту персональних даних клієнтів банку не достатньо досконалий і потребує суттєвого доопрацювання. Сам процес роботи банків з персональними даними має бути врегульовуваним не тільки шляхом прийняття відповідних процедурних документів в самому банку, але і на державному рівні шляхом прийняття відповідного спільного документу Національним банком України та Державною службою України з питань захисту персональних даних. Також вирішення даного питання по захисту персональних даних обов'язково повинно включати в себе розробку відповідної політики безпеки банку щодо захисту персональних даних та побудову власної системи захисту, яка буде спиратись на європейський досвід по захисту персональних даних (наприклад, BS 10012:2009 «Захист даних. Специфікація системи управління персональними даними» [7]). Тобто мова йде про створення не вузькоспеціалізованої системи захисту, а цілісної системи управління персональними даними, яка могла б оперативно реагувати на випадки несанкціонованого доступу до них.

Також особливу увагу потрібно приділити застосуванню системних продуктів таких як ArcSight ESM, та на новинку захисту персональних даних - тест на проникнення.

**Метою статті** є підвищення ефективності системи управління захистом персональних даних клієнтів банку та практичне застосування цієї моделі на підприємстві для доказу її ефективності та доцільності.

**Виклад основного матеріалу**. Проблемою захисту персональних даних за кордоном почали займатися у другій половині XX століття. В цей час швидко розвивалися технології обміну інформацією, що давало можливість бізнесу стрімко розвиватися. Але це, водночас, збільшило кількість зловживань у комерційній діяльності (зокрема банківській), насамперед шляхом незаконного використання персональних даних клієнтів. Інформація про клієнтів має велику цінність, тому сьогодні її вартість є надзвичайно високою.

На сьогоднішній день персональні дані проникли в різні сфери як життя так і бізнесу, отож питанням при їх захисті треба займатися не тільки для задоволення законних вимог, але і для власної безпеки.

Нині організована злочинність активно і наполегливо намагається проникнути до найбільш прибуткових сфер діяльності комерційних структур. Тому проникнення до комерційних банків є особливо бажаною метою злочинних угруповань, адже підпорядкування їх злочинцям може дати великі можливості для здійснення значних махінацій, відмивання "брудних грошей", переведення їх за кордон та інших дій, які приносили б злочинним елементам величезні доходи. Водночас умови конкурентної боротьби роблять нерівномірним розвиток підприємницької діяльності, у тому числі й у банківській сфері. Це, у свою чергу, створює необхідність постійного пошуку шляхів удосконалення виробництва і технологій та зберігання їх у таємниці.

Пошук ринків, боротьба за клієнтів і нейтралізація конкурентів вимагають усебічної інформації. За таких умов ефективна діяльність банку може бути реалізована вжиттям як пасивних заходів безпеки, пов'язаних із різними видами захисту, так і активних дій сил безпеки, насамперед спрямованих на створення сприятливого інформаційного простору для роботи банку. Забезпечення інформаційної безпеки банку передбачає виконання таких завдань: інформаційно-аналітичний супровід прийняття рішень керівництвом банку; протидія спробам несанкціонованого збору інформації з обмеженим доступом, яка є власністю банку, його клієнтів або партнерів. Інформаційно-аналітичний супровід прийняття рішень керівництвом банку здійснюється шляхом збирання і аналітичної обробки інформації про стан і можливі перспективи діяльності суб'єктів банківського ринку.

Метою цієї діяльності є виключення можливості несподіваної появи несприятливих факторів і загроз діяльності банку та забезпечення прийняття управлінських рішень, здатних мінімізувати наслідки негативного впливу сфери діяльності банку. Протидія спробам несанкціонованого збору інформації з обмеженим доступом у банку передбачає виконання заходів з попередження неправомірного отримання інформації банку спецслужбами, конкурентами та зловмисниками з використанням технічних засобів або через працівників банку. Заходи протидії несанкціонованому збору інформації у банку спрямовуються на:

- розроблення відповідної нормативної бази, яка регулює режим і порядок доступу, зберігання і використання інформації банку;

- контроль дотримання заходів інформаційної безпеки працівниками банку;
- захист інформації в засобах і мережах її передавання та обробки.

Захист інформації банку з обмеженим доступом здійснюється усім персоналом банку відповідно до службових обов'язків. Розроблення нормативної бази захисту інформації в банку і контроль дотримання інформаційної безпеки працівниками банку здійснює підрозділ безпеки. Заходи захисту інформації в засобах і мережах її передавання та обробки передбачають використання апаратних, програмних та криптографічних засобів захисту.

Апаратні засоби захисту застосовуються для вирішення таких завдань:

- перешкоджання візуальному спостереженню і дистанційному підслуховуванню;
- нейтралізація паразитних електромагнітних випромінювань і наводок;
- виявлення технічних засобів підслуховування і магнітного запису, несанкціоновано використовуваних у приміщеннях банку;
- захист інформації, що передається засобами зв'язку і міститься в системах автоматизованої обробки даних.

Програмні засоби захисту представляють собою спеціальні програми, включені до складу програмного забезпечення комп'ютерів та інформаційних систем, які реалізують функції захисту конфіденційної інформації від неправомірних дій – несанкціонованого доступу, копіювання або руйнування.

Для захисту від несанкціонованого доступу за допомогою програмних засобів здійснюється:

- ідентифікація об'єктів і суб'єктів;
- розмежування доступу до інформаційних ресурсів;
- контроль і реєстрація дій з інформацією і програмами.

Захист інформації від копіювання забезпечується виконанням таких функцій:

- ідентифікація середовища, з якого запускається програма копіювання;
- автентифікація середовища, з якого запущена програма копіювання;
- реакція на запуск з несанкціонованого середовища;
- реєстрація санкціонованого копіювання;
- протидія вивченню алгоритмів роботи системи.

Якщо розглядати захист персональних даних з боку застосування програмно-технічних засобів захисту, то тут можна виділити спеціалізовані системи моніторингу подій інформаційної безпеки.

Одним із прикладів подібних систем є продукт ArcSight ESM. ArcSight CM - це провідна платформа на ринку для моніторингу корпоративних загроз і ризиків безпеки, яка займає одну з лідируючих позицій в даній області.

Цей продукт стане в нагоді:

- службі інформаційного контролю та аудиту (коли необхідно отримати задовільну оцінку аудиту);
- службі інформаційної безпеки (коли необхідно визначити хто хоче отримати доступ до інформації, і чи є у цієї особи відповідні повноваження);
- службі IT (коли інфраструктура повинна відповідати вимогам затвердженої політики і ми повинні швидко реагувати на нові загрози).

Рішення ArcSight ESM надає широкий спектр функцій, які забезпечують швидкий і зручний доступ до необхідної інформації. Настроювані панелі управління з прекрасною графікою забезпечують бізнес і технічний огляд інформації, необхідної конкретним співробітникам банку. Консоль ESM забезпечує єдиний огляд поточного рівня безпеки компанії та надає інформацію про виявлені атаках і бізнес - ризики. Наявні мережеві та географічні карти дозволяють користувачам виявити загрози, які знаходяться в їх компетенції. Рішення ArcSight ESM надає комплексні технічні, операційні та трендові звіти, в яких міститься інформація про поточний рівень безпеки. Ці звіти повністю задовольняють вимогам до підготовки контрольної звітності. Система підготовки звітів спрощує завдання підготовки звітності на рівні бізнесу завдяки наявності стандартних і користувальницьких шаблонів для звітів про відповідність вимогам регуляторів, звітів про бізнес-ризики та параметрах користувачів .

Сьогодні також є ще одна дуже цікава послуга в галузі захисту інформації - тест на проникнення. Тест на проникнення (penetration test або скорочено pentest) - це практичний спосіб показати, наскільки захищена компанія від зазіхань на її конфіденційні дані і інших загроз для інформації. За кордоном також часто зустрічається термін етичний хакінг (ethical hacking). Даний

метод симулює набір «хакерських» атак, цілі яких - проникнення у внутрішню інфраструктуру мережі компанії, крадіжка та / або модифікація конфіденційних даних, порушення роботи критичних бізнес процесів компанії. Кожен банк може перевірити свою систему безпеки на надійність і, виходячи з результатів цієї перевірки, вживати необхідних заходів. Ця послуга являє собою імітацію послідовності дій зломщика щодо здійснення несанкціонованого проникнення в інформаційну систему замовника.

Тест на проникнення є корисним з кількох причин:

- визначення можливості певного набору атак;
- виявлення вразливостей вищого ризику, які є результатом комбінації вразливостей меншого ризику, що використовуються в певній послідовності;
- виявлення вразливостей, які може бути важко або неможливо знайти за допомогою автоматизованої мережі або застосування програмного забезпечення із сканування вразливостей;
- оцінювання величини потенційного впливу успішних атак на бізнес;
- тестування здатності захисників мережі успішно виявляти і реагувати на атаки;
- надання доказів на підтримку збільшення інвестицій у персонал і технології безпеки.

Тести на проникнення є складовою частиною повного аудиту безпеки.

Цей вид аудиту зараз активно застосовується зарубіжними компаніями. В результаті успішного і якісного проведеного тестування на проникнення банк отримує підсумковий звіт, що відображає об'єктивний і реальний погляд на рівень інформаційної безпеки банку очима професійного хакера. Звіт також буде містить докладний технічний опис всіх вжитих і вдало реалізованих сценаріїв проникнення, аналіз усього можливого спектру впливу на інформаційну інфраструктуру банку, а також рекомендації щодо підвищення рівня захищеності кредитно-фінансової організації. Рекомендації містять покроковий опис тих дій, які необхідно вжити для підвищення рівня захищеності банку від зовнішніх загроз, що є на сьогоднішній день дуже доцільною порадою.

Заходи захисту від руйнування інформації передбачають заборону використання у банку несанкціонованого програмного забезпечення, використання спеціальних антивірусних програм, виконання архівації і резервування інформації тощо.

Отож, забезпечення інформаційної безпеки банку – це складна система заходів із забезпечення необхідного рівня інформованості керівництва і персоналу банку, а також зовнішнього середовища, ефективний захист усіх видів інформації від зовнішніх і внутрішніх загроз, що досягається організацією збору інформації про внутрішнє і зовнішнє середовище банку, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів, інформаційного аудиту та інформаційного моніторингу в банку, аналітичною обробкою інформації; організацією системи інформаційного забезпечення прийняття рішень керівництвом банку; визначенням категорій банківської інформації та виробленням відповідних заходів її захисту; дотриманням відповідних режимів діяльності банку; виконанням усіма працівниками банку норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів витоку інформації та їх нейтралізації.

Продовжуючи дослідження системи захисту персональних даних в банківській сфері, також бажано було б розглянути ***Рекомендації щодо порядку обробки персональних даних у базах персональних даних*** [8]. В них визначаються загальні правила та умови обробки персональних данних, встановлюються рекомендації щодо порядку збору персональних данних, порядок поширення персональних данних, знищення та зміна персональних даних , організація обробки персональних даних володільцями та розпорядниками баз персональних даних , особливості обробки персональних даних у картотеках персональних данних.

І вже недавно, завдяки зусиллям Державної Служби з питань захисту персональних даних 30 грудня 2011 Міністерством юстиції України був прийнятий Наказ №3659/5 "Про затвердження Типового порядку обробки персональних даних у базах персональних даних" [9]. Цей документ дозволяє визначити основні дії відносно персональних даних.

Крім того, у банку доцільно розробити такий документ з безпеки, як "Політика інформаційної безпеки банку". Політика інформаційної безпеки банківської установи являє собою науково обґрунтовану систему поглядів на визначення основних напрямків, умов і порядку практичного рішення задач інформаційного захисту банківської справи від протиправних дій. Під інформаційною безпекою банку розуміється стан захищеності інформації щодо власників, керівництва, клієнтів банку, технологій та інформаційних ресурсів банку від внутрішніх і зовнішніх погроз. Забезпечення інформаційної безпеки є невід’ємною складовою частиною діяльності

комерційного банку. Стан інформаційної безпеки банку являє собою уміння і здатність банку протистояти будь-яким спробам завдати шкоди законним інтересам банку.

Об'єктами безпеки є:

- інформація про персонал (керівництво, відповідальні виконавці, співробітники);
- інформація щодо технологій, які використовуються банком;
- інформаційні ресурси (інформація з обмеженим доступом, що складає банківську та комерційну таємницю, інша конфіденційна інформація, надана у виді документів і масивів незалежно від форми і виду їхнього представлення), в тому числі:
- інформація щодо діяльності та фінансового стану клієнта, що стала відома банку у процесі обслуговування;
- інформація щодо всіх операцій банку та фінансова звітність банку;
- конфіденційні електронні мережі банку.

Політика інформаційної безпеки банку створюється на основі результатів аудиту інформаційної інфраструктури та наявних систем і засобів захисту інформації банку. Політика інформаційної безпеки повинна бути затверджена, видана та належним чином доведена до відома всіх співробітників банку. Політика повинна визначати відповідальність керівництва та викладати підхід банку до управління захистом інформації. Доцільність розробки та затвердження такого документа передбачена міжнародними стандартами, зокрема, ISO 17799 «Інформаційна технологія. Практичні правила управління інформаційною безпекою»[10].

Цей документ повинен містити такі положення:

- визначення інформаційної безпеки, її загальних цілей та сфери дії;
- виклад цілей та принципів інформаційної безпеки;
- короткий виклад найбільш істотних для банку політик безпеки, принципів, правил та вимог, наприклад:
  1) відповідність законодавчим вимогам та договірним зобов'язанням;
  2) вимоги відносно навчання питанням безпеки;
  3) запобігання появам та виявлення вірусів й іншого шкідливого програмного забезпечення;
  4) управління безперервністю функціонування банку;
  5) відповідальність за порушення політики безпеки;
- визначення загальних та конкретних обов'язків співробітників у межах управління інформаційною безпекою, включаючи інформування про інциденти порушення інформаційної безпеки;
- посилання на документи, які доповнюють політику інформаційної безпеки, наприклад, більш детальні політики та процедури безпеки для конкретних інформаційних систем, а також правила безпеки, яких повинні додержуватися співробітники банку на автоматизованих робочих місцях.

За стандартом ISO 17799 у банку має бути призначена відповідальна за політику інформаційної безпеки службова особа, яка повинна відповідати за її реалізацію та перегляд відповідно до встановленої процедури.

У положеннях стандарту ISO 17799, як у національних нормативно правових актах, підкреслюється важливість використання цифрових підписів і шифрування для забезпечення конфіденційності переданої інформації між банками і т.ін.; забезпечення безпеки інтернет-банкінгу; забезпечення стійкості до вірусних атак; забезпечення безпеки електронної пошти. При цьому стандартом ISO 17799 вимагається, щоб криптографічні ключі, які використовуються для цифрових підписів, відрізнялися від тих, які використовуються для шифрування. При використанні цифрових підписів необхідно враховувати вимоги національного чинного законодавства, яке визначає умови, при яких цифровий підпис має юридичну силу.

Отже, як національні нормативно-правові акти, так і міжнародні стандарти дозволяють розробити внутрішньобанківські документи із забезпечення безпеки банку, зокрема Положення про політику безпеки банку. Проте вказані міжнародні стандарти визначають вимоги до розробки лише тих документів банку, які безпосередньо стосуються питань захисту інформації на об'єктах інформаційних технологій. Але для розробки ефективної політики банку також мають бути розроблені адміністративні (режимні, організаційні) заходи безпеки як окремий напрям (вид) захисту банку, заходи щодо захисту інформації від витоку технічними каналами. Тому у цих питаннях необхідно користуватися національними стандартами (ДСТУ, нормативними документами НД ТЗІ), нормативними актами НБУ тощо.

**Висновки**. Захист персональних даних - це досить важка і рутинна справа, яка спрямована на повне виключення несанкціонованого доступу до персональних даних клієнтів банку. Реалізувати цей захист в повній мірі можливо лише комплексно, тобто банк повинен прийняти відповідні правові, організаційні, технічні заходи, аби організувати і забезпечити надійний захист персональних даних від різного роду зловмисників і конкурентів.

Забезпечення безпеки персональних даних досягається:

1. Визначенням загроз безпеки персональним даним при їх обробці та подальшому використанні і зберіганні.
2. Застосуванням організаційних і технічних заходів щодо забезпечення безпеки персональних даних.
3. Оцінкою ефективності прийнятих заходів щодо забезпечення безпеки персональних даних.
4. Виявленням фактів несанкціонованого доступу до персональних даних і вживанням відповідних заходів безпеки.
5. Контролем за прийнятими заходами щодо забезпечення безпеки персональних даних та їх рівнем захищеності.

Тому на сьогоднішній день все більше і більше банків приходять до розуміння того, що відповідно до вимог міжнародних стандартів, а також правильно розроблена і побудована система захисту персональних даних дозволяють не тільки створити надійну інформаційну структуру, але й забезпечити надійне функціонування організації.

Отож, якщо застосовувати спеціалізовані системи моніторингу подій інформаційної безпеки і використовувати нетрадиційний аудит інформаційної безпеки - тест на проникнення, то можна з впевненістю сказати, що саме подібний варіант контролю за подіями в інформаційному середовищі банку по збереженню персональних даних і захисті від несанкціонованого доступу є найбільш ефективним на сьогоднішній час.

В подальших публікаціях планується дослідити модернізацію системи управління захистом персональних даних клієнтів банку, яка обов'язково буде пов'язана із розвитком сучасних інформаційних технологій, котрі суттєво допоможуть забезпечити надійний захист персональних даних клієнтів банку.

## ЛІТЕРАТУРА

1. Про захист персональних даних [Текст] : Закон України від 2 червня 2010 року № 2297-V. [Електронний ресурс]. - Режим доступу: http://www.president.gov.ua/documents/11965.html.

2. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : Закон України від 02.06.2011 року № 3454-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3454-17.

3. Про інформацію [Текст] : Закон України від 10.08.2012 року № 2657-XII [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12.

4. Про банки і банківську діяльність [Текст] : Закон України від 7 грудня 2000 року № 2121-III, остання редакція 11.10.2013 [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/2121-14.

5. Швець В.А., Домарев В.В., Шестаков В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навч. посіб. – К: НАУ, 2006, - 108с.

6. Домарев В.В., Домарев Д.В. «Управлінння інформаційною безпекою в банківських установах (теорія і практика впровадження стандартів серії ISO 27k). » – Донецьк: Велстар, 2012. – 146с.

7. BS 10012:2009 «Захист даних. Специфікація системи управління персональними даними» - Режим доступу: http://shop.bsigroup.com/ProductDetail/?pid=000000000030175849.

8. Рекомендації щодо порядку обробки персональних даних у базах персональних даних [Електронний ресурс]. – Режим доступу: http://www.kadrovik.ua/content/rekomendats-shchodo-poryadku-obrobki-personalnikh-danikh-u-bazakh-personalnikh-danikh.

9. Про затвердження Типового порядку обробки персональних даних у базах персональних даних : Закон України від 30.12.2011 року №3659/5 . [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0001-12.

10. Міжнародний стандарт ISO 17799:2000 «Інформаційна технологія. Практичні правила управління інформаційною безпекою (Інформаційні технології - Кодекс Практичні правила управління інформаційної безпеки)». [Електронний ресурс]. – Режим доступу: http://www.kmgep.kz/data/filedat/default/ISO_IEC_17799_2000_rus.pdf.

Надійшла 18. 02. 2014р. Рецензент д.т.н., проф. Тупкало В.М.