Главным преимуществом метода является тот факт, что перед началом контрольных испытаний не обязательно иметь информацию о параметрах КО и нет необходимости в ИЛ с более точными характеристиками. Однако, поскольку каждая ИЛ исследует свой «персональный» набор КО, то общее количество задействованных образцов велико, что для системы ТЗИ практически невозможно реализовать.

VI Выводы

1. Специфика ИЛ как объекта контрольных сличительных испытаний заключается в том, что необходимо учитывать влияние на результат измерения как лабораторных факторов (оборудование, оператор, условия окружающей среды и т. п.), так и параметров исследуемого объекта. В соответствии с этим предлагается комплексная оценка точности проводимых ИЛ испытаний, на основании которой можно делать заключение о профессиональном уровне ИЛ.

2. Кроме того, предложена классификация методов оценки профессионального уровня ИЛ, представленных в [6], в зависимости от наличия информации о параметрах исследуемого лабораторией объекта (СО с известными параметрами или КО с неизвестными параметрами). Такой подход позволяет выбрать оптимальный метод в каждом конкретном случае.

3. Из анализа методов оценки профессионального уровня можно заключить, что наиболее оптимальным является метод межлабораторных испытаний, который позволяет получить полную оценку точности испытаний, проводимых ИЛ. Однако, недостаток этого метода в том, что он требует использования значительного количества КО. Поэтому на сегодняшний день актуальной остается задача разработки методик проведения контрольных испытаний ИЛ с минимизацией используемых ресурсов.

Литература: ***1.*** *International Trade Centre. UNCTAD/WTO. Standards and Quality Management. Road map for quality. Guidelines for the Review of the Standardization, Quality Management, Accreditation and Metrology (SQAM). Infrastructure at National Level. 2004.* ***2.*** *ДСТУ ISO/IEC 17025-2001. Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій.* ***3.*** *Ефремова Н. Ю. Руководство по применению стандартов СТБ ИСО 5725. Практическое пособие. – Минск: БГИМ, 2003.* ***4.*** *ДСТУ 3021-95. Випробування та контроль якості продукції. Терміни та визначення.* ***5.*** *ISO 5725-94 Accuracy (trueness and precision) of measurement methods and results.* ***6.*** *ISO Guide 43-1997. Перевірка професійного рівня шляхом міжлабораторних порівнянь.* ***7.*** *Семенко Н. Г., Панева В. И., Лахов В. М. Стандартные образцы в системе обеспечения единства измерений. – М: Издательство стандартов, 1990 г.* ***8.*** *Руководство по выражению неопределенности измерения. – Государственное предприятие «Всероссийский научно-исследовательский институт метрологии им. Д. И. Менделеева». – С.-Петербург: 1999 г.* ***9.*** *ISO 3534-1: 1993. Statistics – Vocabulary and symbols – Part 1: Probability and general statistical terms.* ***10.*** *Смирнов Н. В., Дунин-Барковский И. В. Курс теории вероятностей и математической статистики для технических приложений. – М.: «Наука», 1969 г.* ***11.*** *ГОСТ 8.531-85 (СТ СЭВ 4569-84). Однородность стандартных образцов состава дисперсных материалов.* ***12.*** *ГОСТ 27872-88 (СТ СЭВ 5892-87). Стандартные образцы. Методика изготовления и аттестации стандартных образцов состава горных пород и минерального сырья.*

УДК 65.012.8

АНАЛІЗ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ АСПЕКТІВ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ ГАЛУЗІ УКРАЇНИ

Віталій Носов, Олександр Манжай

Харківський національний університет внутрішніх справ, м. Харків

Анотація: **Аналізуються організаційно-технічні аспекти системи захисту інформації в банківській галузі України та пропонуються шляхи її вдосконалення.**

Summary: **In the article the organizationally technical aspects of the information security system are analyzed in bank industry of Ukraine and the ways of its perfection are offered.**

Ключові слова: **Організація захисту інформації, банківська сфера, захист електронного документообігу, банківська таємниця.**

I Вступ

Розвиток інформаційних технологій зумовлює прогрес в усіх сферах людського життя. Нинішнє покоління людства стає свідком поступового переходу від індустріального суспільства до постіндустріального, однією з концепцій якого є, так зване, інформаційне суспільство. Збільшення ролі

інформації в житті світової спільноти звичайно призводить до підвищення вимог щодо її захисту. Особливого значення захист інформації набуває в такій чутливій царині як банківська сфера. І це не є випадковим. Адже стан банківської сфери впливає не тільки на економічну безпеку держави, але й безпосереднім чином – на повсякденне життя пересічних громадян.

Дослідження вимог щодо організації системи захисту інформації в банківській галузі України показало, що на даний момент в цій царині існує багато різнорідних нормативно-правових документів, які потребують системного упорядкування та доповнення з точки зору відомих підходів до організації захисту інформації.

Авторами дослідження проаналізовано організаційно-технічні аспекти системи захисту інформації в банківській галузі України та запропоновано шляхи її вдосконалення.

II Основна частина

Аналіз нормативних документів, які регламентують захист інформації в банківській галузі України, дозволяє в контексті організації системи захисту інформації в банківських установах знайти відповіді на наступні питання.

Яка інформація відповідно до законодавства є об'єктом захисту? [1]

В Законі [1] за режимом доступу інформація поділяється на *відкриту* та *з обмеженим доступом* (ІзОД), яка в свою чергу поділяється на *конфіденційну* і *таємну*. В [2] поняття технічного захисту інформації (ТЗІ) визначається як діяльність, спрямована на обов'язкове забезпечення захисту інженерно-технічними заходами:

- інформації, яка складає *державну* і *іншу* передбачену законом *таємницю*;
- *конфіденційної* інформації, яка є власністю держави;
- *відкритої інформації*, важливої для держави, незалежно від того, де вказана інформація циркулює;
- *відкритої інформації*, важливої для особи і суспільства, якщо ця інформація циркулює в державних органах, підприємствах, установах і організаціях.

Для перших двох видів інформації захищаються – конфіденційність, цілісність та доступність, для останніх двох видів - цілісність та доступність.

Який орган визначає політику захисту інформації в банківській системі України?

Відповідно до [3] таким органом є Національний банк (НБ) України, який, зокрема, визначає напрями розвитку засобів захисту банківської інформації; реалізує державну політику з питань захисту державних секретів у системі Національного банку; здійснює методологічне забезпечення з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю.

Яка інформація в банківській системі складає державну таємницю?

Така інформація циркулює тільки в НБ України, і в загальному вигляді це відомості, що розкривають: організацію охорони перевезення спеціальних вантажів і охорони цінностей; технічні характеристики і систему захисту від підроблення монет та банкнот України нових зразків до офіційного повідомлення НБ України з цих питань; рецептурний склад матеріалів, які розробляються та застосовуються Банкнотно-монетним двором НБ України для виготовлення монет, банкнот України або цінних паперів.

Яка інформація відноситься до банківської таємниці?

В Законі [4] під *банківською таємницею* розуміється інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Тут же для банків визначені шляхи збереження банківської таємниці та порядок розкриття банківської таємниці.

Яка юридична відповідальність передбачена за порушення банківської таємниці?

Кодекси [5, 6, 7] передбачають цивільну, адміністративну та кримінальну відповідальність за незаконне розголошення, збирання, використання інформації, що становить банківську таємницю.

Які вимоги Національного банку України щодо захисту банківської таємниці?

В [8] НБ України зобов'язує всі банки забезпечувати зберігання та захист інформації, яка містить банківську таємницю. В загальному вигляді регламентовано такі *організаційні заходи захисту* банківської таємниці:

- працівники банку в разі прийняття їх на роботу підписують зобов'язання щодо збереження банківської таємниці;
- банки зобов'язані за погодженням із клієнтом відображати в договорах, що укладаються між банком і клієнтом, застереження щодо збереження банківської таємниці та відповідальності за її незаконне розголошення або використання;

- суб'єкти, які мають доступ до інформації, що містить банківську таємницю, у власних інструкціях з діловодства з урахуванням особливостей своєї діяльності повинні встановити особливий порядок реєстрації, використання, зберігання та доступу до документів, що містять банківську таємницю;
- банки зобов'язані у внутрішніх положеннях встановити спеціальний порядок ведення діловодства з документами, що містять банківську таємницю, зокрема визначити:
  - порядок реєстрації вихідних документів, роботи з документами, що містять банківську таємницю, відправлення та зберігання документів, які містять банківську таємницю;
  - особливості роботи з електронними документами, які містять банківську таємницю;
- під час роботи з документами, що містять гриф "Банківська таємниця", працівники банку мають забезпечити зберігання таких документів у сейфах або шафах, які надійно замикаються і до яких не мають доступу треті особи;
- забороняється відправлення документів з грифом "Банківська таємниця" з використанням факсимільного зв'язку або іншими каналами зв'язку, що не забезпечують захист інформації;
- під час роботи з документами, що містять банківську таємницю на електронних носіях, банки мають забезпечити дотримання таких вимог:
  - позначка грифа "Банківська таємниця" до інформації та даних в електронному вигляді, що мають визначений формат і обробляються автоматизованими системами, а також до лістингів програмних модулів не додається;
  - для текстових повідомлень, які створюються, оброблюються, передаються та зберігаються в електронному вигляді, наявність позначки грифа "Банківська таємниця" є обов'язковою;
  - автоматизовані системи оброблення інформації повинні мати вбудовану систему захисту інформації;
  - обмежити доступ користувачів автоматизованої системи лише в межах, що необхідні для виконання їх службових обов'язків;
  - передавання інформації, яка містить банківську таємницю, електронною поштою або в режимі on-line здійснюється лише в захищеному (зашифрованому) вигляді з контролем цілісності та з обов'язковим наданням підтвердження про її надходження з електронним підписом отримувача з використанням засобів захисту;
  - у разі відправлення даних на електронному носії додається супровідний лист у письмовій формі з грифом "Банківська таємниця", у якому зазначаються дані про вміст носія;
  - архіви в електронному вигляді зберігаються на серверах або зовнішніх носіях у захищеному вигляді із забезпеченням контролю цілісності інформації під час роботи з архівними документами

Також в [8] регламентується порядок та межі розкриття банками інформації, що містить банківську таємницю, компетентним органам та НБ України.

Як законодавчо визначено поняття електронних документів і передбачено їх обіг в інформаційно-телекомунікаційних системах?

Діяльність банків в значній мірі пов’язана з обігом інформації на електронних носіях, і ця інформація є об’єктом технічного захисту. Тому потрібно визначити поняття електронного документу (яким може бути будь-який платіжний інструмент) та регламентовану систему забезпечення його безпеки.

В законі [9] визначено, що *електронний документ* – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи *обов'язкові реквізити* документа. *Електронний підпис* є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу. Накладанням електронного підпису завершується створення електронного документа. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. Також в [9] вказані основні принципи організації електронного документообігу.

Електронний документообіг в банківських розрахунках чутливий до часових параметрів чинності платіжних документів, тому ще одним важливим реквізитом електронного документу є *позначка часу*. Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу встановлено відповідною постановою КМ України [10], де визначено, що послуги фіксування часу надаються *акредитованими центрами сертифікації ключів* або *центрами сертифікації ключів.*

Який правовий статус електронного цифрового підпису і відносин, що виникають при його використанні?

В Законі [11] визначено правовий статус електронного цифрового підпису та врегульовано відносини, що виникають при використанні електронного цифрового підпису. Суб'єктами правових відносин у сфері послуг електронного цифрового підпису є:

- підписувач;

- користувач;
- центр сертифікації ключів;
- акредитований центр сертифікації ключів;
- центральний засвідчувальний орган;
- засвідчувальний центр органу виконавчої влади або іншого державного органу;
- контролюючий орган.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Схема взаємодії суб'єктів правових відносин у сфері послуг електронного цифрового підпису представлена на рис. 1, де ЕД – електронний документ.

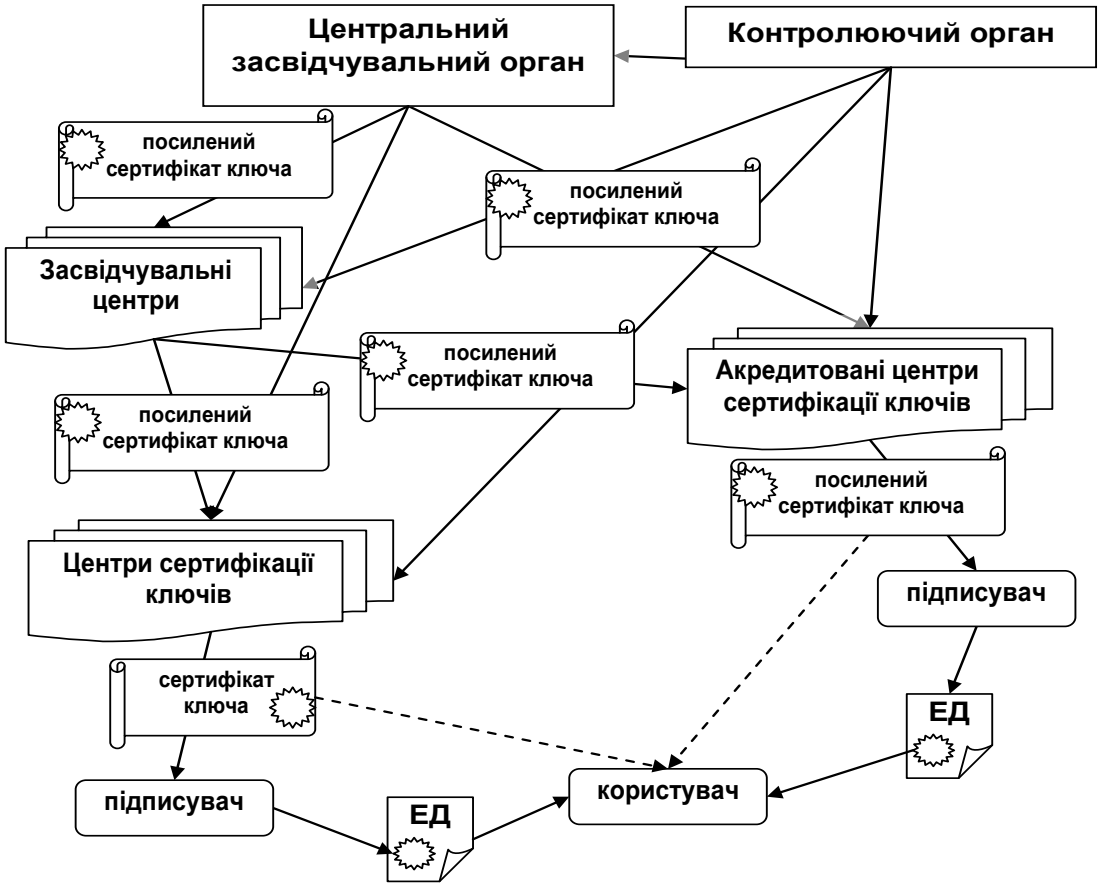

Рисунок 1 – Взаємодія суб'єктів правових відносин у сфері послуг електронного цифрового підпису

Порядок акредитації центру сертифікації ключів та правила посиленої сертифікації викладено в [2, 12].

Для того, щоб електронні банківські документи мали повноцінний юридичний статус і відповідні гарантії цілісності та авторства, банківській системі потрібно мати або свої акредитовані центри сертифікації ключів, або взаємодіяти з зовнішніми акредитованими центрами.

Як законодавством визначені правила захисту інформації в інформаційно-телекомунікаційних системах?

Законом [13] визначено, що умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

В державних банках інформація має оброблятися із застосуванням *комплексної системи захисту інформації* з *підтвердженою відповідністю*. Підтвердження відповідності здійснюється за результатами *державної експертизи* в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають *сертифікат відповідності* або *позитивний експертний висновок за результатами державної експертизи* у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює *службу захисту інформації* або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Вимоги до *комплексної системи захисту інформації* інформаційно-телекомунікаційних систем комерційних банків висуває НБ України в частині захисту автоматизованих робочих місць (АРМ-НБУ[1] та АРМ-СЕП[2]), підключених до системи електронних платежів або інформаційної системи НБ України і, де встановлені засоби захисту, які були отриманні згідно з договором з Національним банком. Умови та правила обробки інформації, яка становить банківську таємницю, у власних системах комерційні банки визначають самостійно.

Які вимоги захисту електронних банківських документів для банків-учасників системи електронних платежів Національного банку України?

Однією з основних операцій обробки інформації, що містить банківську таємницю, є переказ коштів із застосуванням платіжних систем. Закон [14] вимагає, щоб електронні документи на переказ, розрахункові документи та документи за операціями із застосуванням спеціальних платіжних засобів, що містять банківську таємницю, під час їх передавання засобами телекомунікаційного зв'язку були *зашифровані* згідно з вимогами відповідної платіжної системи.

Порядок захисту та використання засобів захисту інформації членами та учасниками міжнародних платіжних систем визначається правилами цих систем.

Захист інформації забезпечується шляхом обов'язкового впровадження та використання відповідної системи захисту, що складається з:

1) *законодавчих актів* України та інших нормативно-правових актів, а також внутрішніх *нормативних актів* суб'єктів переказу, що регулюють порядок доступу та роботи з відповідною інформацією, а також відповідальність за порушення цих правил;

2) *заходів охорони* приміщень, технічного обладнання відповідної платіжної системи та персоналу суб'єкта переказу;

3) *технологічних* та *програмно-апаратних засобів криптографічного захисту* інформації, що обробляється в платіжній системі.

Система захисту інформації має забезпечувати:

1) *цілісність інформації*, що передається в платіжній системі, та *компонентів* платіжної системи;

2) *конфіденційність інформації* під час її обробки, передавання та зберігання в платіжній системі;

3) *неможливість відмови* ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання;

4) *забезпечення постійного та безперешкодного доступу* до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором.

Розробка заходів охорони, технологічних та програмно-апаратних засобів криптографічного захисту здійснюється платіжною організацією відповідної платіжної системи, її членами або іншою установою на їх замовлення.

Більш детально вимоги захисту електронних банківських документів в СЕП Національного банку визначені в [15, 16, 17].

В [15, 16] визначені режимні вимоги та правила з технічного захисту інформації для приміщень банків, в яких обробляються електронні банківські документи. В цьому контексті ці приміщення поділяються на:

- *приміщення з обмеженим доступом* - приміщення, в яких розташовані робочі місця з комп'ютерною технікою, обробляються електронні банківські документи, що містять відомості з грифом "Банківська таємниця", та інша електронна інформація, доступ до якої обмежений банком;

---

[1] **АРМ-НБУ** - автоматизоване робоче місце з програмними засобами захисту інформації, призначене для роботи в інформаційних задачах Національного банку

[2] **АРМ-СЕП** - автоматизоване робоче місце АРМ-НБУ з програмними та апаратними засобами захисту інформації, призначене для роботи в системі електронних платежів (СЕП)

- *комутаційні кімнати* - приміщення, в яких розташовано телекомунікаційне обладнання, що забезпечує функціонування локальних і корпоративних мереж банку, а також зв'язок з іншими установами та мережами загального користування;
- *серверні приміщення* - приміщення, в яких розташовані сервери баз даних, сервери прикладних програм, файлові сервери тощо, на яких обробляються та зберігаються електронні банківські документи і бази даних.

До таких приміщень висуваються вимоги щодо: їх розташування, захисту вікон, оснащення відповідними системами контролю доступу, обладнання охоронною сигналізацією з кількома рубежами, наявності сейфів (металевих шаф), обліку ключів від сейфів і приміщень, переліку кола осіб, які мають доступ у приміщення і т. п. Додатково для технічного захисту інформації в серверних і приміщеннях електронних архівів виконується екранування приміщення або використовуються екрановані шафи, екрановані сейфи (клас опору до злому не нижче II), екрановані кабіни з метою запобігання витоку інформації через побічні випромінювання і наведення, а також порушенню її цілісності внаслідок впливу зовнішніх електромагнітних полів.

В [16] детально виписані вимоги до обладнання екранованих приміщень, систем заземлення, систем захисту від пошкодження блискавкою, систем електроживлення, побудови структурованих і локальних мереж.

Для забезпечення доступності інформації в СЕП передбачено *три рівня резервування* центру оброблення СЕП (ЦОСЕП), який розташований в Центральній розрахунковій палаті (ЦРП) Національного банку. Для учасників СЕП передбачено надання технологічної документації щодо відновлення роботи СЕП за кожним рівнем резервування. Також учасники СЕП зобов’язані мати *резервний комп'ютер*, підготовлений для забезпечення роботи АРМ-СЕП в разі виходу з ладу основного комп'ютера, на якому розгорнута діюча версія АРМ-СЕП, та вжити заходи для створення резервних копій службових файлів ключової інформації АРМ-СЕП, файлів конфігурації та допоміжних файлів.

В [17] наведені вимоги щодо захисту електронних банківських документів у банках-учасниках СЕП. *Система захисту електронних банківських документів* (система захисту) забезпечує:

а) захист від несанкціонованої модифікації та несанкціонованого ознайомлення зі змістом електронних банківських документів на будь-якому етапі їх оброблення;

б) автоматичне ведення захищеного від несанкціонованої модифікації протоколу оброблення електронних банківських документів з метою визначення причин появи порушень роботи програмно-технічних комплексів у СЕП;

в) захист від технічних порушень роботи апаратури (у тому числі від псування апаратних і програмних засобів, перешкод у каналах зв'язку);

г) умови для роботи програмно-технічних комплексів у СЕП, за яких фахівці банків - учасників СЕП і Національного банку не можуть втручатися в оброблення електронних банківських документів після їх формування, та автоматичний контроль на кожному етапі їх оброблення.

Система захисту:

а) охоплює всі етапи розроблення, впровадження та експлуатації програмно-технічного забезпечення в банках (філіях);

б) включає технологічні, апаратні, програмні засоби та організаційні заходи захисту;

в) визначає чіткий розподіл відповідальності на кожному етапі підготовки, оброблення та виконання електронних банківських документів на всіх рівнях.

Технологічні засоби безпеки в СЕП включають:

- механізм обміну квитанціями, який дає змогу однозначно ідентифікувати отримання адресатом будь-якого файлу або пакета електронних банківських документів у СЕП і забезпечує можливість контролю отриманої в ньому інформації;
- механізм інформування банку-учасника СЕП щодо поточного стану його кореспондентського рахунку за підсумками циклів оброблення платежів у ЦОСЕП;
- механізм надання банку-учаснику СЕП інформації щодо поточного стану його технічного рахунку;
- взаємообмін між банком і ЦОСЕП технологічною інформацією за підсумками банківського дня з переліком відображених за технічним рахунком міжбанківських електронних розрахункових документів, які оброблені засобами СЕП у файловому режимі та режимі реального часу, що дає змогу здійснювати їх програмне звіряння як у ЦОСЕП, так і в банку;
- програмний комплекс самодіагностики, який дає змогу виявляти порушення цілісності баз даних програмного забезпечення ЦОСЕП, псування яких може виникнути внаслідок порушень функціонування системи, спроб несанкціонованого доступу або фізичного псування баз даних;

- автоматичний механізм контролю за несанкціонованим модифікуванням робочих модулів;
- механізм резервування для забезпечення швидкого відновлення роботи ЦОСЕП з мінімальними втратами інформації.

Технологічні засоби безпеки, вбудовані в програмне забезпечення, не можуть бути відключені. У разі виникнення нестандартної ситуації або підозри щодо несанкціонованого доступу ЦОСЕП автоматично формує повідомлення для оперативного реагування ЦРП.

АРМ-СЕП включає вбудовані засоби захисту, що забезпечують конфіденційність і цілісність інформації під час її пересилання каналами зв'язку. Вбудовані засоби захисту інформації забезпечують два режими роботи АРМ-СЕП з використанням *апаратних* і *програмних засобів криптографічного захисту*. АРМ-НБУ включає вбудовані програмні засоби захисту, які забезпечують *програмне шифрування*.

До апаратних засобів захисту для СЕП відносяться: *апаратура криптографічного захисту інформації (АКЗІ)*; *смарт-картки*; *програмне забезпечення керування АКЗІ* (вбудоване в АРМ-СЕП і не може бути вилучене). До програмних засобів захисту для СЕП та інформаційних задач відносяться: *програмний модуль для шифрування* (вбудований в АРМ-СЕП та АРМ-НБУ); *програмний модуль генерації ключів (ПМГК)* з відповідними незаповненими таблицями відкритих ключем (ТВК); *бібліотеки накладання/перевірки ЕЦП* (Національний банк надає безкоштовно всім організаціям, які використовують засоби захисту, для вбудовування в програмне забезпечення системи автоматизації банків (САБ) або інше відповідне програмне забезпечення).

Апаратно-програмні засоби криптографічного захисту інформації в СЕП забезпечують автентифікацію відправника та отримувача електронних банківських документів і службових повідомлень СЕП, гарантують їх достовірність та цілісність, неможливість підроблення або викривлення документів у шифрованому вигляді та за наявності ЕЦП.

Для здійснення суворої автентифікації банків (філій), які є учасниками СЕП, застосовується система ідентифікації користувачів, яка є основою системи розподілу ключів криптографічного захисту. На робочих місцях САБ, де формуються та обробляються електронні банківські документи, використовуються *ідентифікатори ключів* криптографічного захисту, логічна структура яких зображена на рис. 2.

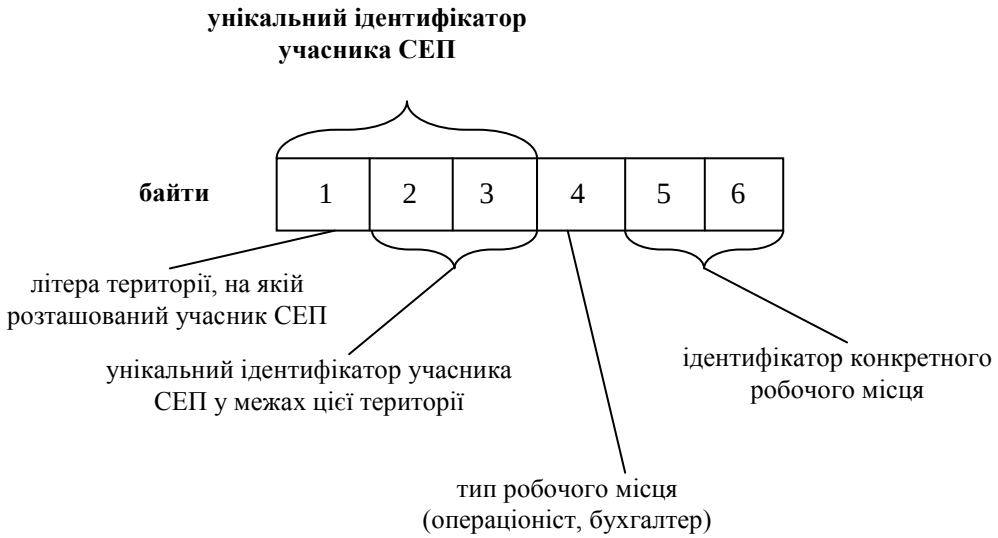

Рисунок 2 – Логічна структура ідентифікатора ключів криптографічного захисту

Ідентифікатори ключів записуються в АКЗІ, яка надається учасникам СЕП і забезпечує апаратне формування (перевірку) ЕЦП та апаратне шифрування (розшифрування) на АРМ-СЕП.

Для забезпечення захисту інформації від модифікації з одночасною суворою автентифікацією та безперервного захисту електронних банківських документів з часу їх формування система захисту СЕП включає *механізми формування (перевірки) ЕЦП* на базі несиметричних алгоритмів RSA та ДСТУ 4145.

Для забезпечення роботи алгоритму RSA учасник СЕП отримує від територіального управління *персональний генератор ключів з вбудованим ідентифікатором учасника СЕП* (*ПГК з ІУ СЕП*). За допомогою цього генератора ключів учасник СЕП має змогу генерувати ключі для всіх робочих місць, де працюють з електронними банківськими документами. Кожен таємний ключ робочого місця обов'язково має бути захищений особистим паролем відповідальної особи, яка працює з цим ключем. Для забезпечення захисту ключової інформації (а саме відкритих ключів) від несанкціонованої модифікації відкриті ключі

ЕЦП мають надсилатися до Департаменту інформатизації для сертифікації (крім відкритих ключів для робочих місць операціоністів, що використовуються лише в САБ). Логічна схема генерації та розподілу ключів ЕЦП в банку показана на рис.3.

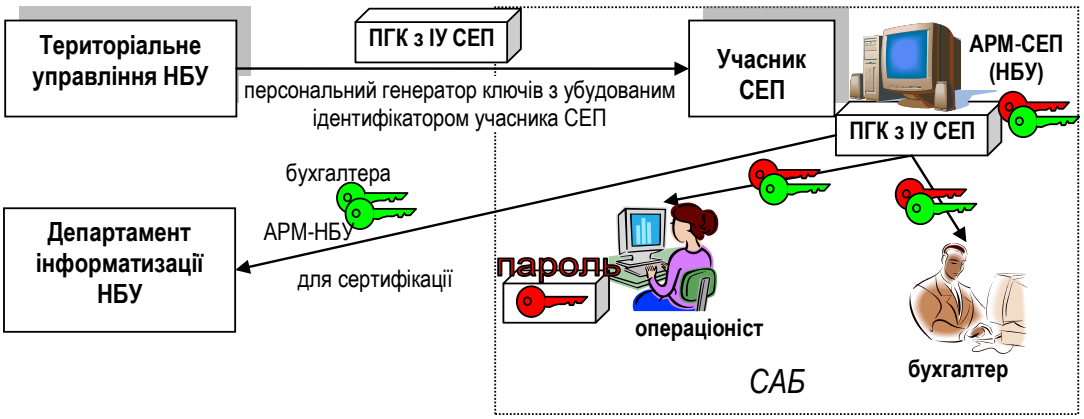

Рисунок 3 – Логічна схема генерації та розподілу ключів ЕЦП

Генерація ключів для АКЗІ здійснюється на комп'ютері, де розміщується програмно-технічний комплекс АРМ-СЕП, за допомогою генератора, вбудованого в АРМ-СЕП. Для забезпечення неперервної роботи АРМ-СЕП з апаратурою захисту під час генерації ключа АКЗІ згенерований ключ має бути записаний на *дві смарт-картки* (основну та резервну).

Під час формування електронного банківського документа (ЕБД) на робочому місці операціоніста САБ відповідальна особа, яка формує цей документ, має накладати ЕЦП на документ за допомогою свого таємного ключа. Під час формування файлу (пакету) електронних банківських документів на робочому місці бухгалтера САБ накладається ЕЦП на цей файл (пакет) у цілому, що забезпечує його захист від модифікації. Сформований таким чином файл (пакет) обробляється АРМ-СЕП, де виконується перевірка ЕЦП операціоніста на кожному електронному банківському документі та накладається ЕЦП АРМ-СЕП, який можуть перевірити всі учасники СЕП. Під час оброблення файлів (пакетів) ЦОСЕП виконує перевірку підписів на кожному електронному банківському документі та файлі (пакеті) у цілому та після формування файлів (пакетів) відповідних платежів накладає ЕЦП на файл (пакет) у цілому за допомогою таємного ключа ЦОСЕП. Разом з цим на кожному електронному банківському документі залишається ЕЦП АРМ-СЕП учасника СЕП, який відправляв цей електронний банківський документ. Під час отримання файлів (пакетів) відповідних платежів виконується така сама перевірка (накладання) ЕЦП до часу остаточного оброблення документів операціоністом САБ отримувача. Логічна схема накладання (перевірки) ЕЦП показана на рис.4.

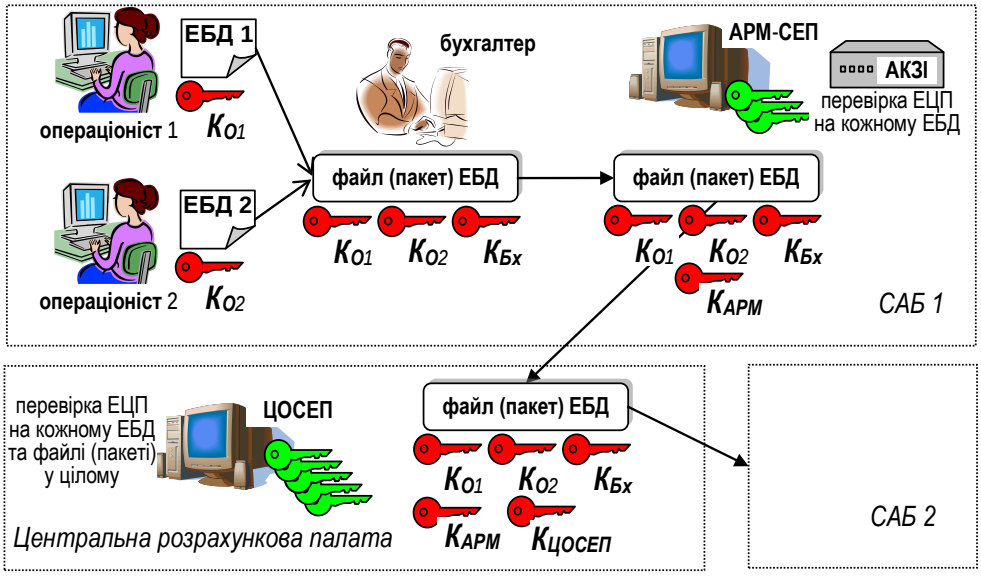

Рисунок 4 – Логічна схема накладання (перевірки) ЕЦП

Основним засобом шифрування файлів (пакетів) СЕП є *АКЗІ*. Робота АКЗІ контролюється вбудованими в АРМ-НБУ програмними засобами захисту інформації і забезпечує апаратне шифрування (розшифрування) інформації за стандартом ГОСТ 28147[3].

Як *резервний засіб шифрування* в СЕП використовується вбудована в АРМ-СЕП *функція програмного шифрування*. Для кожного файлу (пакету) СЕП, що обробляється АРМ-СЕП, генерується *одноразовий ключ шифрування* для алгоритму ГОСТ 28147-89, який обробляється відповідно до стандарту ISO 11166-94[4] і додається до повідомлення в зашифрованому вигляді. Такий спосіб передавання повідомлень забезпечує розшифрування їх лише дійсним отримувачем повідомлень (рис. 5).

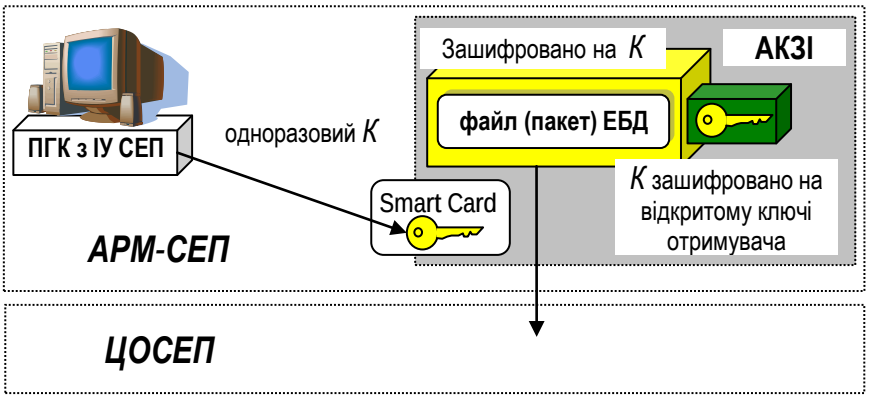

Рисунок 5 – Спосіб передавання повідомлень

Узагальнюючи, можна зазначити криптографічні стандарти, які використовуються в СЕП України (рис. 6).

Криптографічні стандарти, які використовуються в СЕП України

несиметричні криптографічні алгоритми	**симетричні криптографічні алгоритми**
ДУТУ 41445 – формування (перевірка) ЕЦП	ГОСТ 28147-89 **–** апаратне шифрування (розшифрування) в АКЗІ
ISO 11166-94 – розподілення ключів для симетричних алгоритмів шифрування	

Рисунок 6 – Криптографічні стандарти, які використовуються в СЕП України

Засоби шифрування АРМ-СЕП (як АКЗІ, так і програмне шифрування) забезпечують сувору автентифікацію відправника та отримувача електронного банківського документа, цілісність кожного документа в результаті неможливості його підроблення або несанкціонованого модифікування в шифрованому вигляді.

[3] **ГОСТ 28147-89** — радянський і російський стандарт симетричного шифрування, введений в 1990 році. Повна назва «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

[4] **ISO/IEC 11166-94** - "Банковское дело. Управление ключами посредством асимметричного алгоритма". Часть 1. Принципы процедуры и форматы. Часть 2. Принятые алгоритмы, использующие криптосистему RSA.

АРМ-СЕП в режимі реального часу забезпечує додаткову сувору взаємну автентифікацію АРМ-СЕП учасника СЕП та ЦОСЕП під час встановлення сеансу зв'язку.

Під час роботи АРМ-СЕП створює *шифровані архіви оброблених електронних банківських документів* та захищений від модифікації *протокол роботи АРМ-СЕП*, у якому фіксуються всі дії, що ним виконуються, із зазначенням дати та часу оброблення електронних банківських документів. Наприкінці банківського дня шифровані архіви та протокол роботи АРМ-СЕП підлягають обов'язковому збереженню в архіві. Цей архів використовується для надання Національним банком інформаційних послуг у разі виникнення спорів.

Ключова інформація під час роботи АКЗІ використовується виключно всередині смарт-картки, що унеможливлює підроблення та перехоплення ключової інформації (рис. 7). Ключова інформація для програмного шифрування та для ЕЦП має генеруватися безпосередньо відповідальною особою банку (філії) в присутності адміністратора захисту інформації банку (філії) за допомогою генератора ключів, який надається учаснику СЕП територіальним управлінням. Генератори ключів є персональними для кожного учасника СЕП, мають вбудований унікальний ідентифікатор учасника СЕП, який не може бути вилучений або змінений. Генератори мають змогу запису таємного ключа на носії двох видів – *на дискету* або на *Touch Memory*[5], в якому додатково вбудований захист від копіювання ключової інформації з одного носія на інший (рис. 7). Таємні ключі, які зберігаються на дискетах, обов'язково мають бути *захищені паролем*, що забезпечує додатковий захист від спроб несанкціонованого використання скопійованих таємних ключів. *Довжина пароля становить шість символів* і не може бути зменшена.

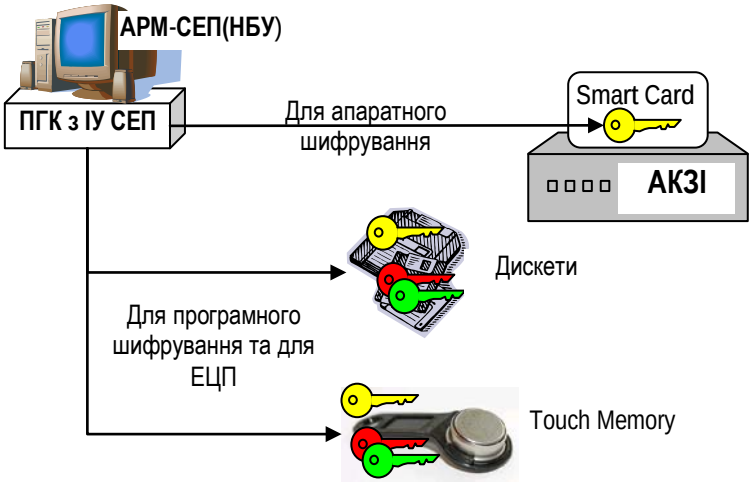

Рисунок 7 – Збереження ключової інформації

Для учасників СЕП передбачено виконання *організаційних заходів* інформаційної безпеки, які полягають у наступному:

- *укладення договору про використання криптографічних засобів захисту інформації* в СЕП НБУ між банком (філією) і територіальним управлінням тієї області, в якій розташований банк (філія);
- *забезпечення відповідності приміщень*, у яких обробляються електронні банківські документи, використовуються та зберігаються в неробочий час засоби захисту інформації, вимогам до приміщень учасників СЕП, які використовують засоби захисту інформації Національного банку, що визначені нормативно-правовими актами Національного банку щодо правил організації захисту електронних банківських документів;
- *призначення службових осіб*, які відповідають за зберігання та використання засобів захисту інформації з поданням належно завіреної копії наказу про призначення до територіального управління;
- *подання листа-доручення про отримання конкретних засобів захисту інформації.*

Для забезпечення контролю за виконанням вимог щодо захисту інформації банками (філіями) територіальні управління НБ України мають виконувати планові та позапланові перевірки всіх учасників СЕП, що використовують засоби захисту інформації Національного банку. Визначено такий орієнтований перелік порушень в організації роботи із засобами захисту інформації НБ України.

[5] **Touch Memory** представляє собою незалежну пам'ять, яку розміщено в металевому корпусі. Корпус у вигляді невеликої пігулки без зусиль кріпиться на будь-якому носієві - виробі, картці, брелоці. Інформація записується і зчитується з пам'яті приладу простим торканням до зчитувального пристрою.

1. Використання засобів захисту інформації НБ України у внутрішній платіжній системі організації, які не є безпосередніми учасниками СЕП та/або інформаційних задач НБ України, системі «клієнт-банк» тощо.
2. Неправильний розподіл повноважень відповідальних осіб, які використовують засоби захисту інформації НБ України.
3. Платіжний документ організації, підписаний однією відповідальною особою цієї організації.
4. Допуск адміністратора захисту інформації або адміністратора САБ до оброблення електронних платежів.
5. Порушення правил генерації, використання та зберігання таємних ключів.
6. Використання засобів захисту інформації особами, які не були призначені відповідальними за роботу із засобами захисту інформації НБ України згідно з розпорядчим документом.
7. Передавання засобів захисту інформації НБ України в інші організації та використання засобів захисту інформації НБ України, які були видані іншим організаціям.
8. Використання для захисту електронних платежів засобів захисту інформації НБ України, контроль за якими був утрачений.
9. Наявність неврахованих копій засобів захисту інформації НБ України (програмного модуля генерації ключів, таємних ключів тощо).
10. Наявність копій таємних ключів операціоністів, невчасне вилучення з таблиці відкритих ключів АРМ-СЕП/АРМ-НБУ відкритих ключів операціоністів, які припинили оброблення електронних платіжних документів.
11. Зберігання на жорсткому диску ПЕОМ АРМ-СЕП/АРМ-НБУ програм, які не використовуються під час оброблення електронних банківських документів.

В [15] розкрито: порядок отримання засобів захисту; порядок роботи з апаратними засобами захисту та ПМГК; порядок зберігання та роботи з таємними ключами програмних засобів захисту; призначення відповідальних осіб за роботу із засобами захисту. Детально виписані функціональні обов'язки: адміністратора захисту інформації; адміністратора АРМ-СЕП/АРМ-НБУ організації; операторів АРМ бухгалтера САБ, операціоністів та операторів інших робочих і технологічних місць САБ та інформаційних задач, які працюють із засобами захисту. Визначена організація діловодства з питань захисту інформації з переліком обов’язкових документів, порядок перевірки готовності організації до включення в СЕП, порядок повернення засобів захисту, використання і зберігання засобів захисту в разі виникнення надзвичайних ситуацій, порядок інформування територіального управління/Центральної розрахункової палати Національного банку та контроль за організацією захисту інформації в організації.

Чи потрібно ліцензування діяльності в сфері криптографічного захисту інформації в банківській системі України?

При експлуатації комерційними банками засобів криптографічного захисту інформації виникають питання ліцензування діяльності у сфері криптографічного захисту інформації в банківській системі України. Деяке роз’яснення щодо цього дає відповідний інформаційний лист НБ України [18].

1. Банківські установи, які є учасниками інформаційної мережі НБ України та використовують виключно засоби криптографічного захисту інформації, що надаються НБ України в системі електронних платежів або в інформаційних завданнях НБ України, не отримують ліцензії на право провадження господарської діяльності в галузі криптографічного захисту інформації.

НБ України самостійно здійснює контроль щодо порядку та умов використання банківськими установами вказаних засобів криптографічного захисту інформації.

2. Ліцензію на право провадження господарської діяльності в галузі криптографічного захисту інформації отримує тільки банк – юридична особа, для філій центральної установи надаються копії ліцензій.
3. Дозвіл для ввезення засобів криптографічного захисту інформації для міжнародних платіжних систем надається Державною службою спеціального зв’язку та захисту інформації України без обов'язкового проведення державної експертизи за умови підтвердження необхідності та обов'язковості застосування конкретного засобу у відповідній платіжній системі.

III Висновки

Аналіз нормативних документів щодо організаційно-технічних аспектів системи захисту інформації в банківській галузі України дозволяє сформулювати наступні пропозиції щодо вдосконалення організації захисту банківської інформації.

1. Необхідно розробити типове положення про службу захисту інформації в системі автоматизації банка, яке уточнює положення НД ТЗІ 1.4-001-2000. «Типове положення про службу захисту інформації в автоматизованій системі» з урахуванням специфіки діяльності банків.

2. Доцільно розробити нормативно-методичні документи, що визначають основний перелік інформаційних загроз для банківської інформації (модель загроз) та методики оцінки вразливостей і ризиків для САБ.

3. Для отримання відповідних формальних гарантій захисту інформації системи обробки електронних банківських документів (платіжні системи) потребують сертифікації, наприклад, щодо відповідності міжнародному стандарту ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій».

4. З нормативних документів незрозумілою є легітимність цифрових підписів електронних банківських документів, тобто яким є статус центра сертифікації ключів Департаменту інформатизації НБ України, і входить він чи ні в схему взаємодії суб'єктів правових відносин у сфері послуг електронного цифрового підпису (рис. 1). Очевидно, що такий центр має бути в цій системі (принаймні для взаємодії з державними банками).

*Література: **1.** Закон України «Про інформацію» від 02.10.1992 // Відомості Верховної Ради України, 1992, № 48 (01.12.1992), ст. 650 (зі змінами та доповненнями на 23.06.2005). **2.** Постанова КМ України № 903 від 13 липня 2004 р. «Про затвердження Порядку акредитації центру сертифікації ключів» // Офіційний вісник України, 2004, № 28 (30.07.2004) (частина 1), ст. 1884 (зі змінами та доповненнями на 08.12.2006). **3.** Закон України «Про Національний банк України» від 20.05.1999 // Відомості Верховної Ради України, 1999, № 29 (23.07.1999), ст. 238. (зі змінами та доповненнями на 09.07.2007). **4.** Закон України «Про банки і банківську діяльність» від 07.12.2000 // Відомості Верховної Ради України, 2001, № 5-6 (09.02.2001), ст. 30 (зі змінами та доповненнями на 27.04.2007). **5.** Цивільний кодекс України від 16.01.2003 // Офіційний вісник України, 2003, № 11 (28.03.2003), ст. 461 (зі змінами та доповненнями на 31.05.2007). **6.** Кодекс України про адміністративні правопорушення від 07.12.1984 // Відомості Верховної Ради УРСР, 1984, додаток до № 51, ст. 1122 (зі змінами та доповненнями на 01.01.2008). **7.** Кримінальний кодекс України від 05.04.2001 // Відомості Верховної Ради України, 2001, № 25-26 (29.06.2001), ст. 131 (зі змінами та доповненнями на 01.10.2007). **8.** Постанова Правління Національного банку України № 267 від 14 липня 2006 року. «Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці» // Офіційний вісник України, 2006, № 32 (23.08.2006), ст. 2330 (зі змінами та доповненнями на 09.11.2006). **9.** Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 // Відомості Верховної Ради України, 2003, № 36 (05.09.2003), ст. 275 (зі змінами та доповненнями на 31.05.2005). **10.** Постанова КМ України № 680 від 26 травня 2004 р. «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу» // Офіційний вісник України, 2004, № 21 (11.06.2004), ст. 1428 (зі змінами та доповненнями на 08.12.2006). **11.** Закон України «Про електронний цифровий підпис» від 22.05.2003 // Відомості Верховної Ради України, 2003, № 36 (05.09.2003), ст. 276. **12.** Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України 13.01.2005 № 3 «Про введення в дію нормативного документу «Про затвердження Правил посиленої сертифікації»» // Офіційний вісник України, 2005, № 5 (18.02.2005), ст. 288 (зі змінами та доповненнями на 10.05.2006). **13.** Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 20.05.1999 // Відомості Верховної Ради України, 1994, № 31 (02.08.1994), ст. 286 (зі змінами та доповненнями на 31.05.2005). **14.** Закон України «Про платіжні системи та переказ коштів в Україні» від 05.04.2001 // Відомості Верховної Ради України, 2001, № 29 (20.07.2001), ст. 137 (зі змінами та доповненнями на 27.04.2007). **15.** Постанова Правління Національного банку України № 112 від 2 квітня 2007 року. «Про затвердження Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України» // Офіційний вісник України, 2007, № 31 (07.05.2007), ст. 1250. **16.** Постанова Правління Національного банку України № 243 від 4 липня 2007 року. «Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи» // Офіційний вісник України, 2007, № 62 (31.08.2007), ст. 2443 (зі змінами та доповненнями на 29.12.2007). **17.** Постанова Правління Національного банку України № 320 від 16 серпня 2006 року. «Про затвердження Інструкції про міжбанківський переказ коштів в Україні в національній валюті» // Офіційний вісник України, 2006, № 36 (20.09.2006), ст. 2507 (зі змінами та доповненнями на 16.11.2006). **18.** Лист Національного банку України № 24-112/876 від 31.05.2005 р. «Щодо ліцензування діяльності у сфері криптографічного захисту інформації в банківській системі України» [Електронний ресурс] / Ліга:Еліт: Мережна версія. **19.** Постанова КМ України № 377 від 29 березня 2006 р. «Деякі питання здійснення розрахунків за продані товари (надані послуги) з використанням спеціальних платіжних засобів» // Офіційний вісник України, 2006, № 13 (12.04.2006), ст. 882. **20.** Постанова КМ України № 1126 від 08.10.97 р. «Концепція технічного захисту інформації в Україні» [Електронний ресурс] / Ліга:Еліт: Мережна версія. **21.** Указ Президента України № 1229 від 27.09.99 р. «Про затвердження положення про технічний захист інформації в Україні» // Офіційний вісник України, 1999, № 39 (15.10.1999),*

ст. 1934 (зі змінами та доповненнями на 06.10.2000). ***22.*** *Наказ Служби безпеки України від 12 серпня 2005 року № 440. «Про затвердження Зводу відомостей, що становлять державну таємницю» // Офіційний вісник України, 2005, № 34 (09.09.2005), ст. 2089 (зі змінами та доповненнями на 28.12.2007).* ***23.*** *Постанова Правління Національного банку України № 620 від 10 грудня 2004 року. «Про затвердження Правил Національної системи масових електронних платежів» // Офіційний вісник України, 2005, № 2 (28.01.2005), ст. 93.* ***24.*** *Лист Національного банку України № 25-312/1359-6378 від 19.06.2006 р. «Щодо безпеки ринку платіжних карток в Україні» // Офіційний вісник нормативно-правових актів з митної справи, фінансів, податків та бухгалтерського обліку, 2006, 06, № 26*

УДК 621.396

СИСТЕМНЫЙ АНАЛИЗ ПРОЦЕССОВ ЭНЕРГОИНФОРМАЦИОННОГО ОБМЕНА НА ОИД

Владимир Журавлёв, Александр Архипов
Национальный технический университет Украины"КПИ"

Анотація: **Виконано системний аналіз сінергетичного енергоінформаційного обміну на ОІД. Визначені системоутворюючі фактори та функції відкритих дисипативних біологічних та технічних систем.**
Summary: **The system analysis of synergetic energy-information exchange on IAO is realized. System forming factors and open desiccative biological and technical systems functions are defined.**
Ключевые слова: **Системный анализ, синергетика, энергоинформационный обмен.**

I Введение

Современные темпы развития экономических и социальных общественных отношений характеризуюся резким увеличением объемов оперативной информации, непосредственно связывающей самостоятельных в принятии решений людей. В связи с этим возрастает социальная значимость параметров достоверности процесса защиты информации, в частности, конфиденциальности процесса речевого обмена информацией. Технической разведкой (ТР) противника интенсивно развиваются и совершенствуются угрозы информации $I\,[O(t)]$, содержащейся в речевом сигнале, что акцентирует значимость параметра достоверности защищенности, который обеспечивается процессом технической защиты предполагаемого канала утечки (КУ).

Независимо от темпов развития и внедрения систем передачи и обработки текстовой и видеоинформации, речевой процесс останется первичным методом преобразования вербальной информации $I(t)$ при обмене сведениями об объектах $O(t)$ мышления. В ходе реализации речевого процесса (РП) информация об объекте мышления $I\,[O(t)]$ кодируется в информативный речевой сигнал $sv^a(t) = f^C\{I[O(t)]\}$, информационным свойством которого является изменение параметров среды передачи сигнала в параметрах времени t и пространства ℓ канала передачи. На современном этапе развития технических средств, анализ и исследование информационного свойства РС в точках ℓ_i пространства выделенного помещения осуществляется после акустоэлектрического преобразования его в речевой электрический сигнал (РС) $sv_i(t) = f^{ae}[sv^a(t)]$ – аналоговую модель акустического сигнала.

II Постановка задачи

В соответствии с Законом Украины об информации [1] целью технической защиты процесса речевого обмена является предотвращение утечки, хищения, утраты, искажения и подделки (имитации) информации, содержащейся в РС. Факт отсутствия системной методологии [2], поясняющей как информационные свойства РС, так и пространство их параметров, определяет современный метод технической защиты. Отношение электрических мощностей речевого сигнала и сигнала маскирования $SN^K(t) = 10\lg\dfrac{N[sv(t)]}{N[sn(t)]}$ на границе зоны безопасности в настоящее время [3] характеризует параметр эффективности обеспечения параметров достоверности процесса защиты канала утечки.

В процессе эволюционного развития психофизиологическая речеслуховая система человека сформировала помехоустойчивый к мешающим природным акустическим сигналам метод кодирования вербальной информации в форму РС. Поэтому, свойство потенциальной помехоустойчивости метода