Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення

магістерської кваліфікаційної роботи
за освітньо-кваліфікаційним рівнем «магістр»
на тему:

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ

Виконав: студент 2-го курсу,
групи ТКС-18м
спеціальності 172 – Телекомунікації та радіотехніка _____.

_____ Бакісс Едена Маурісіна Бонже

Керівник: к.т.н., доцент каф. ТКСТБ
_____ Стальченко О.В.

«____» _____ 2019 р.

Рецензент: к.т.н., доцент каф. РТ
_____ Гаврілов Д.В.

«____» _____ 2019 р.

Вінниця ВНТУ - 2019 рік

Актуальність теми дослідження

Магістерська кваліфікаційна робота, присвячена дослідженню протоколів забезпечення інформаційної безпеки IP-телефонії, а також розробці пропозицій щодо вдосконалення цих протоколів для підвищення безпеки і ефективного функціонування при роботі по каналах зв'язку з різними параметрами, відповідає сучасній науковій проблематиці і є актуальною.

Однак залишається недостатньо освітленим питання забезпечення інформаційної безпеки для сценарію IP-телефонії точка-точка в разі, коли кореспонденти не мають заздалегідь виробленого ключового матеріалу. Також залишаються маловивченими ймовірносно-часові характеристики протоколів безпеки IP-телефонії і питання про вплив цих протоколів на виконання встановлених норм при використанні IP-телефонії.

Метою МКР є підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії і скорочення часу встановлення захищеного з'єднання.

Наукова новизна МКР

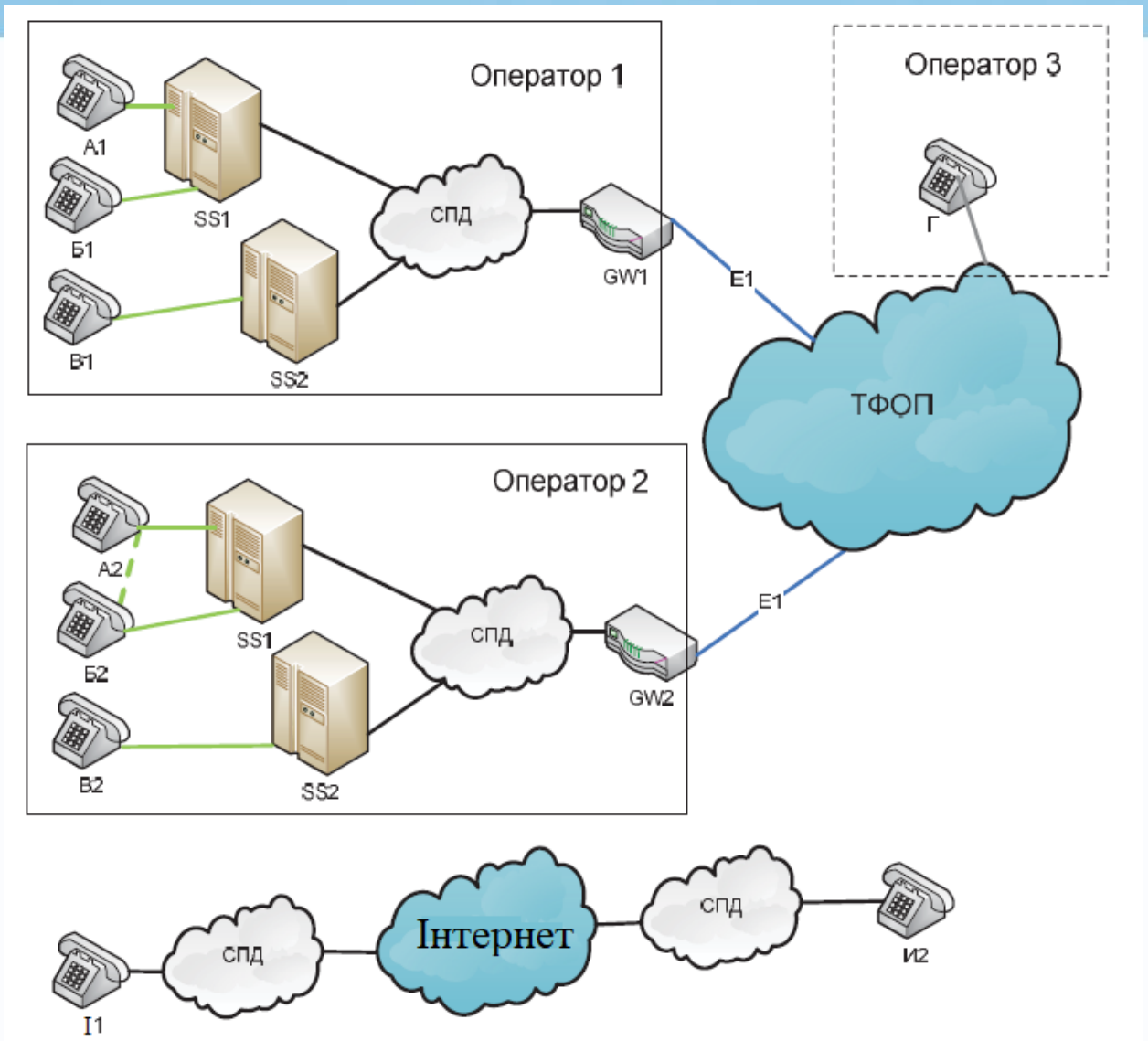
1. Розглянута модель порушника інфозахисту з урахуванням атаки на протоколи забезпечення безпеки IP- телефонії.

2. Виконане оцінювання ймовірнісно-часових характеристик протоколів розподілу ключів на відміну від існуючих враховує особливості протоколів розподілу ключів, виражені в наявності обмеження числа повторних передач повідомлень зі змінним таймером повторної передачі при роботі по каналах з помилками і затримками.

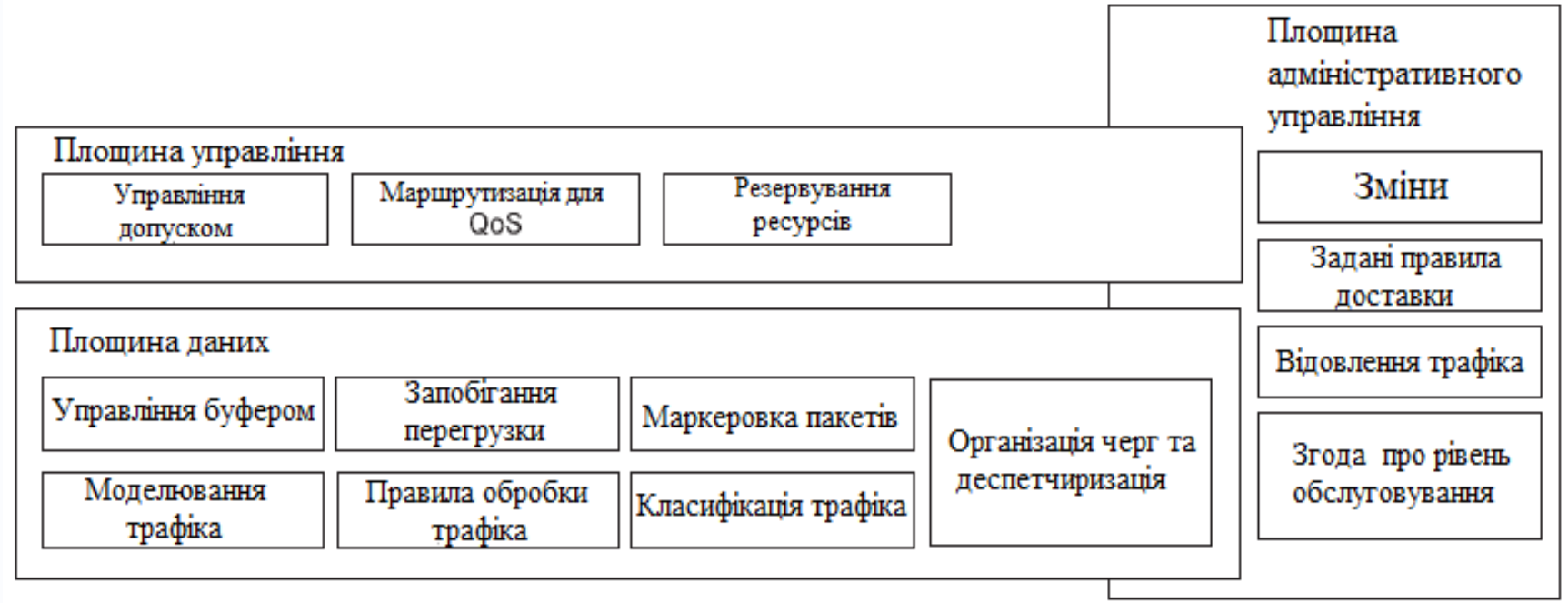
3. Досліджений метод виявлення порушника інформаційного захисту на відміну від існуючих методів дозволяє виявити активного порушника протоколів у використовуваних каналах зв'язку при відсутності загального довіреного центру або ключа між кореспондентами, а також автоматично виявити порушника, що володіє технологією синтезу голосу.

4. Розглянутий протокол захисту (ZRTP) характеризується зменшеними часовими витратами при роботі протоколу по каналах зв'язку з затримками і помилками.

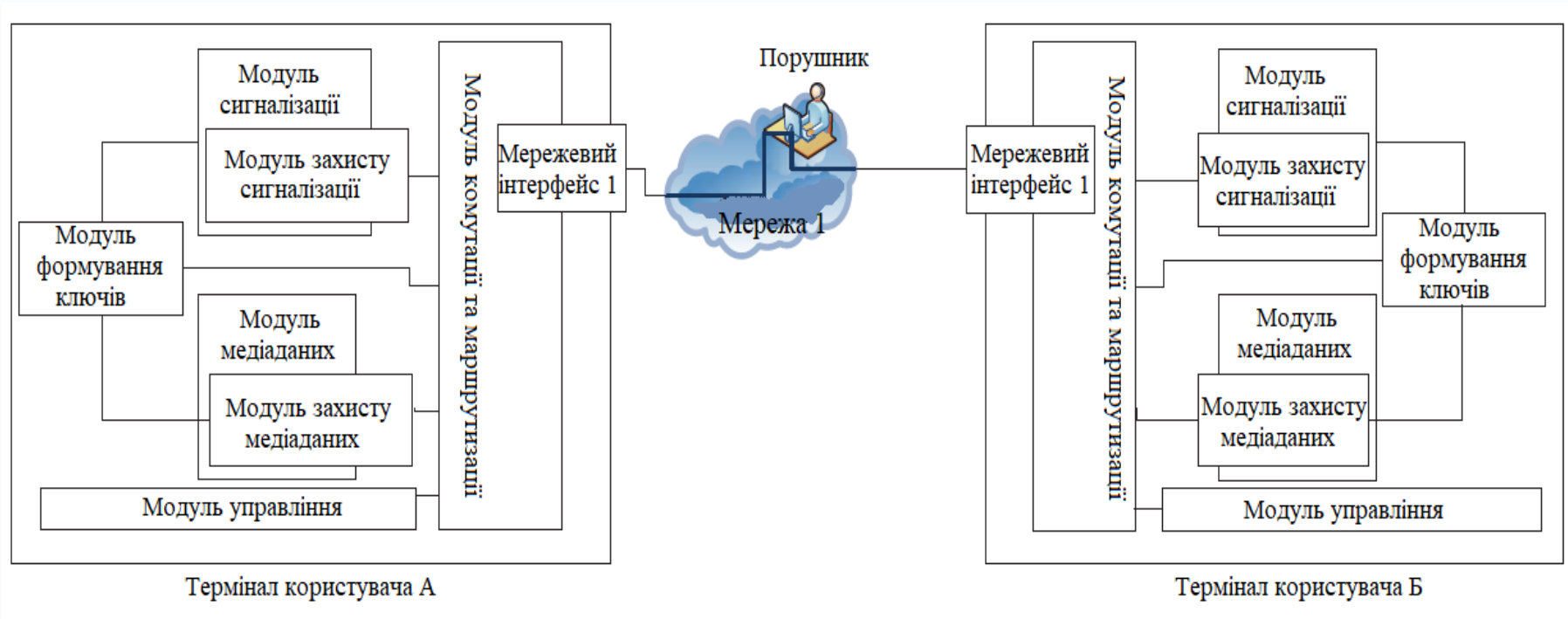
Принципова схема підключення оператора VoIP



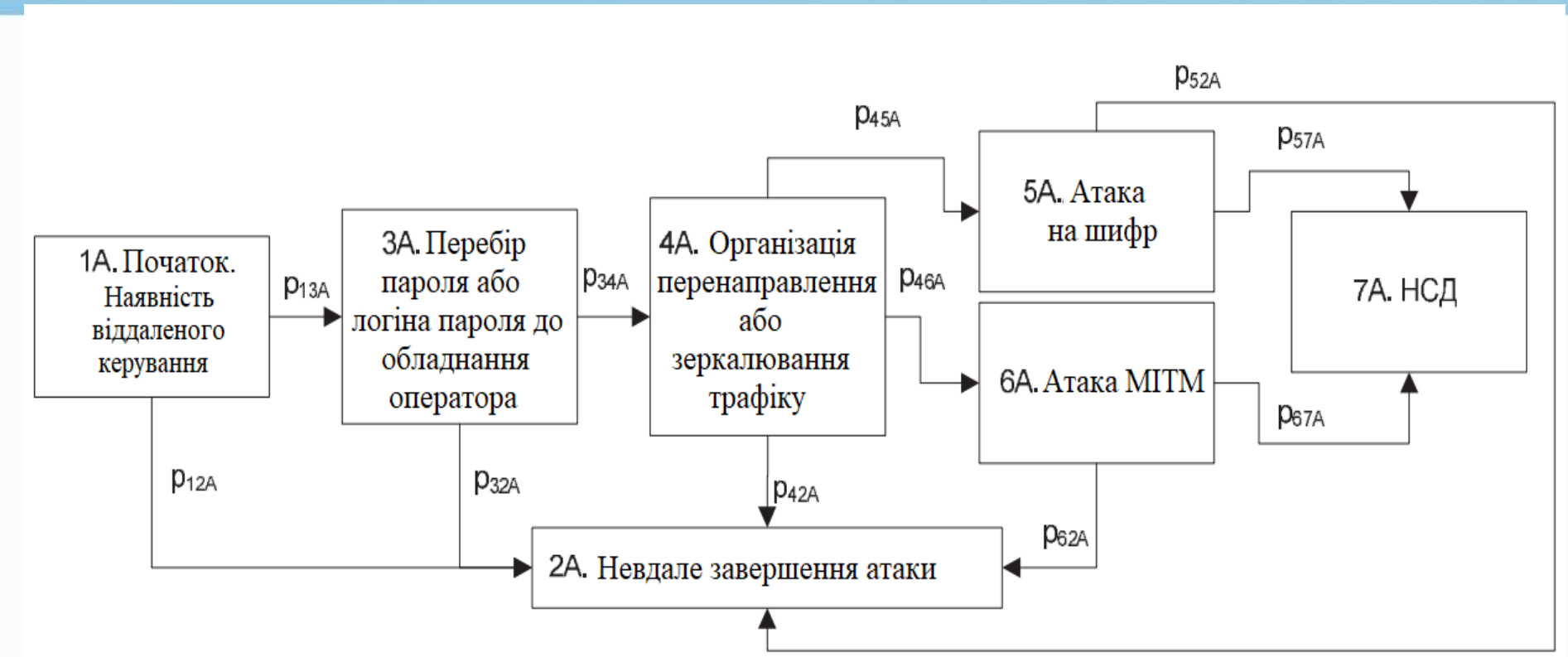
Архітектурна модель для підтримки QoS



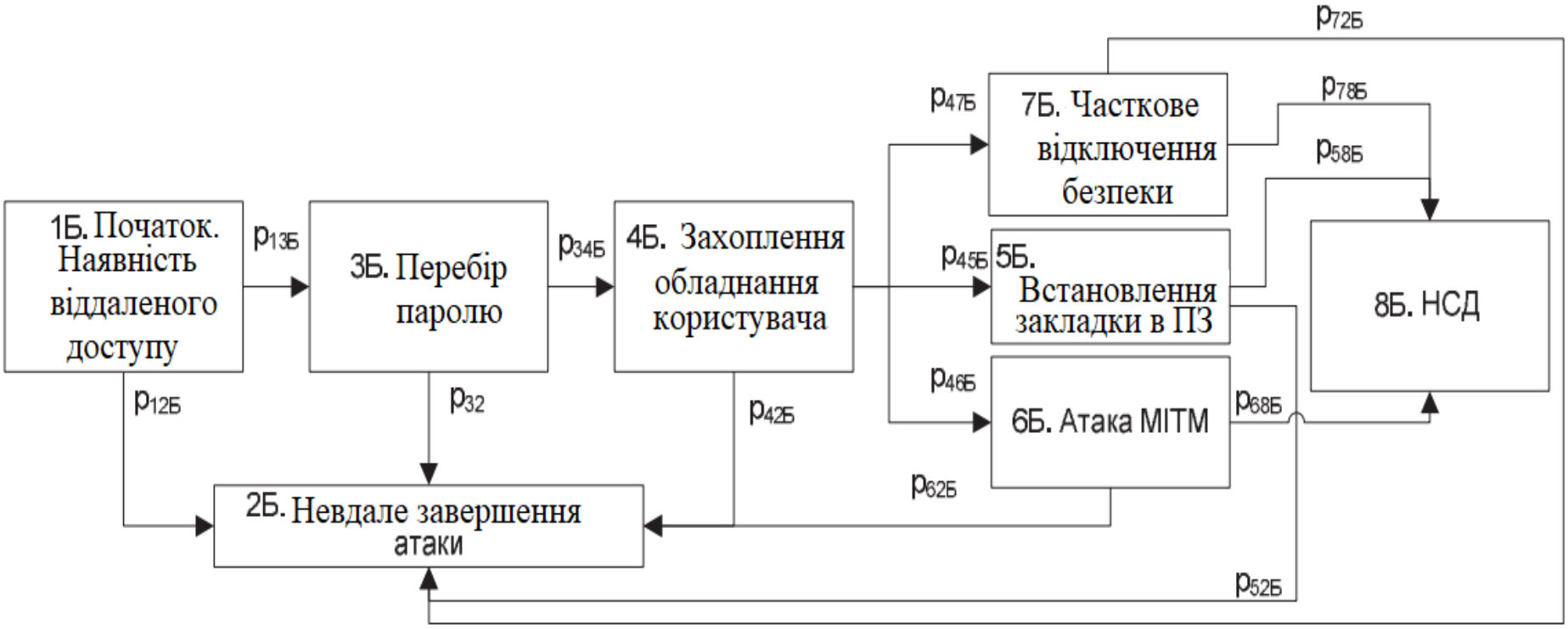
Структурна схема з'єднання в сценарії клієнт-клієнт



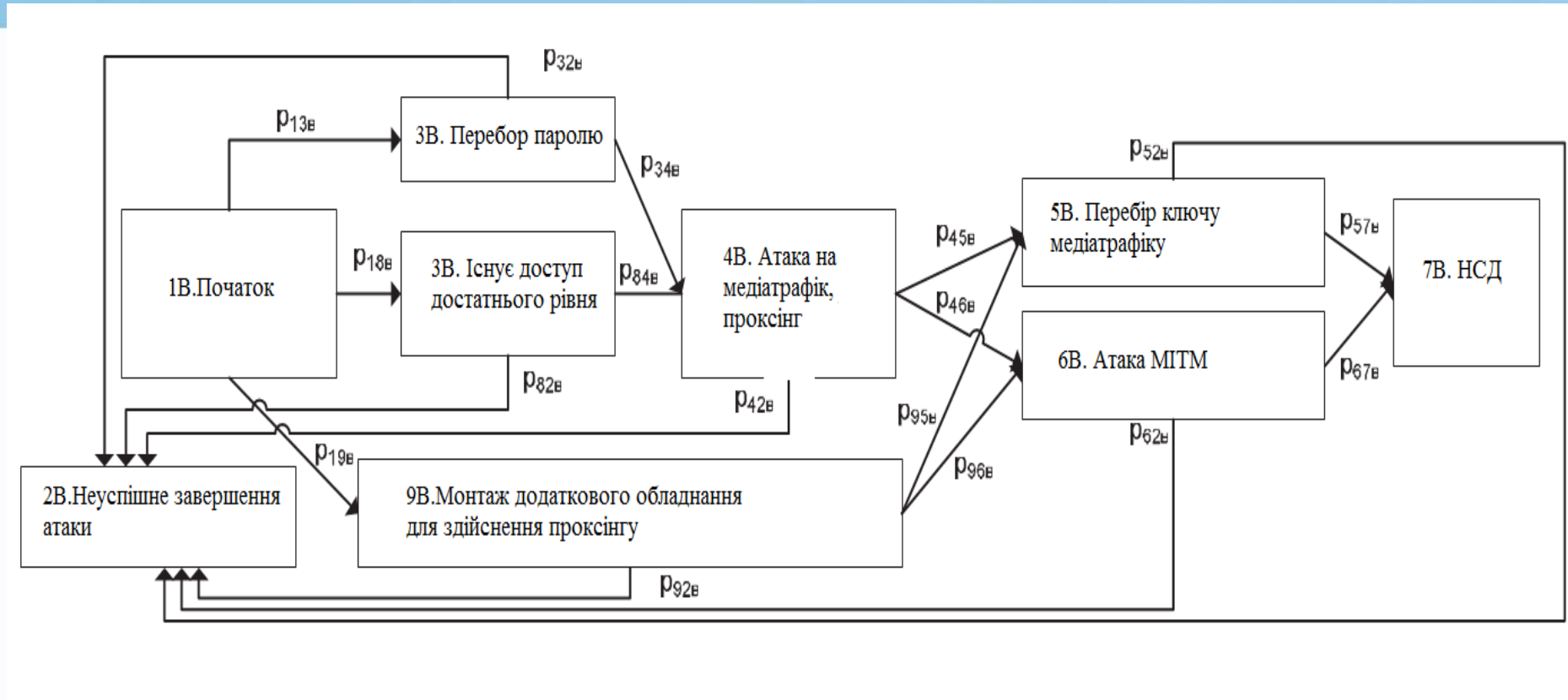
Алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником



Алгоритм дій при захопленні терміналу користувача зовнішнім порушником



Алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником



Алгоритм дій при виконанні захоплення терміналу користувача внутрішнім порушником

ВИСНОВКИ

У МКР вирішена актуальна науково-технічна задача підвищення рівня захищеності інформації в сеансах безпечної IP- телефонії та скорочення часу встановлення захищеного з'єднання за рахунок поліпшення ймовірнісно-часових характеристик протоколів, в тому числі отримані наступні основні результати:

Запропоновано математичну модель активного порушника для захищеної IP-телефонії, що враховує можливість цього порушника реалізувати атаку людина посередині на протокол розподілу ключів, яка дозволяє розрахувати ймовірність успішної атаки, націленої на несанкціонований доступ до інформації (НСД), в залежності від значень ймовірностей проміжних атак .

Запропоновано методику оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії, що враховує особливості протоколів, виражені в наявності обмеження числа повторних передач повідомлень і змінного таймера повторної передачі.

Досліджено метод виявлення порушника протоколів розподілу ключів, який застосовується при роботі за сценарієм клієнт-клієнт для кореспондентів, які не мають заздалегідь розподіленого ключового матеріалу. Метод дозволять з більш високою ймовірністю встановити захищене з'єднання між двома кореспондентами в порівнянні з існуючими методами, а також виявити наявність активного порушника в каналі зв'язку.

Дякую за увагу!