Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

МАТЕРІАЛИ

VI Міжнародної науково-практичної конференції

"ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ"

02 – 06 вересня 2020 року

Одеса 2020

УДК 004.056.5
П 26

Перспективні няпрями захисту інформації: матеріали шостої
П 26 міжнародної наук.-пр. конф. – м. Одеса, 02 – 06 вересня 2020 р. –
Одеса: Бондаренко М.О., 2020. – 120 с.

ISBN 978-617-7829-61-3

Даний збірник містить тези матеріалів, що представлені на шосту всеукраїнську науково-практичну конференцію "**Перспективні няпрями захисту інформації**", що проводиться 02 – 06 вересня 2020 р. в Одеській національній академії зв′язку ім. О.С. Попова.

У збірник включені тези доповідей за такими напрямками:

- організаційно-правові методи захисту інформації;
- захист критичної інформаційної інфраструктури держави;
- кібербезпека, протидія кібертероризму та кіберзлочинності;
- управління інцидентами інформаційної безпеки;
- технології захисту хмарних обчислень;
- постквантова криптографія;
- технічні засоби виявлення каналів витоку інформації;
- засоби захисту інформації в інформаційних і телекомунікаційних системах;
- елементи і компоненти для систем захисту інформації;
- телекомунікаційні системи та мережі.

Робочі мови конференції – українська, російська, англійська.

УДК 004.056.5

ISBN 978-617-7829-61-3

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Воробієнко П.П. голова, д.т.н., проф., ректор ОНАЗ ім. О.С. Попова;

Каптур В.А. заступник голови, к.т.н., с.н.с., проректор з наукової роботи ОНАЗ ім. О.С. Попова;

Василіу Є.В. д.т.н., проф., директор навчально-наукового інституту Кібербезпеки, комп'ютерних і радіо технологій ОНАЗ ім. О.С. Попова;

Гнатюк С.О. д.т.н., заступник декана ФККПІ з наукової роботи, Національний авіаційний університет;

Кільдішев В.Й. к.т.н., доц. каф. кібербезпеки та технічного захисту інформації, ОНАЗ ім. О.С. Попова;

Корченко О.Г. д.т.н., проф., зав. каф. безпеки інформаційних технологій, Національний авіаційний університет;

Корчинський В.В. д.т.н., зав. каф. кібербезпеки та технічного захисту інформації, ОНАЗ ім. О.С. Попова;

Лахно В.А. д.т.н., проф., зав. каф. комп'ютерних систем і мереж, Національний університет біоресурсів і природокористування України;

Онацький О.В. к.т.н., доц. каф. кібербезпеки та технічного захисту інформації, ОНАЗ ім. О.С. Попова;

Рудницький В.М. д.т.н., проф., зав. каф. системного програмування, Черкаський державний технологічний університет

Смірнов О.А. д.т.н., проф., зав. каф. кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Василіу Є.В. д.т.н., проф., директор навчально-наукового інституту кібербезпеки, комп'ютерних і радіо технологій, ОНАЗ ім. О.С. Попова;

Сідень С.В. відповід. за наукову роботу навчально-наукового інституту кібер-безпеки, комп'ютерних і радіо технологій, ОНАЗ ім. О.С. Попова;

Корчинський В.В. д.т.н., зав. каф. кібербезпеки та технічного захисту інформації, ОНАЗ ім. О.С. Попова;

Пилявський В.В. к.т.н., п.н.с. НДЦ ТКС та МЗ, ОНАЗ ім. О.С. Попова;

Стайкуца С.В. к.т.н., доц. каф. кібербезпеки та технічного захисту інформації, ОНАЗ ім. О.С. Попова;

Севастєєв Є.О. ст. викл. каф. кібербезпеки та технічного захисту інформації, ОНАЗ ім. О.С. Попова;

Рябуха О.М. к.т.н., викл. каф. кібербезпеки та технічного захисту інформації, ОНАЗ ім. О.С. Попова;

Буюклі Ю.Б. директор бази відпочинку «Електрон», ОНАЗ ім. О.С. Попова

ЗМІСТ

1	*Юдін О.Ю., Одарченко Р.С.* ДОСЛІДЖЕННЯ МОЖЛИВОСТІ РОЗГОРТАННЯ МЕРЕЖ УРЯДОВОГО РАДІОЗВ'ЯЗКУ НА БАЗІ КОНЦЕПЦІЇ МЕРЕЖ 5G	6
2	*Хлапонін Ю.І., Єліссаві К.К.* ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДВИЩЕННЯ СТАЛОСТІ МЕРЕЖЕВОЇ СИНХРОНІЗАЦІЇ В СУЧАСНІЙ МУЛЬТИСЕРВІСНІЙ МАКРОМЕРЕЖІ	9
3	*Баранник В.В.* ТЕХНОЛОГИЯ КОДИРОВАНИЯ БИНОМИАЛЬНО-ПОЗИЦИОННЫХ ЧИСЕЛ В СИСТЕМАХ ИНФОКОММУНИКАЦИЙ	12
4	*Баранник В.В., Бабенко Ю.М. Шульгинс.С.С., Баранник Н.В.* ТЕХНОЛОГИЯ КОДИРОВАНИЯ СЕГМЕНТОВ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ВИДЕОРЕСУРСОВ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ	14
5	*Баранник В.В., Сидченко С.А. Баранникв.Д.В., Баранникв.В.В.* ТЕХНОЛОГИЯ КОНФИДЕНЦИАЛЬНОЙ ЗАЩИТЫ ВИДЕОИНФОРМАЦИОННЫХ РЕСУРСОВ	17
6	*Бараннік Д.В.* ТЕХНОЛОГІЯ КОМПРЕСІЙНОГО КОДУВАННЯ З ІМПЛАНТАЦІЄЮ ПРИХОВУВАНИХ ПОВІДОМЛЕНЬ	20
7	*Мусієнко О.П., Коломієць В.Д., Химeнко В.В., Стеценко О.В* МЕТОД КЛАСТЕРНОГО АНАЛІЗУ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ ОБРОБКИ ВІДЕОІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ПОВІТРЯНИХ СИЛ	22
8	*Хаханова Г.В., Пархоменко М.В.* МЕТОД ЕФЕКТИВНОГО КОДУВАННЯ ВІДЕОІНФОРМАЦІЙНОГО РЕСУРСУ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ	25
9	*Жирова Т.О., Котенко Н.О.* ОСОБЛИВОСТІ АВТОМАТИЗАЦІЇ ТЕСТУВАННЯ БЕЗПЕКИ WEB-ДОДАТКІВ	27
10	*Мазулевський О.Є., Чевардін В.Є.* ПОГЛЯД НА РОЗВИТОК ОСВІТИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ	30
11	*Дика Т.В., Одарченко Р.С., Дика Н.В., Одарченко М.С.* МОЖЛИВІ СТРАТЕГІЇ ОПЕРАТОРІВ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ ПО ЗАПУСКУ 5G В УКРАЇНІ	34
12	Фауре Е.В., Щерба А.І., Лавданський А.О., Тинимбаєв С.Т., Байкенов А.С. МЕХАНІЗМ УЗГОДЖЕННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ НА ОСНОВІ ПЕРЕСТАНОВОК У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ З БАГАТЬМА КОРИСТУВАЧАМИ	38
13	*Одарченко Р.С., Даков С.Ю., Дакова Л.В. Федюра Т.В.* СИСТЕМА МОНІТОРИНГУ КІБЕРАТАК БЕЗДРОТОВИХ МЕРЕЖ 5G НА БАЗІ ТЕХНОЛОГІЇ SCOM	42
14	*Шестак Я.В., Мирутенко Л.В., Толюпа С.В.* КОНЦЕПЦІЯ РОЗРОБКИ МЕТОДИКИ ОЦІНКИ ЗАХИЩЕНОСТІ СКЛАДНИХ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ	46
15	*Асаёнок М. А.* ИЗМЕРИТЕЛЬ ИНТЕНСИВНОСТИ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ КРЕМНИЕВОГО ФОТОЭЛЕКТРОННОГО УМНОЖИТЕЛЯ	48
16	*Зубок В.Ю.* ЗАСТОСУВАННЯ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ ДО ПРОТИДІЇ АТАКАМ НА ГЛОБАЛЬНУ МАРШРУТИЗАЦІЮ В ІНТЕРНЕТІ	50
17	*Миронюк М.В., Онацький О.В.* ДОСЛІДЖЕННЯ СИМЕТРИЧНОГО ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ І ОБМІНУ КЛЮЧАМИ ОТВЕЯ-РІССА	54
18	*Смірнова Т.В., Щербань А.В., Моторін Ю.Ю., Смірнов О.А* ПЕРСПЕКТИВНІ НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СЕРВІСУ CAEaaS	58

19	*Гізун А. І., Гріга В. С.* МОДЕЛЬ ІНФОРМАЦІЙНОГО ВПЛИВУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ВИБОРЧИЙ ПРОЦЕС В УКРАЇНІ В 2019 РОЦІ	60
20	*Корчинський В.В., Аль-Файюми Халед, Копитін Ю.В., Копитіна М.В., Валигурський Ю.П.* ПРОГНОЗУВАННЯ ТА ОЦІНКИ РИЗИКІВ ІНСАЙДЕРСЬКИХ ЗАГРОЗ	64
21	*Корчинський В.В., Рябуха О. М., Бердніков О.М., Поліщук К.В.* МЕТОД РОЗШИРЕННЯ СПЕКТРА НА ОСНОВІ ТАЙМЕРНИХ СИГНАЛІВ І ЛІНІЙНОЇ ЧАСТОТНОЇ МОДУЛЯЦІЇ	66
22	*Кононович В.Г., Стайкуца С.В. , Кононович І.В., Романюков М.Г.* КОНТУРИ СИСТЕМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЦИФРОВІЗОВАНОГО СУСПІЛЬСТВА ТА КІБЕРНЕТИЗОВАНОГО ВИРОБНИЦТВА, БІЗНЕСУ Й УПРАВЛІННЯ	70
23	*Катаєв В.С.* ЗАХИСТ ІНФОРМАЦІЇ ВІД ПЕРЕХОПЛЕННЯ ЛАЗЕРНИМИ МІКРОФОНАМИ	76
24	*Сінюгін В. В., Яремчук Ю.Є.* ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ ОПТИКО-ЕЛЕКТРОННИМ ТА ЕЛЕКТРОМАГНІТНИМ КАНАЛАМИ	79
25	*Салієва О. В.* ВИЗНАЧЕННЯ ВИТРАТ НА ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ РАНЖУВАННЯМ ЗАГРОЗ	83
26	*Приймак А.В., Яремчук Я.Ю.* МЕТОД ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО МАЙНІНГУ КРИПТОВАЛЮТИ НА ОСНОВІ ВИЯВЛЕННЯ ПІДОЗРІЛИХ ПРОЦЕСІВ В КОНТЕЙНЕРАХ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ	85
27	А.М. Бігдан, Т.В. Бабенко ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗГІДНО МОДЕЛІ АДАПТИВНОЇ АРХІТЕКТУРИ БЕЗПЕКИ	87
28	*Теліженко О.Б.* АЛГОРИТМ ВИПАДКОВОГО ПОШУКУ РОЗВ'ЯЗКУ ЗАДАЧІ ДИСКРЕТНОГО ЛОГАРИФМУВАННЯ (*DLP*) У СКІНЧЕННИХ ПРОСТИХ ПОЛЯХ	89
29	*А. О. Фесенко, Д. В. Щутенко* ЗАХОДИ, ЩО ПРОВОДЯТЬСЯ ДЛЯ ЗАХИСТУ ВІД ЗАСТОСУВАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, ЗОКРЕМА ФІШИНГУ	91
30	*Руденко А. М.* ТЕХНОЛОГІЇ DEEPFAKE. ПОТЕНЦІЙНА ЗАГРОЗА ДЛЯ СУСПІЛЬСТВА ТА ПОЗИТИВНІ АСПЕКТИ ТЕХНОЛОГІЇ	95
31	*Kodenets V.P., Onatskiy A.V.* CRYPTOGRAPHIC AUTHENTICATION PROTOCOL ZERO-KNOWLEDGE SECRET ON ELLIPTIC CURVES	98
32	*Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Лукашенко В.В., Галенко В.В.* ВИЗНАЧЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ АВІАЦІЙНОЇ ГАЛУЗІ	101
33	*Вакарчук А. А., Васильев Л. С.* ЭФФЕКТИВНОСТЬ РАСПРОСТРАНЕНИЯ СИГНАЛА ОТ АНТЕННЫ СЕТИ 4G	104
34	*Вакарчук А.О., Федоренко А.Ю., Недайвода П.П.* ОЦІНКА ВТРАТ ПРИ РОЗПОВСЮДЖЕННІ РАДІОХВИЛЬ В УМОВАХ МІСТА	108
35	*Дорожинський С.А., Охріменко Т.О.* АНАЛІТИЧНИЙ ОГЛЯД ПРОТОКОЛІВ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ НА ОСНОВІ ПОЛЯРИЗАЦІЙНОГО КОДУВАННЯ	112
36	*Skuratovskii Ruslan, Williams Aled, Osadhyy Volodymyr* AN ESTIMATION OF A KEY SPACE SIZE IN KEY EXCHANGE PROTOCOL BASED ON METACYCLIC *P*-GROUP	115
37	*Плескач Б.М.* КОНТРОЛЬ ТА ЗАХИСТ КОНСОЛІДОВАНОЇ ІНФОРМАЦІЇ ПРИ МОНІТОРИНГУ ЕНЕРГЕТИЧНИХ ВТРАТ В ТЕХНОЛОГІЧНИХ СИСТЕМАХ	119
38	*Козловський В.В., Лазаренко С.В., Мартинюк Г.В., Баланюк Ю.В.* ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАГУВАННЯ НА СОЦІОТЕХНІЧНІ АТАКИ	122
39	*Васьковська А.О.* ІНФОРМАЦІЙНА ВІЙНА, ЯК ФОРМА ВЕДЕННЯ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА	125

Катаєв В.С.

ЗАХИСТ ІНФОРМАЦІЇ ВІД ПЕРЕХОПЛЕННЯ ЛАЗЕРНИМИ МІКРОФОНАМИ

Вінницький національний технічний університет
kataev@vntu.net

Анотація. Сучасний розвиток шпигунських пристроїв дозволяє зловмиснику підслуховувати розмови, що ведуться у приміщенні, взагалі без необхідності проникнення всередину і, навіть, знаходячись на значній відстані. Пристрої, що дозволяють це робити, – лазерні мікрофони або лазерні системи акустичної розвідки. Існують декілька поширених методів захисту від такого типу загроз, однак усі вони мають свої недоліки. У даному дослідженні запропоновано метод лазерної протидії, як альтернатива існуючим, та наведено концепцію його реалізації. Даний метод ґрунтується на процесі «перемішування» зондуючого лазерного променю зловмисника із протидіючим випромінюванням, що значно ускладнить процес приймання та виділення інформативного сигналу на приймальній стороні ЛСАР.

Ключові слова: технічний захист інформації, методи активного захисту, лазерні системи акустичної розвідки, лазерні мікрофони, засоби захисту акустичної інформації.

Одним з актуальних каналів витоку мовної інформації на сьогодні є оптико-електронний технічний канал, перехоплення інформації через нього реалізується за допомогою лазерних систем акустичної розвідки (ЛСАР) або лазерних мікрофонів [1]. Головною перевагою ЛСАР над іншими засобами розвідки є те, що вони дозволяють вирішувати задачі знімання мовної інформації максимально безпечно для зловмисника, оскільки виключається необхідність проникнення у приміщення з метою розміщення там закладних пристроїв і т.п. ЛСАР у спрощеному вигляді складається з лазерного випромінювача в інфрачервоному діапазоні та оптичного приймача. Принцип роботи цих пристроїв наступний: лазерний випромінювач, за допомогою оптичного прицілу, направляється на плоску вібруючу поверхню (найкращим прикладом такої поверхні є шибка вікна), далі генерується лазерний промінь (високочастотний сигнал), що поширюється через атмосферу і падає на цю поверхню. Після він відбивається від віконного скла і при цьому модулюється за законом акустичного сигналу, який також впливає на скло, повторно долає атмосферу в зворотному напрямку і приймається фотоприймачем, що відновлює інформаційний сигнал.

Для захисту від такого типу загроз існують різні методи та засоби захисту, як активні, так і пасивні, але усі вони мають ряд недоліків: вони або не дозволяють забезпечити достатню захищеність, або потребують значних фінансових витрат, або значно погіршують комфортність роботи у приміщенні. Більш того, наведені недоліки нероздільно пов’язані один з одним. Це пояснюється тим, що більшість методів не здатні забезпечити необхідну захищеність по одинці. Тому вони використовуються у комплексі і це спричиняє ситуацію, коли усунення одного недоліку спричиняє ще більше погіршення іншого.

Розглянемо існуючі методи захисту від ЛСАР. Найпростішим прикладом є забезпечення звуко- та віброізоляції вікон приміщення, з яких може зніматися акустична інформація [1]. Це дозволить усунути або значно зменшити небезпечні інформативні вібрації на зовнішніх поверхнях вікон. Але реалізація такого способу вимагатиме значних фінансових витрат, пов’язаних не тільки з виготовленням та закупівлею спеціальних вікон, а й з проведенням значного обсягу будівельних робіт. Як, альтернативу, можна використати захисні та тонуючі плівки [2], які клеяться на віконне скло. Вони, теоретично, теж можуть знизити рівень вібрації скла і, відповідно, ускладнити виділення звукового сигналу у прийнятому лазерному випромінюванні. Недоліком такого захисту є те, що знімання інформації ускладнюються лише зменшенням коефіцієнту модуляції відбитого променя, що для сучасних ЛСАР не є значною проблемою.

Активний захист від ЛСАР реалізується за допомогою генераторів шуму, які створюють шумоподібні електричні сигнали у мовному частотному діапазоні, і ці сигнали передаються на поверхню за допомогою п'єзоелектричних і електромагнітних вібраторів [3]. Дані перетворювачі встановлюються на усіх проблемних поверхнях, з яких можливе знімання інформаційних вібрацій. Але і такий захист має недоліки, проблема полягає у тому, що у деяких випадках кількість таких віброперетворювачів може бути досить великою, адже на кожну шибку вікна необхідно встановити мінімум один датчик. І в результаті загальний рівень акустичних завад буде настільки високий, що у приміщенні створяться некомфортні умови для розмов.

Слід звернути увагу ще на один важливий недолік наведених методів захисту - це не здатність забезпечення повної захищеності інформації. Він полягає у тому, що лазерний промінь при потраплянні на вікно частково відбивається, але й частково проходить крізь нього, оскільки скло є оптично прозорим матеріалом. Спрощено це означає, що інформаційну вібрацію можна зчитати не тільки з поверхні вікна, але й з будь-якої іншої поверхні, що знаходиться за вікном всередині приміщення (наприклад дзеркало на стіні). Таким чином, для захисту інформації необхідно ще додатково вирішувати питання потрапляння лазеру всередину приміщення. Зробити це можна встановленням на вікні оптично непрозорої конструкції, яка буде закривати інтер'єр, але слід пам'ятати, що, якщо таку конструкцію розмістити всередині приміщення, то і на ній самій може бути присутня небезпечна вібрація. Такий захист можна реалізувати за допомогою спеціальних електрохромних плівок або електрохромного скла [4]. У спрощеному вигляді принцип їх роботи можна описати так: при подачі напруги на скло активний полімерний шар, розташований усередині триплексу, набуває забарвлення певного відтінку, тим самим зменшуючи прозорість, а при відключенні напруги скло повертається у початковий стан. Таким чином, можна знизити пропускаючі, відбиваючі та поляризаційні властивості віконного скла, тим самим значно ускладнивши можливість зняття інформації з внутрішніх поверхонь приміщення. Недоліками такого способу є енергозалежність цих конструкцій, оскільки вони потребуватимуть постійної подачі напруги та висока вартість таких плівок і скла.

Викладене вище свідчить про таку проблему: навіть, якщо на вікні створюється вібраційна завада, то, налаштувавшись на промінь відбитий з внутрішньої поверхні, зловмисник все одно зможе слухати розмову. Для захисту від такої загрози необхідно унеможливити появу відбитого з середини приміщення променю. Для цього можна використати зазначені вище спеціалізовані плівки, які будуть значно відхиляти та послаблювати лазерний промінь. Але це, зрозуміло, призведе до неприйнятного здороження системи, адже активний захист при цьому теж лишається, тому на практиці такі системи не використовуються. Тому, на сьогодні оптимальним варіантом системи захисту від ЛСАР, як з точки зору забезпечення захищеності, так і з точки зору фінансових затрат, є встановлення на вікнах приміщення активного захисту, а ззовні вікон встановлення оптично непрозорих металевих ролет, які під час озвучення інформації будуть повністю закривати вікна, а також, відповідно, внутрішній інтер'єр приміщення. У результаті, ми маємо ситуацію, коли, вирішуючи питання забезпечення захищеності інформації і зменшення вартості системи, ми не вирішуємо питання комфортності роботи у приміщенні, а навпаки погіршуємо її, оскільки до шумів, що створюють засоби активного захисту, додається ще й той факт, що працювати у приміщенні необхідно при повністю закритих ролетами вікнах.

Для вирішення усіх викладених недоліків пропонується принципово інший підхід та метод до побудови захисту [5]. Проблему потрапляння лазера у середину приміщення пропонується вирішувати не шляхом усунення самої можливості проникнення променя, а шляхом унеможливлення або значного ускладнення перехоплення зловмисником вже відбитого променя. Реалізувати це можна за допомогою створення протидіючого лазерного випромінювання, яке буде направлено зсередини приміщення через вікно назовні. Реалізувати це можна за допомогою створення протидіючого завадового лазерного випромінювання, яке буде направлено з середини приміщення через вікно на зовні. При цьому дане випромінювання буде складатись із множини променів, напрям яких може змінюватись у просторі випадковим чином і, які будуть мати параметри (зокрема, спектральні, енергетичні і/або просторово-енергетичні параметри) подібні до параметрів зондувального променю зловмисника. Також, протидіюче випромінювання повинно

мати широку діаграму направленості, достатню, щоб перекрити усі можливі кути відбиття лазеру зловмисника. Окрім цього, протидіючі промені повинні бути промодульовані шумовими або хибними сигналами, реалізуючи при цьому шумову або мовоподібну заваду. В результаті ми отримаємо ситуацію, при якій відбитий промінь зловмисника на виході буде «змішуватись» із протидіючими завадовими променями, що значно ускладнить його перехоплення та виділення на приймальній стороні ЛСАР. Також, оскільки промені будуть проходити через скло і поширюватись назовні, то ми вирішуємо питання захисту не тільки від зняття вібрації всередині приміщення, а й з поверхні вікна. Тобто, теоретично даний метод дозволить забезпечити захищеність інформації без застосування вібраційного зашумлення та використання різних оптично непрозорих загороджувальних конструкцій по типу металевих ролет. Засіб, що буде реалізовувати даний метод, повинен розташовуватись із врахуванням можливостей лазерних мікрофонів.

Висновки

У результаті аналізу існуючих методів захисту акустичної інформації від зняття лазерними системами акустичної розвідки, можна зробити висновок, що усі вони мають ряд недоліків. У зв'язку з цим було запропоновано метод, який полягає у тому, що всередині приміщення створюється завада у вигляді маскуючого лазерного випромінювання, яке складається із множини променів з параметрами, подібними до параметрів можливого зондувального променю зловмисника, і направлені зсередини приміщення через вікно назовні таким чином, що відбитий від вібруючої поверхні промінь зловмисника на виході з приміщення маскується змішуванням із завадовими протидіючими променями, ускладнюючи зловмиснику виділення його променю з множини маскуючих завадових променів.

Результати досліджень показали, що застосування розробленого методу при побудові систем захисту мовної інформації дозволить покращити зручність та комфортність роботи у приміщенні та зменшити матеріально-фінансові витрати при забезпеченні необхідної захищеності інформації, оскільки відпадає необхідність встановлення спеціальних віброперетворювачів та додаткових оптично не прозорих конструкцій на вікнах приміщення.

Література

1. Каторин Ю. Ф. Большая энциклопедия промышленного шпионажа / Ю. Ф. Каторин, Е. В. Куренков, А. В. Лысов, А. Н. Остапенко. – СПб. : ООО "Издательство Полигон", 2000. – С. 734.
2. Принципи зняття звукової інформації зі скла і її захист [Електронний ресурс]. Режим доступу: http://ua.nauchebe.net/2012/09/principi-znyattya-zvukovo%D1%97-informaci%D1%97-zi-skla-i-%D1%97%D1%97-zaxist/
3. Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. – К.: Юниор, 2003. – 504с.
4. Glass-shield | Стекло для защиты от прослушивания помещений с помощью направленного лазерного луча [Електронний ресурс]. Режим доступу: http://www.zoohall.com.ua/2541-glass-shield-steklo-proslushivanie.html
5. Катаєв В.С., Яремчук Ю.Є. Спосіб створення активної завади для протидії несанкціонованому зняттю інформації через лазерні системи акустичної розвідки // Патент України на корисну модель, № 137710; заявл. 21.03.2019; Опубл. 11.11.2019, Бюл. №21.