Львівський державний університет
безпеки життєдіяльності

Національний університет
"Львівська політехніка"

Akademia Techniczno-Humanistyczna,
Bielsko-Biała (Polska)

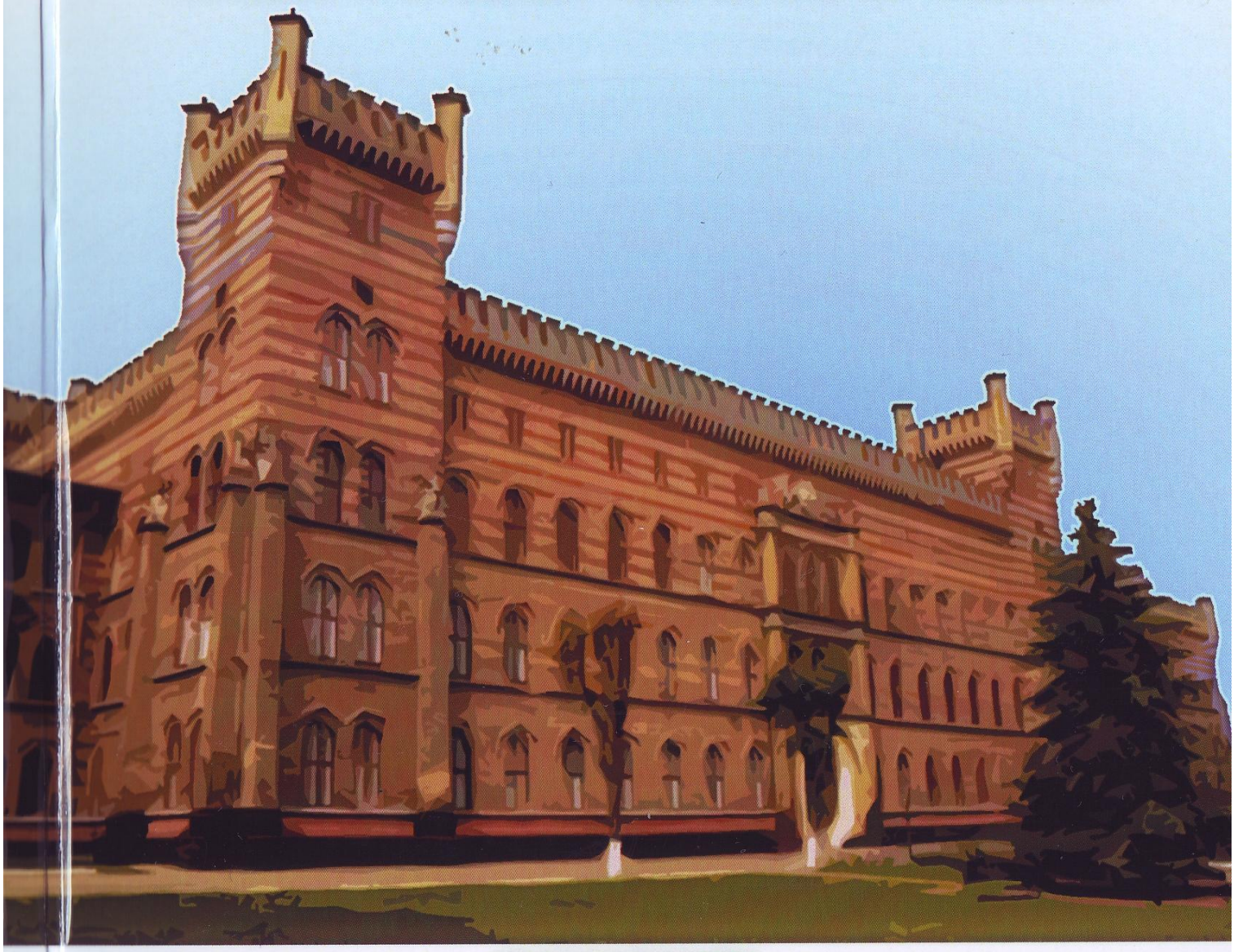
Державна служба України
з надзвичайних ситуацій

Національний технічний університет
"Київський політехнічний інститут"

Politechnika Krakowska (Polska)

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ СУСПІЛЬСТВІ

Матеріали II Міжнародної науково-технічної конференції



24-25 листопада 2016
Львів, Україна

Державна служба України з надзвичайних ситуацій

Львівський державний університет безпеки життєдіяльності

Національний університет "Львівська політехніка"

Politechnika Krakowska (Polska)

Національний технічний університет "Київський політехнічний інститут"

Akademia Techniczno-Humanistyczna, Bielsko-Biała (Polska)

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ СУСПІЛЬСТВІ

ТЕЗИ ДОПОВІДЕЙ

ІІ-ої Міжнародної науково-технічної конференції

24-25 листопада 2016 р.

Організатори конференції:

Львівський державний університет безпеки життєдіяльності

Національний університет "Львівська політехніка"

Politechnika Krakowska (Polska)

Національний технічний університет "Київський політехнічний інститут"

Akademia Techniczno-Humanistyczna, Bielsko-Biała (Polska)

У збірнику опубліковано матеріали конференції, присвячені проблемам інформаційної безпеки в сучасному суспільстві, зокрема управлінню інформаційною безпекою, безпеці інформаційно-комунікаційних систем, технічному захисту інформації.

Поштова адреса оргкомітету:
м. Львів, 79000, вул. Клепарівська, 35, кафедра управління інформаційною безпекою, кім. № 415

Відповідальний за випуск – професор Самотий В. В.

Комп'ютерне макетування та верстка – доцент Лагун А. Е.

Матеріали подано у авторській редакції

ПРОГРАМНИЙ КОМІТЕТ

ГОЛОВА

Козяр М.М. – ректор Львівського державного університету безпеки життєдіяльності, доктор педагогічних наук, професор, Член-кореспондент НАПН України, Заслужений працівник освіти України, генерал-лейтенант служби цивільного захисту

ЗАСТУПНИК ГОЛОВИ

Самотий В. В. – завідувач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, д.т.н., професор

ЧЛЕНИ ПРОГРАМНОГО КОМІТЕТУ

Бурячок В.Л. – завідувач кафедри безпеки інформаційних технологій Державного університету телекомунікацій, доктор технічних наук, професор

Горбенко І.Д. – професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, доктор технічних наук, професор

Грицюк Ю.І. – професор кафедри програмного забезпечення, НУ "Львівська політехніка", доктор технічних наук, професор

Дудикевич В.Б. – завідувач кафедри захисту інформації НУ "Львівська політехніка", доктор технічних наук, професор

Корченко О.Г. – завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, доктор технічних наук, професор

Кузнецов О.О. – професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В. Н. Каразіна, доктор технічних наук, професор

Максимович В.М. – завідувач кафедри безпеки інформаційних технологій НУ "Львівська політехніка", доктор технічних наук, професор

Мачуський Є.А. – завідувач кафедри фізико-технічних засобів захисту інформації Національного технічного університету України "Київський політехнічний інститут", доктор технічних наук, професор

Мельник А.О. – завідувач кафедри електронних обчислювальних машин НУ "Львівська політехніка", доктор технічних наук, професор

Мороз Л.В. – професор. кафедри безпеки інформаційних технологій НУ "Львівська політехніка", доктор технічних наук, доцент

Пархуць Л.Т. – професор кафедри захисту інформації НУ "Львівська політехніка", доктор технічних наук, професор

Рак Т. Є. – проректор з науково-дослідної роботи Львівського державного університету безпеки життєдіяльності, доктор технічних наук, доцент, полковник служби цивільного захисту

Ренкас А.Г. – начальник інституту цивільного захисту Львівського державного університету безпеки життєдіяльності, кандидат технічних, доцент

Саченко А.О. – завідувач кафедри інформаційно-обчислювальних систем і управління Тернопільського Національного економічного університету, доктор технічних наук, професор

Хорошко В.О. – професор кафедри безпеки інформаційних технологій Національного авіаційного університету, доктор технічних наук, професор

Шевчук В.О. – завідувач кафедри міжнародних економічних відносин Львівської комерційної академії, доктор економічних наук, професор

Яремчук Ю.Є. – директор Центру інформаційних технологій і захисту інформації Вінницького Національного технічного університету, доктор технічних наук, професор

Karpiński M. – prof. ATH, Katedra Matematyki i Informatyki, dr hab. inż., Akademia Techniczno-Humanistyczna, Bielsko-Biała (Polska)

Khoma V. – prof. PO, Katedra Systemow Sterowania i Systemow Decyzyjnych, dr hab. inż., Politechnika Opolska (Polska)

Kirenko I. – Phd, Project Leader at Philips Research (Nederland)

Kovela S. - PhD MBA PGCE CITP Senior Lecturer Accounting, Finance and Informatics, Kingston University London (United Kingdom)

Petrov O. – prof. AGH, Katedra Informatyki Stosowanej, dr hab. inż., Akademia Gorniczo-Hutnicza im. Stanisława Staszica, Kraków (Polska)

Shakya S. – Professor and Asst. Dean at Institute of Engineering, Tribhuvan University (Nepal)

Yurish S. – Professor, Technical University of Catalonia (UPC, Barcelona, Spain)

Zając M. – prof. nadzw. PK, Katedra Informatyki i Technik Informacyjnych, dr hab. inż., Politechnika Krakowska (Polska)

ГОЛОВА ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

Лагун А. Е. – заступник завідувача кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук, доцент

ЗАСТУПНИК ГОЛОВИ ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

Кухарська Н. П. – доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат фізико-математичних наук, доцент

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Гриник Р. О. – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, старший лейтенант служби цивільного захисту

Дзелендзяк У. Ю. – доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук, доцент

Мандрона М. М. – старший викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук

Полотай О. І. – старший викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук

Процько І.О. – доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, кандидат технічних наук

ЗМІСТ

ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЛОКАЛІЗАЦІЇ ЗАКЛАДНИХ ПРИСТРОЇВ ПРИ ЗАСТОСУВАННІ НЕЛІНІЙНОЇ ЛОКАЦІЇ

Віталій Катаєв

Вінницький національний технічний університет, м. Вінниця, Україна

Experimentally investigated the problem of localization of eavesdropping devices which located in shielded enclosures when using nonlinear locator. Results show that the using of same types of radiostable fabrics as shielding materials, can greatly complicate the detection of eavesdropping devices.

Keywords: information protect, bug devices, radio opaque fabrics

Велику частину загроз для інформації становлять закладні пристрої або апаратні закладки. Найчастіше закладки слугують для перехоплення акустичної (мовної) та видової інформації, для цього можуть використовуватись портативні диктофони, провідні та радіо мікрофони та мініатюрні відеокамери і т.д. Виявлення закладних пристроїв зазвичай здійснюється з допомогою спеціальної пошукової апаратури. Причому цей спосіб повинен враховувати всі технічні характеристики та особливості роботи закладок, адже від принципу їх роботи буде залежати і метод, яким можна буде їх виявити [1].

Найбільш проблемними з точки зору виявлення являються портативні диктофони, адже дані пристрої під час своєї роботи не випромінюють ніяких сигналів, не підключаються до провідних ліній та працюють автономно. Тому виявити їх можна лише небагатьма пошуковими пристроями, такими як тепловізори та нелінійні локатори, при чому кожен з цих пристроїв мають свої недоліки. Наприклад, при використанні тепловізорів виникають значні обмеження, оскільки ступінь нагрівання об'єкта в якому знаходиться закладка залежить від багатьох факторів. Тому можливі випадки, коли локалізація закладного пристрою з допомогою тепловізора буде ускладнена або навіть неможлива [2]. Нелінійні локатори також мають свої проблеми - це і випадкові спрацювання на матеріали, які не є напівпровідниками, і неможливість виявлення закладок схованих у офісній та іншій техніці. Окрім цього, використання даних локаторів також може ускладнюватись і у випадку, якщо закладний пристрій має корпус виготовлений із екрануючих матеріалів, адже, це напряму буде впливати на сам принцип локалізації. Тому виникає необхідність дослідження даної проблеми більш детально.

В доповіді описані лабораторні виміри, які було проведено при розташуванні нелінійного елемента, який виступає у ролі складової апаратної закладки, у корпусах виконаних із різних типів екрануючих матеріалів в якості яких було використано радіонепрозорі тканини вітчизняного виробництва типу М1, М2, М3 та Н1, Н2, Н3. В якості нелінійного елемента використовувався напівпровідниковий діод, який розміщувався у діелектричному корпусі, що почергово огортався кожним із типів тканин. На відстані 0,15 м від корпусу розміщувався нелінійний локатор NR-μ. Локатор NR-μ являється індикаторним пристроєм і виявлення напівпровідникових матеріалів супроводжується загоранням лінійки світлодіодів, що знаходяться на корпусі пристрою. Тому при дослідженні впливу екрануючих матеріалів на процес локалізації нелінійних елементів, у якості вихідних даних будемо використовувати зображення індикаторних світлодіодів.

На рис. 1 представлені зображення індикаторної лінійки локатора при розміщенні напівпровідникового діоду у екранованих корпусах різних типів. Для аналізу впливу екрануючих матеріалів на можливість локалізації закладних пристроїв, будемо визначати кількість світлодіодів що світиться, тим самим ми визначимо, як змінюється ступінь впливу напівпровідникових елементів на поле локатора в якому вони знаходяться.

Як видно з рис. 1а при розташуванні діоду безпосередньо у полі локатора, засвічується шість індикаторних світлодіоди, тому вважатимемо це контрольним значенням відносно якого можна буде спостерігати вплив екрануючих матеріалів.

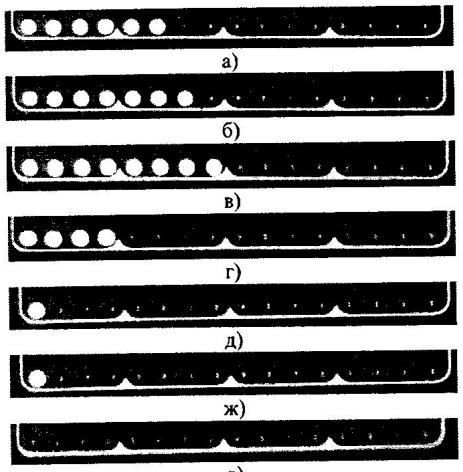


Рис. 1. Покази індикаторної лінійки локатора при розташуванні напівпровідникового діоду безпосередньо перед пристроєм а), у корпусі з тканини М1 б), у корпусі з тканини М2 в), у корпусі з тканини М3 г), у корпусі з тканини Н1 д), у корпусі з тканини Н2 ж) та у корпусі з тканини Н3 з)

При розміщенні напівпровідникового елементу у корпусах із тканин типу М ми спостерігаємо наступні результати, тканини М1 та М2 (рис.1 б,в) замість того, щоб зменшити вплив діода на поле локатора, навпаки його збільшують, і на пристрої засвідчується сім та вісім світлодіоди відповідно. Такий ефект можна пояснити недосконалістю установки, що використовується в дослідженні, а саме тим, що напівпровідниковий елемент розміщується в прямокутному корпусі, який обгортається екрануючою тканиною, і стінки корпуса в сумі з тканиною виконують роль спрямовуючої антени, а зміна діаграми направленості спричиняє зростання рівня сигналу. У випадку тканини М3 (рис.1 г) спостерігається зменшення впливу, про що сигналізують чотири світлодіоди. При розміщенні досліджуваного діода у корпусах із тканин типу Н ми спостерігаємо практично протилежні результати, адже у випадку використання тканин Н1 та Н2 (рис.1 д,ж) досліджуваний елемент індикується дуже слабо, оскільки світиться лише один світло діод, а при розміщенні діода у корпусі з тканини Н3 (рис.1 з) він взагалі перестає визначатись нелінійним локатором.

Таким чином в доповіді наведені результати дослідження, які показують, що якщо закладні пристрої будуть мати корпус виготовлений із використанням певних радіонепрозорих тканин то локалізація та виявлення цих закладок з допомогою нелінійних локаторів значно ускладниться, а в деяких випадках навіть буде неможливою. Тому застосування нелінійних локаторів необхідно проводити лише у комплексі з іншими заходами пошуку та локалізації, для підвищення ймовірності знаходження таких закладних пристроїв, як мініатюрні диктофони.

Література

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации./ А.А. Хорев - М.: НПЦ «Аналитика», 2008. - 436 с.
2. Яремчук Ю.Є., Катаєв В.С., Гижко М.Ю. Можливості практичного застосування тепловізорів у питаннях захисту інформації. — "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" — 2016 — №1.- С.99-105.

ПРОБЛЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ЛАЗЕРНИМ КАНАЛОМ

Вадим Сінюгін

Вінницький національний технічний університет, м. Вінниця, Україна

In paper is investigated the problem of protecting acoustic speech information from leaks on laser channel and is substantiated features of this problem and possible ways to solve it

Keywords: protection of information, technical channels, a laser channel

Не дивлячись на розвиток і широке використання засобів обчислювальної техніки і представлення інформації в цифровому вигляді, існує проблема витоку інформації технічними каналами, а саме технічними каналами витоку інформації яка оброблюється у технічних засобах передавання інформації, технічними каналами витоку інформації при передаванні її по каналам зв'язку, технічними каналами витоку зорової інформації та технічними каналами витоку мовної інформації [1].

В залежності від середовища розповсюдження мовних сигналів і способів їхнього перехоплення технічні канали витоку інформації розділяють на акустичні, віброакустичні, електроакустичні та лазерні.

Різке зростання об'ємів інформації, що передається обумовило необхідність освоєння оптичного діапазону і систем обробки інформації на його основі [2].

Одним з актуальних каналів витоку мовної інформації на сьогоднішній день є лазерний канал. Лазерний канал витоку інформації відноситься до технічного каналу витоку мовної інформації. Говорячи про мовну інформацію, перш за все, мається на увазі проведення переговорів, нарад тощо. Витік інформації лазерним каналом здійснюється шляхом опромінення вібруючих поверхонь лазерним променем в акустичному полі тонких відбиваючих поверхонь (скла вікон, картин, дзеркал і тому подібне). Відбите лазерне випромінення (дифузне чи дзеркальне) модулюється по амплітуді і фазі (по закону вібрації поверхні) і приймається приймачем лазерного випромінення, при демодуляції якого виділяється мовна інформація [3].

Лазерне прослуховування є порівняно новою технологією. Проблема протидії знімання інформації з використанням лазерного мікрофона залишається досить актуальною і водночас однією з найменш вивчених у порівнянні з іншими засобами промислового шпигунства. Особлива привабливість таких систем обумовлена тим, що вони дозволяють вирішувати задачі знімання мовної інформації максимально безпечно, на відстані, опосередковано, уникаючи необхідності знаходження в приміщення з ціллю розміщення там закладних пристроїв, що завжди було пов'язано з ризиком, а також завдяки доступності, в наш час, достатньої кількості засобів, які дозволяють створювати такі системи самостійно і з мінімальним затратами [4]. Крім того, виявлення лазерного мікрофона досить складно, а в ряді випадків технічно нездійсненне. Для кожного виду апаратури технічної розвідки існує відпрацьована технологія її пошуку. Так для пошуку і локалізації радіомоніторингу успішно використовуються програмно-апаратні комплекси радіомоніторингу та індикатори поля, для пошуку пристроїв, які мають напівпровідникові елементи – нелінійні локатори. Існують комплекси, які дозволяють оцінювати рівень побічних електромагнітних випромінювань, є пристрої виявлення диктофонів та інше. А ось проблема оцінювання ступеня вразливості конкретного приміщення для знімання інформації з використанням лазерних мікрофонів залишається відкритою. Очевидно, що необхідним є збалансований підхід, оснований на реальній, комплексній і методично досконалій оцінці вразливості та захисту кожного конкретного об'єкта чи приміщення. Однак, при найближчому розгляді виявляється, що в цій області практично немає

серйозних напрацювань і, що саме головне, немає інструментів, які б дозволили проводити об'єктивні дослідження такого роду, а тому існує необхідність створення нових методів, засобів, покращення існуючих методів, які б забезпечували достатній рівень захисту інформації від витоку лазерним каналом.

З усього вище викладеного можна зробити висновок, що лазерні системи розвідки є досить ефективним засобом отримання інформації на відстані від об'єкту спостереження. Тому, для виключення загрози лазерного прослуховування потрібні нові або вдосконалені методи захисту інформації від витоку лазерним каналом, та засобів, які б не тільки обмежувались генераторами шуму.

Література

1. Чекатков А.А., Хорошко В.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.
2. Железняк В.К., Чернова И.С., Оценка модели оптико-электронного канала утечки речевой информации / В.К. Железняк, И. С. Чернова // Фундаментальные науки. Информационные технологии. 2015. – № 12. – С. 33-39.
3. Зайцев А.П., Шелупанов А.А, Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защити информации.- Москва: «Машиностроение». -2009 г. – 508 с.
4. Laser Spy Device [Електронний ресурс]. Режим доступу: http://www.lucidscience.com/pro-laser%20spy%20device-1.aspx