3. Элсенпитер Р. Windows 10 Professional. Администрирование сетей / Р. Элсенпитер, Т. Дж. Велт. — М. : Эком, 2018. — 560 с.

4. Максимальная безопасность в Linux. — К. : ДиаСофт, 2000. — 400 с. 8. Интернет-магазин ROZETKA. [Электронный ресурс]. — Режим доступа: http://rozetka.com.ua/

УДК 004.056.53

ОСОБЛИВОСТІ ПРОЦЕСУ ВИЯВЛЕННЯ ПРИХОВАНИХ ВІДЕОКАМЕР

Коротка Г. М., здобувач вищої освіти гр. МКБп-201
Науковий керівник: **Петренко Т. А**., к.т.н., доцент
Національний університет «Чернігівська політехніка»

Візуальне спостереження є найдавнішим та досить дієвим методом збору інформації. Приховане спостереження (дистанційна зйомка відеоінформації) завдяки своєї високої інформативності та конспіративності є одним з найперспективніших способів отримання конфіденційної інформації, тому досить велика кількість зусиль була направлена зловмисниками на їх розробку та вдосконалення. Задача своєчасного виявлення оптичного спостереження стає однією з основних при проведенні профілактичних та спеціальних захисних та охоронних заходів. Своєчасне викриття наявності несанкціонованого спостереження дає змогу встановити мету проведення та визначити загрозу, яку несе спостерігач за об'єктом, персоною або групою осіб [1].

Реально протидіяти прихованій відеозйомці вкрай складно, оскільки в більшості випадків встановлення прихованих відеокамер виконують професіонали високого класу, встановлюючи мініатюрні відеокамери не тільки в стіни приміщень, але і вмонтовують їх у побутові предмети: настінні годинники, книги, попільнички, тощо. Виявити таку камеру неозброєним оком, особливо при її камуфлюванні, досить складно.

На сьогодні, відеокамери можна виявити декількома відомими способами:

1) за допомогою індикатора поля (у випадку, коли передача інформації з камери ведеться по радіоканалу);

2) оптичним способом (лазерний промінь, який виходить з оптичного детектора, відображується від об'єктива відеокамери);

3) електромагнітний детектор відеокамер [2].

Найпростішими та найдешевшими детекторами радіовипромінювання закладних пристроїв є індикатори електромагнітного поля, які світовим або звуковим сигналом сигналізують про наявність у точці розташування антени електромагнітного поля з напругою вище порогової. Більш складні з них – частотоміри, які у додаток до того забезпечують вимірювання частоти найбільш «сильного» у точці прийому сигналу. До таких детекторів-приймачів можна віднести, наприклад, трьох-діапазонний індикатор поля «iPROTECT 1216» (рис. 1). iPROTECT 1216 – точний і надійний прилад, що призначений для знаходження різних видів радіочастотних підслуховуючих пристроїв в діапазоні від 50 МГц до 12 ГГц. На відміну від інших RF-детекторів, він має значно вищу чутливість до 3G, Wi-Fi і Bluetooth пристроїв. Тому Wi-Fi, Bluetooth та інші бездротові протоколи, що працюють в діапазонах від 2,4 до 5 ГГц, виявляються на більшій відстані.

Пошук прихованої зйомки оптичними детекторами ґрунтується на зворотному відбитті спрямованого випромінювання оптичною системою об'єктиву камери відеоспостереження. Оскільки всі оптичні прилади спостереження містять світлочутливий елемент (наприклад, ПЗС-матрицю), промінь, спрямований на цей елемент, відіб'ється від нього і повернеться назад до джерела, тобто до детектора. Таким чином, оператор надсилає зондуючий промінь на місце передбачуваного розміщення прихованої відеокамери, і в разі, якщо камера дійсно встановлена, він побачить відблиск, відбитий від світлочутливого елемента. Однак, крім потрібного сигналу в поле зору будуть потрапляти випромінювання від інших елементів, для

позбавлення від них в оптичні детектори налаштована система відсіювання таких шумів. Одним з таких приладів є детектор прихованих камер «WEGA-i» (рис. 2). За його допомогою можна визначити наявність всіх типів відеокамер незалежно від їх робочого стану та каналу передачі відеосигналу. Пошук і виявлення мікрооб'єктів прихованих відеокамер проводиться шляхом візуального аналізу поверхонь приміщення, всіх елементів меблів та інтер'єру через окуляр приладу.

Існує ще один спосіб виявлення відеокамер – за допомогою електромагнітних детекторів. Будь-яка, навіть сама мініатюрна камера, формує певне випромінювання, яке можна виявити за допомогою спеціальних приладів. Для цього прилад аналізує обстановку на об'єкті та аналізує випромінювання на всіх частотах і може виявити частоту, на якій працює камера. Прикладом даного типу пристроїв є багатофункціональний пошуковий прилад «ANDRE» (рис. 3). ANDRE дозволяє виявляти всі основні типи пристроїв негласного знімання інформації, включаючи аудіо, відео, телефонні, інфрачервоні і передавачі, які носяться на тілі. Комплектація приладу має широкий набір пошукових зондів і аксесуарів, що дозволяють збільшити ефективність пошуку [3].

Рисунок 1 – індикатор поля «iPROTECT 1216»

Рисунок 2 – Детектор прихованих камер

Рисунок 3 – пошуковий «ANDRE»

Дальність виявлення прихованих відеокамер і для оптичних, і для електромагнітних детекторів коливається в межах кількох метрів. У першому випадку на дальність впливають кілька факторів: тип підсвічування, наявність або відсутність налаштування по діоптріями, гострота зору оператора, освітленість приміщення, в якому проводиться огляд та ін.. Дальність дії електромагнітних детекторів залежить в основному від типу камери і від того, як камера випромінює. Камери, що погано випромінюють зазвичай виявляються на відстані близько 3 м, а що добре випромінюють – аж до 50 м, середня дальність виявлення становить 7-10 м [4].

Тривалість пошуку для електромагнітних детекторів у більшості залежить від обсягу видів відеокамер, що збережені у пам'яті пристрою. Сучасні електромагнітні детектори можуть здійснювати пошук відеокамер майже непомітно для оточуючих: у більшій частині з них наявні світлова, звукова і вібраційна індикації. Оптичні ж детектори не можуть вести таємний пошук. Однак оптичні прилади, на відміну від електромагнітних, здатні виявляти всі види відеокамер в незалежності, від того вимкнені вони чи включені.

Отже, протидія несанкціонованій фото- та відеозйомці є досить актуальною на сьогодні. При виборі типу детектора пошуку прихованого відеоспостереження необхідно відштовхуватись від задачі, яку необхідно виконати: у випадку, коли швидкість та скритність пошуку не відіграють значної ролі, можна застосовувати оптичні детектори, ціна на які вдвічі нижче, ніж вартість приладів електромагнітного типу.

Список використаних джерел

1. Т. Г. Дуброва. Пошук прихованого відеоспостереження в приміщенн [Електронний ресурс] / Т. Г. Дуброва, О. Д. Василенко – Режим доступу до ресурсу: http://ptmip.ipt.kpi.ua/wp-content/uploads/sites/6/2014/06/Dubrova.pdf.

2. Як виявити приховані відеокамери в приміщеннях [Електронний ресурс] – Режим доступу до ресурсу: https://www.likeme.pp.ua/iak-vyiavyty-prykhovani-videokamery-v-prymishchenniakh/.

3. Багатофункціональний пошуковий прилад ANDRE [Електронний ресурс] – Режим доступу до ресурсу: https://www.das-ua.com/ru/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/mnogofunkcionalnyj-poiskovyj-pribor-andre/.

4. Виявлення прихованих камер електромагнітним шукачем відеокамер. [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/5725661/page:14/.

УДК 004.056.55

Кузнецова А. М., здобувачка вищої освіти гр.КБ-181
Науковий керівник: **Семендяй С. М.**, викладач
Національний університет «Чернігівська політехніка»

КВАНТОВА КРИПТОГРАФІЯ

Інформація в сучасному світі є найціннішим товаром, тому завдання, що стоять перед шифрувальником - забезпечення її конфіденційності, цілісності і невідстежуванності, актуальні як ніколи. Можна сказати, що зараз завдяки розвитку класичної криптографії (зокрема, поширення стійких схем шифрування і цифрового підпису з використанням відкритого ключа) ці завдання виконуються цілком успішно.

Однак будь-який шифр коли-небудь зламується. У наш час найбільш суттєвою загрозою класичної криптографії є використання принципів квантової механіки в обчисленнях.

Квантова механіка, з одного боку, погрожує розкриттям ключових класичних шифрів, проте з іншого - дає можливість створювати принципово нові і потенційно абсолютно надійні криптографічні системи.

Квантова криптографія вивчає можливість генерації криптографічних ключів, секретність яких гарантується фундаментальними законами квантової механіки. Становлення квантової криптографії як науки почалося в 1984 року з розробки першого квантового протоколу розподілу ключів BB84. За ним інформація передається за допомогою кодування станів фотонів на передавальному кінці і подальшому їх вимірі на приймальному. У разі якщо порушник спробує вклинитися в канал між легітимними абонентами і перехопити передані фотони, то відповідно до принципу невизначеності Гейзенберга легітимні абоненти зможуть визначити факт такого вторгнення через різке збільшення числа помилок при реєстрації фотонів. Важливим є находження точної величини критичної помилки для протоколу BB84, яка є рівною приблизно 11%.

Отже, головною перевагою криптографічних протоколів є те, що зловмисник може володіти необмеженими можливостями для перехоплення ключової інформації, проте факт прослуховування каналу завжди залишиться поміченим. Це робить використання квантової криптографії привабливим для боротьби зі шпигунством і шахрайством.

Актуальністю використання та розвитку квантової криптографії є можливість протистояти квантовому комп’ютеру в захисті цифрової інформації від злому.

Через надзвичайно широку поширеність алгоритму RSA одним з найважливіших припущень криптографії є складність завдання факторизації великих чисел. І дійсно, до сьогодення не було знайдено алгоритму, досить швидко вирішує цю задачу. Однак у 1994 році був запропоновано алгоритм з поліноміальною складністю, вирішуючий це завдання на квантовому комп'ютері. Головна причина подібного феноменального прискорення - можливість використання так званого "квантового паралелізму" для проведення швидкого перетворення Фур'є, на якому засновані найбільш ефективні з відомих алгоритмів факторизації. Знаходження цього алгоритму дозволяє звести задачу факторизації до технологічної задачі побудови квантового комп'ютера: якщо його вдасться побудувати, схема шифрування RSA виявиться ненадійною. Це ставить можливості шифрування з відкритим ключем під велику загрозу.