

### 3 Технічні засоби системи захисту інформації. Стандартизація та метрологічне забезпечення систем ТЗІ. Визначення відповідності засобів ТЗІ

УДК: 621.384.3

#### МОЖЛИВОСТІ ПРАКТИЧНОГО ЗАСТОСУВАННЯ ТЕПЛОВІЗОРІВ У ПИТАННЯХ ЗАХИСТУ ІНФОРМАЦІЇ

*Яремчук Юрій; Катаєв Віталій; Гижко Максим; Скуратов Сергій*  
Вінницький національний технічний університет

#### THE PRACTICAL APPLICATION OF THERMAL IMAGER FOR THE PROTECTION OF INFORMATION

*Yaremchuk Yurii; Kataiev Vitalii; Guzhko Maxym; Skuratov Sergiy*  
Vinnytsia National Technical University

*Анотація:* Експериментально досліджено технічні можливості тепловізора у питаннях захисту інформації, зокрема для локалізації закладних пристроїв. Лабораторні виміри проведено при розташуванні закладки у різних об'єктах. Отримані дані дозволяють стверджувати, що працюючий технічний пристрій малих розмірів, такий як апаратна закладка, може в достатній мірі змінювати температуру об'єкту, в якому він знаходиться, для того щоб це можна було зафіксувати.

*Ключові слова:* Захист інформації, закладні пристрої, тепловізор, інфрачервоне випромінювання.

*Summary:* Experimentally investigated the thermal imager technical capabilities for the protection of information in particular for localization eavesdropping devices. Laboratory measurements conducted in cases where eavesdropping devices are located in the different objects. Results of measurement show, that technical device small size, for example eavesdropping device, can sufficiently change the temperature of the object in which it is located, so that it can be recorded.

*Keywords:* Information security, filling devices, thermal, infrared radiation.

#### Вступ

Захист інформації являє собою цілеспрямовану діяльність, направлену на виключення або суттєве обмеження неконтрольованого та несанкціонованого витоку відомостей, що мають обмежений доступ, а також різних видів впливів на інформаційні процеси. При цьому спектр можливих загроз досить широкий, адже існує велика кількість каналів витоку інформації. Класифікація таких каналів, в свою чергу, залежить від фізичної природи виникнення інформаційних сигналів, середовища їх поширення, методів обробки та зберігання, засобів перехоплення і т. д. До основних можна віднести: електромагнітні, електричні, параметричні, акустичні, віброакустичні, акустоелектричні, оптикоелектронні та канали витоку видової інформації [1].

Велику частину загроз становлять закладні пристрої (далі ЗП) або апаратні

закладки. Вони являють собою мініатюрні передавачі, що встановлюються безпосередньо у приміщенні де циркулює інформація з обмеженим доступом, а сигнали від них модулюються інформаційними сигналами. Проблема полягає в тому, що ЗП для знімання інформації можуть використовувати більшість існуючих каналів. Однак, найчастіше закладки слугують для перехоплення акустичної (мовної) та видової інформації, для цього можуть використовуватись:

- портативні диктофони, провідні мікрофони та мініатюрні відеокамери для прихованого звуко- або відеозапису;
- радіозакладки для передавання інформації радіосигналами;
- мережеві закладки для передавання інформації лініями електроживлення, телефонного зв'язку і т. д;

- акустичні телефонні закладки типу електронних вух.

Таким чином, однією із задач захисту є усунення можливостей витоку інформації саме через ЗП. Тому знання конструктивних та технічних особливостей побудови апаратних закладок необхідне для виявлення їх сильних та слабких сторін та вибору оптимального способу протидії.

### Аналіз існуючої проблеми

Електронні ЗП являють собою організований канал несанкціонованого отримання та передачі акусто-візуальної інформації, що циркулює на об'єкті інформаційної діяльності [2].

Метою захисту інформації від витоку через ЗП є локалізація та знешкодження або, у випадках коли локалізація неможлива, створення таких умов, при яких нормальна робота цих пристроїв буде ускладнена, а також проведення заходів, які унеможливають встановлення закладок у приміщенні.

Виявлення ЗП може здійснюватись двома способами: організаційним та технічним. Перший – це аналітична робота з визначення можливих місць встановлення ЗП із врахуванням особливостей їх роботи і візуальний огляд приміщення та пошук певних демаскуючих ознак в місцях можливого знаходження даних пристроїв. Другий – це локалізація апаратних закладок за допомогою спеціальної пошукової апаратури. Причому цей спосіб повинен враховувати всі технічні характеристики та особливості роботи ЗП, адже від принципу роботи закладки буде залежати і метод, яким можна буде цю закладку виявити. Наприклад, радіозакладки під час своєї роботи випромінюють електромагнітний сигнал, і відповідно пошуковий пристрій повинен вміти цей сигнал виявити з поміж інших та обробити його і т. п. Тому заходи технічного способу виявлення можуть включати: контроль сигналів у лініях зв'язку та електроживлення; контроль радіовипромінювань у області об'єкту; контроль інфрачервоних випромінювань;

використання приладів нелінійної локації, металодетекції, тепловізійних систем та ін.

Тобто технічний спосіб вимагає великої бази різних пошукових пристроїв, при чому, в деяких випадках, конкретний пристрій може використовуватись для виявлення ЗП, які мають лише конкретні складові або характеристики. Так, для виявлення прихованих відеокамер можна використовувати пристрій, робота якого заснована на ефекті "зворотного відблиску", суть якого полягає в наступному: пристрій створює оптичний промінь, який при попаданні на об'єкт відеокамери відбивається і поширюється у вузькому куті точно в напрямку зондуючого випромінювача при однопозиційній локації. Але проблема такого пристрою полягає в тому, що з його допомогою можна локалізувати лише пристрої, які в своєму складі мають об'єкт, тобто відеокамери.

Таким чином, виникає питання можливості виявлення різних апаратних закладок за допомогою одного універсального пошукового пристрою. Робота такого пристрою повинна базуватись на знаходженні певних ознак, фізичних явищ або характеристик, що притаманні різним видам ЗП. Такою ознакою може виступати температура, адже, як відомо, закладки, як і будь-які електронні пристрої, у своєму складі мають радіоелементи, для роботи яких необхідне джерело живлення, а при споживанні енергії від джерела ці елементи будуть нагріватись, збільшуючи тим самим загальну температуру усього пристрою. Зафіксувавши зміну температури у певному місці можна буде зробити висновок про наявність в цьому місці працюючого технічного пристрою.

Тому виникає необхідність практичного дослідження можливості виявлення ЗП за допомогою тепловізора. Хоча, можливості застосування тепловізорів у питаннях захисту інформації досить очевидні, відомо не так багато досліджень, в яких би висвітлювалось дане питання. В основній більшості публікацій розглядаються лише загальні принципи використання тепловізорів [3], [4] або досліджуються

галузі, які взагалі не відносяться до інформаційної безпеки [5]. Таким чином, подібне експериментальне дослідження є актуальним.

### Постановка задачі

Провести дослідження технічних можливостей тепловізора з точки зору пошуку ЗП. Визначити залежність зміни температури певних об'єктів при встановленні у них ЗП, і виявити спроможність локалізації цих апаратних закладок. Дослідження провести для випадків, коли закладний пристрій встановлений у елементах інтер'єру, а також у працюючому технічному пристрої.

### Методика пошуку та аналізу даних

Для експериментального пошуку ЗП використовується тепловізор Testo 875i. Як апаратна закладка використовується схема підсилювача сигналів, виконана на основі операційного підсилювача, що працює від напруги живлення 9В. Закладка встановлюється в наступних об'єктах: датчик руху, решітка від вентиляційної шахти, канцелярська тека.

Принцип дії тепловізора базується на перетворенні інфрачервоного спектру у видимий діапазон світлового випромінювання із розподіленням температури по відповідним кольорам. Тому як вихідні дані будемо використовувати спектрограму з екрану тепловізора із зазначенням температури у градусах Цельсія. Результатом дослідження буде висновок про

можливість знаходження ЗП у об'єкті, що досліджується за допомогою даного пошукового пристрою. Висновок про наявність апаратної закладки можна зробити у випадку, якщо температура об'єкту або його частини зі встановленою закладкою буде відрізнятися від температури при відсутній закладці.

### Виявлення закладних пристроїв з допомогою тепловізора

Як перший об'єкт для дослідження використаємо типовий датчик руху охоронної сигналізації. Для цього визначимо його температуру у нормальному режимі роботи (рис. 1,а), після чого використаємо аналогічний датчик зі встановленим всередині його корпусу ЗП (рис. 1,б).

Як бачимо максимальна температура датчика без закладки при нормальній роботі складає 19,4°C (рис. 1,а, точка М1), при цьому в аналогічного датчика зі встановленим ЗП на спектрограмі видно характерну ділянку на корпусі пристрою з максимальною температурою 38,5°C (рис. 1,б, точка М1). Тобто, у випадку, коли є можливість порівняти температуру двох аналогічних пристроїв, що працюють в однакових умовах, і при цьому їх температури відрізняються, існує ймовірність, що у пристрої з більшою температурою встановлені додаткові складові, які можуть являти собою закладний пристрій.

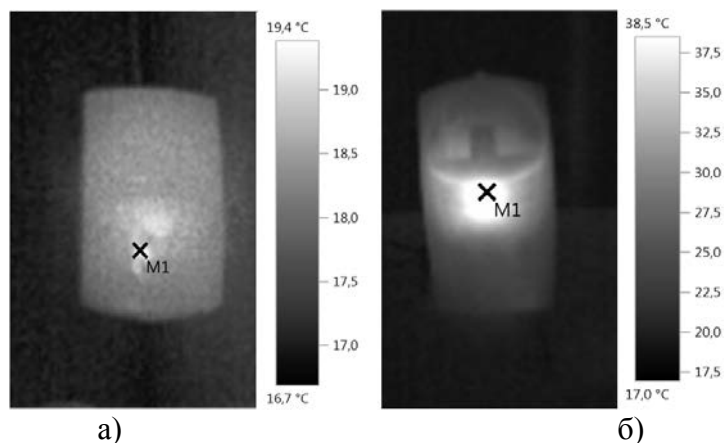


Рис. 1. Спектрограма датчика руху (а) без встановленого ЗП та (б) зі встановленим ЗП

Однак, іноді немає можливості порівняння двох аналогічних об'єктів, зокрема це може відноситись до елементів декору, конструкцій, різноманітних сувенірів тощо. В таких випадках висновок про наявність або відсутність закладного пристрою доводиться робити користуючись лише одним спектральним зображенням конкретного об'єкту. Тому слід зазначити, що при цьому слід керуватись наступною ознакою: працюючий закладний пристрій, звичайно, буде нагрівати собою навколишнє середовище, тобто в міру зростання власної температури ЗП буде зростати температура поверхні, на якій встановлена дана закладка. Таким чином, при дослідженні різноманітних об'єктів висновок про наявність у них ЗП можна буде зробити у випадку, якщо на спектрограмах цих об'єктів будуть спостерігатись ділянки підвищеної температури. Для експериментального підтвердження даного твердження

використаємо наступні об'єкти: решітка від вентиляційної шахти та канцелярська тека.

Працюючий закладний пристрій встановлюється зі зворотної сторони решітки від вентиляційної шахти (рис. 2,а), її спектрограма показана на рис. 2,б. Як видно з отриманого зображення температур, на решітці спостерігається «світла пляма», тобто ділянка з температурою більшою, ніж у навколишньої поверхні. Користуючись шкалою можна визначити, що температура ділянки, де встановлений ЗП, приблизно складає від 22°C до 36°C, при чому температура інших ділянок об'єкта не перевищує 18°C. Тому можна легко зробити висновок про наявність технічного пристрою на даному об'єкті. Однак, такі очевидні покази тепловізора зумовлені самою структурою решітки, оскільки через отвори вона легко пропускає інфрачервоне випромінювання від ЗП.

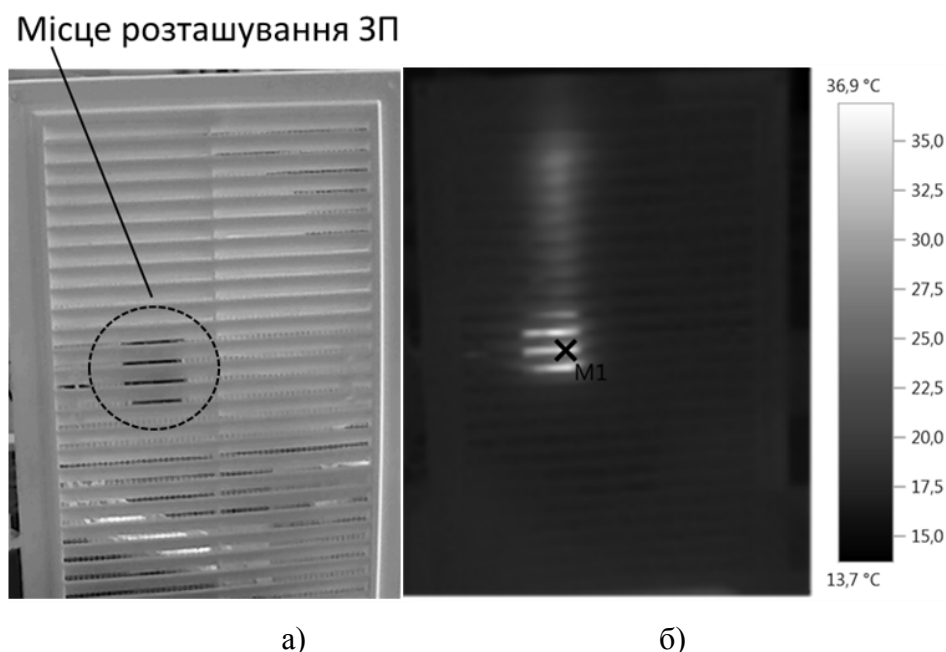


Рис. 2. Зображення (а) та спектрограма (б) решітки від вентиляційної шахти зі встановленим на ній ЗП

Тому проведемо аналогічне дослідження з об'єктом, що має суцільну конструкцію без отворів. Для цього встановимо апаратну закладку у канцелярську теку (рис. 3,а). Як видно зі спектрограми (рис. 3,б), у місці ймовірного розташування ЗП, знову спостерігається «світла пляма», при чому

температура даної ділянки складає 20-23°C, в той час як інші ділянки мають температуру, яка не перевищує 18°C. Тобто в даному випадку також можна зробити висновок про наявність закладного пристрою.

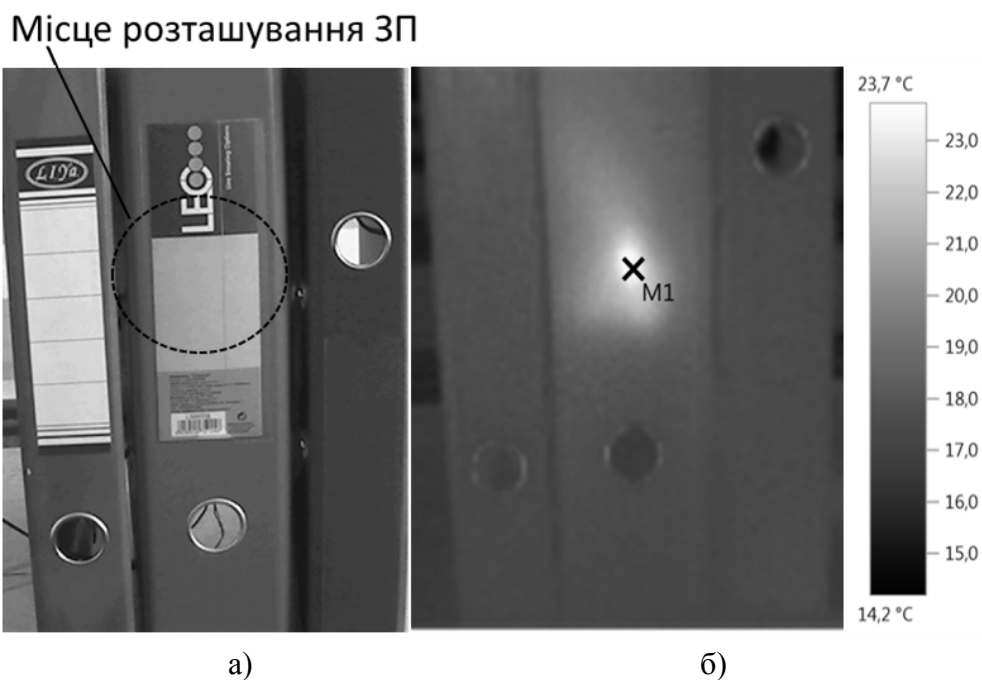


Рис. 3. Зображення (а) та спектрограма (б) канцелярської теки зі встановленим у ній ЗП

### Висновки

У лабораторних умовах проведено експериментальні дослідження технічних можливостей тепловізора з точки зору пошуку закладних пристроїв. В результаті були визначені залежності зміни температури досліджуваних об'єктів при встановленні в них ЗП. Спектрограми, отримані за допомогою тепловізора, дозволяють однозначно стверджувати, що працюючий технічний пристрій малих розмірів, зокрема апаратна закладка, може в достатній мірі змінювати температуру об'єкту, в якому він знаходиться, щоб це можна було зафіксувати. Однак слід зазначити, що ступінь нагрівання об'єкта залежить від багатьох факторів, таких як: безпосередній контакт ЗП з поверхнею об'єкта, структура об'єкта, теплопровідність матеріалу, з якого виготовлено об'єкт і т. д. Тому, очевидним є той факт, що можливі випадки, коли локалізація закладного пристрою за допомогою тепловізора буде ускладнена або навіть неможлива, наприклад якщо ЗП встановлено у пристрої, власна температура якого вища за температуру працюючої закладки.

Отримані результати дозволяють зробити висновок, що можливість використання тепловізора у питаннях захисту інформації, зокрема, для пошуку закладних пристроїв, має суттєві обмеження. Тому використання його як самостійного пошукового пристрою є неможливим, однак застосування тепловізора у комплексі з іншими заходами пошуку та локалізації значно підвищить ймовірність знаходження закладних пристроїв.

### Перелік посилань

- [1] А. А. Хорев, *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] Г. А. Бузов, *Защита от утечки информации по техническим каналам: Учебное пособие* / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев, - М.: Горячая линия - Телеком, 2005. - 416 с.
- [3] О. Т. Богорош, *Тепловізори в Україні: історія і перспективи* / О. Т. Богорош // Київський політехнік. - 2015. - № 11. - С. 2-3.
- [4] *Тепловізори в научно-исследовательской деятельности: увидеть то, что скрыто* [Електронний ресурс]: АО «Пергам-Инжиниринг».

<http://www.pergam.ru/articles/teplovizor-v-rnd.htm>.

- [5] А. Л. Ураков, *Использование тепловизора для оценки постинъекционной и постинфузионной локальной токсичности растворов лекарственных средств* / Н. А. Урабова, Т. В. Урабова, А. А. Касаткин, М. Л. Кашковский, В. Б. Дементьев, Н. В. Соколова, В. И. Шахов, А. П. Решетников, Ю. С. Сюткина // Проблемы экспертизы в медицине. – 2009. – №33-1(9). – С. 27-29.

### References

- [1] A. A. Khorev, *Tekhnicheskaya zashchita ynformatsyy: ucheb. posobie dlia studentov vuzov. V 3 t. Tom 1. Tekhnicheskiye kanaly utechky ynformatsyy.* / A. A. Khorev - M.: NPTs «Analytika», 2008. - 436 s.
- [2] Н. А. Buzov, *Zashchita ot utechky ynformatsyy po tekhnicheskym kanalim: Uchebnoe posobie* / Н. А. Buzov, S. V. Kalynyn, A. V. Kondratev, - M.: Horiachaia lnyia - Telekom, 2005. - 416 s.
- [3] О. Т. Bohorosh *Teplovizory v Ukraini: istoriia i perspektyvy* / О. Т. Bohorosh // Kyivskiy politekhnik. – 2015. – # 11. – С. 2-3.
- [4] *Teplovyzoru v nauchno-ysledovatel'skoi deiatelnosti: uvydet to, chto skryto* [Elektronnyi resurs]: АО «Perham-Ynzhyryn».  
<http://www.pergam.ru/articles/teplovizor-v-rnd.htm>.
- [5] A. L. Urakov, *Yspolzovanye teplovyzora dlia otsenky postyn'ektsyonnoi y postynfuzyonnoi lokalnoi toksychnosti rastvorov lekarstvennykh sredstv* / N. A. Uraкова, Т. V. Uракова, А. А. Kasatkyn, M. L. Kashkovskiy, V. B. Dementev, N. V. Sokolova, V. Y. Shakhov, A. P. Reshetnykov, Yu. S. Siutkina // Problemy ekspertyzy v medytsyne. – 2009. - #33-1(9). – С. 27-29.

### Реферат

*Яремчук Юрій, Катаєв Віталій, Гижко Максим, Скуратов Сергій*

#### **Можливості практичного застосування тепловізорів у питаннях захисту інформації**

Загальновідомо, що сьогодні інформація є найголовнішими ресурсом сучасного світу. Активний розвиток інформаційних технологій і їх інтеграція, обумовлюють крайньо важливі ролі, які вони відіграють у багатьох сферах людського життя. Важливі

відомості державного значення повинні бути захищені від несанкціонованого перехоплення і особливе значення у питанні захисту інформації має проблема витоку інформації через закладні пристрої. Проблема полягає у тому, що такі пристрої для знімання інформації можуть використовувати більшість існуючих каналів витоку. Однак, найчастіше закладки слугують для перехоплення акустичної (мовної) та видової інформації. Тому знання конструктивних та технічних особливостей побудови та функціонування апаратних закладок необхідне для виявлення їх сильних та слабких сторін та вибору оптимального способу протидії. Було експериментально досліджено технічні можливості тепловізора у питаннях захисту інформації, зокрема для локалізації закладних пристроїв. Лабораторні виміри проведено при розташуванні закладки у різних об'єктах. Отримані дані дозволяють стверджувати, що працюючий технічний пристрій малих розмірів, такий як апаратна закладка, може в достатній мірі змінювати температуру об'єкту, в якому він знаходиться, для того щоб це можна було зафіксувати.

*Яремчук Юрій, Катаєв Віталій, Гижко Максим, Скуратов Сергій*

#### **Возможности практического использования тепловизоров в вопросах защиты информации**

Общеизвестно, что сегодня информация является главным ресурсом современного мира. Активное развитие информационных технологий и их интеграция, обуславливают крайне важные роли, которые они играют во многих сферах человеческой жизни. Важные сведения государственного значения должны быть защищены от несанкционированного перехвата и особое значение в вопросе защиты информации имеет проблема утечки информации через закладные устройства. Проблема заключается в том, что такие устройства для съема информации могут использовать большинство

существующих каналов утечки. Однако, чаще всего закладки служат для перехвата акустической (речевой) и видовой информации. Поэтому знание конструктивных и технических особенностей построения и функционирования аппаратных закладок необходимо для выявления их сильных и слабых сторон и выбора оптимального способа противодействия. Было экспериментально исследовано технические возможности тепловизора в вопросах защиты информации, в том числе для локализации закладных устройств. Лабораторные измерения проведены при расположении закладки в различных объектах. Полученные данные позволяют утверждать, что работающее техническое устройство малых размеров, такое как аппаратная закладка, может в достаточной мере изменять температуру объекта, в котором оно находится, для того чтобы это можно было зафиксировать.

*Yaremchuk Yuri, Kataiev Vitalii, Guzhko Maxym, Skuratov Sergiy*

### **The practical application of thermal imager for the protection of information**

It is well known that today, information is the most important resource of the modern world. Active development of information technologies and their integration, causing extreme important role that they play in many areas of human life. Important information of national importance shall be protected against unauthorized interception and of particular importance in the issue of information security is the problem of information leakage through eavesdropping devices. The problem is that such devices for removal of information can use most existing leakage. However, often serve as bookmarks to intercept acoustic (speech) and species information. Therefore, knowledge of design and technical features of construction and operation of hardware bookmarks necessary to identify their strengths and weaknesses and the choice of

optimal method of response. Experimentally investigated the thermal imager technical capabilities for the protection of information in particular for localization eavesdropping devices. Laboratory measurements conducted in cases where eavesdropping devices are located in the different objects. Results of measurement show, that technical device small size, for example eavesdropping device, can sufficiently change the temperature of the object in which it is located, so that it can be recorded.

### **Відомості про авторів**

#### **Яремчук Юрій Євгенович**

**Освіта:** магістр за спеціальністю «Комп'ютерні науки» (1996).

**Місце роботи:** Вінницький національний технічний університет, Центр інформаційних технологій та захисту інформації, професор (2015), д.т.н. (2014).

**Область знань:** системи захисту інформації.

**Наукові інтереси:** криптографічний та стеганографічний захист інформації, безпека інформаційних систем, теорія чисел, рекурентні послідовності.

**Email:** yurevyar@vntu.net

#### **Катаєв Віталій Сергійович**

**Освіта:** спеціаліст за спеціальністю «Радіотехніка» (2013), спеціаліст за спеціальністю «Комп'ютерні системи та мережі» (2013).

**Місце роботи:** Вінницький національний технічний університет, Центр інформаційних технологій та захисту інформації.

**Область знань:** захист інформації, радіотехніка.

**Наукові інтереси:** технічний захист інформації.

**Email:** kataev@vntu.net

#### **Гижко Максим Юрійович**

**Освіта:** магістр за спеціальністю «Управління інформаційною безпекою» (2013).

**Місце роботи:** Вінницький національний технічний університет, Центр інформаційних технологій та захисту інформації,

**Область знань:** безпека інформації, управління інформаційною безпекою.

**Наукові інтереси:** технічний захист інформації

**Email:** voennuy@vntu.net

#### **Скуратов Сергій Миколайович**

**Освіта:** бакалавр за спеціальністю «Управління інформаційною безпекою» (2016).

**Місце роботи:** Вінницький національний технічний університет.

**Email:** Mr.skuratov@inbox.ru