УДК 004.056.53

**Б. М. Клешня**
**О. П. Войтович**

# ДОСЛІДЖЕННЯ БЕЗПЕКИ АВТОМОБІЛЬНИХ СИСТЕМ СИГНАЛІЗАЦІЇ

Вінницький національний технічний університет

***Анотація***

*Проаналізовано узагальнену структурну схему інформаційно-комунікаційних систем контролю доступу до транспортних засобів, а також можливі методи їх взламу.*

*Отже задачею майбутніх досліджень є виявлення вразливостей та можливих атак на системи автомобільної сигналізації.*

**Ключові слова:** сигналізація, автомобіль, безпека, код-граббер, угон.

***Abstract***

*The general structure of the information – communication systems of the access control systems to the vehicles was analyzed. Also possible methods of their hijack were analyzed.*

*So the task of future researches is determining of possible weaknesses and possible attacks on the automobile alarming systems.*

**Keywords**: alarming, vehicle, security, safety, code-grabber, hijack.

## Вступ

Сучасні автомобільні сигналізації – це інформаційно-комунікаційні системи, встановленні на автомобіль, які виконують функції контролю доступу до систем транспортного засобу, ускладнюючи викрадення автомобіля, різноманітних його елементів, або речей, які знаходяться в салоні, або багажному відділенні транспортного засобу [1]. Незважаючи на постійне ускладнення систем захисту, рівень викрадення автомобілів практично ніяк не змінюється протягом останніх п’яти років [2].

Метою роботи є дослідження безпечності сучасних автомобільних систем захисту та сигналізації. для виявлення недоліків та можливостей зламу.

## Результати дослідження

Сучасні автомобільні сигналізації [3, 4] складаються з таких електронних компонентів (рис.1):

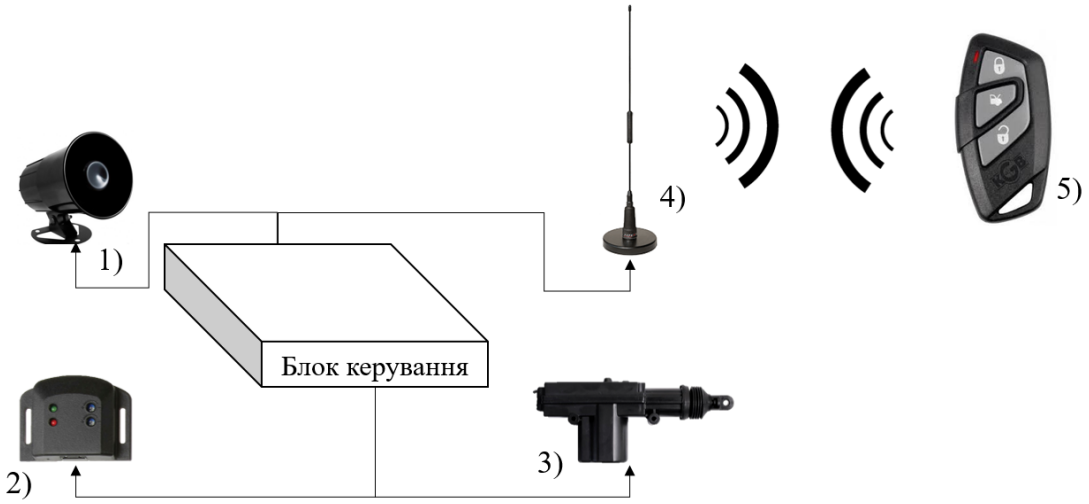


Рис. 1. Узагальнена схема автомобільної сигналізації

1) Звуковий гучномовний пристрій; 2) Сенсор удару; 3) Електронні приводи дверних замків; 4)Радіо – антена; 5) Пульт керування сигналізацією; 6) Блок керування сигналізацією; 7) Різноманітні блокатори; 8) Світлові індикатори роботи.

Системи використовують бездротові канали зв'язку, методи шифрування та різноманітні сенсори руху. Живлення всіх пристроїв сигналізації відбувається від бортової мережі 12 вольт. Розташування та підключення елементів сигналізації може бути різним, залежно від виробника та бажання власника.

В системах сигналізації можуть бути використані різноманітні блокатори, призначенням яких є блокування окремих елементів автомобіля з метою ускладнення викрадення авто, або окремих його елементів. Це можуть бути блокатори керма, бензонасосу, основного блоку керування двигуном, або блокатори різних зон авто, таких як ладник, або багажник.

Функції дистанційного керування сигналізацією виконуються спеціальним бездротовим брелком. Брелок надсилає команди на блок керування за допомогою радіо – передавача.

Для систем автомобільної сигналізації використовуються обмежена кількість радіо – частот. Ці частоти вибрані таким чином, щоб не мати перешкод з боку інших бездротових пристроїв. В основному використовуються частоти 315, 433, 434 та 868 МГц.

Способи автентифікації користувача:

- передавання постійної кодової комбінації;
- передавання динамічної кодової комбінації;
- використання діалогового коду (з нульовим розголошенням);
- динамічна зміна частот передачі та прийому кодових комбінацій.

Пристрій для зламу автомобільної сигналізації називається «Код-граббер» [5]. Він складається з радіо-приймача та передавача, і працює таким чином:

1) приймач перехоплює кодову комбінацію, яка надсилається з брелка сигналізації;
2) код-граббер перераховує кодову комбінацію, яка встановлювала сигналізацію в режим захисту;
3) передавач відправляє перераховану комбінацію на зняття сигналізації з захисту.

Але сучасні автомобільні сигналізації використовують все більш складні схеми автентифікації, для унеможливлення несанкціонованого доступу та керування інформаційною системою транспортного засобу, тому сучасні код-граббери можуть бути значно складнішим пристроєм ніж просто перехоплювач радіосигналу.

## Висновки

Проаналізовано узагальнену структурну схему інформаційно-комунікаційних систем контролю доступу до транспортних засобів. А також можливі методи їх взламу.

Отже задачею майбутніх досліджень є виявлення вразливостей та можливих атак на системи автомобільної сигналізації

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лужецький В. А. Захист персональних даних. Навчальний посібник / Лужецький В. А., Войтович О. П., Дудатьєв А. В. – Вінниця ВНТУ, 2009. – 240 с.

2. Где в Украине угоняют больше всего автомобилей – [Електронний ресурс]: - https://112.ua/statji/gde-v-ukraine-ugonyayut-bolshe-vsego-avtomobiley-337479.html

3. Еремич Н. Г. Как избежать угона. Системы безопасности автомобиля. – Издательский дом" Питер", 2011.

4. Ефремов Е. А., Ковалевский А. Е. Анализ автоматических систем контроля доступа //Молодежный научно-технический вестник. – 2017. – №. 5. – С. 40-40.

5. Матяш Д. І. Аналіз протоколів автентифікації для автосигналізації. – 2015.

***Клешня Борис Михайлович*** — студент групи 1БС-15б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 1bs15bklesnya@gmail.com

***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет

***Kleshnya Borys M.*** — Department of information technologies and computing engineering, Vinnytsia National Technical University, Vinnytsia, email : 1bs15b.mykhailenko@gmail.com

***Voitovich Olesia P.*** — Cand. of Sc. (tech), Assistant Professor of information protection department, Vinnytsia National Technical University, Vinnytsia