ІНФОРМАЦІЙНЕ ТА НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ НАУКОВОЇ ДІЯЛЬНОСТІ

УДК 629.331.047

В.А. Білогуров,
старший науковий співробітник ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0003-1896-0782,
К.В. Заїчко,
здобувач ДНДІ МВС України, начальник відділу ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0001-5987-3197,
Д.С. Назарок,
старший науковий співробітник ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0002-3000-4534

РОЗВИТОК СИСТЕМ КОНТРОЛЮ ДОСТУПУ ДО ТРАНСПОРТНИХ ЗАСОБІВ

У статті розглянуто протистояння засобів і способів протиправного заволодіння транспортними засобами або їх розукомплектування і засобів, які попереджують про початок протиправних дій, а також перешкоджають їхньому завершенню. Розглянуто автомобільні сигналізації без дистанційного керування, з управлінням по радіоканалу і використанням статичного та динамічного кодів; основні принципи кодування сигналу – Keeloq Code Hopping; вразливість радіокерованих автомобільних сигналізацій від дії радіосканерів та граберів. Наведено функціональні та технічні характеристики сучасної дистанційно керованої автомобільної сигналізації з багатоканальним управлінням і 128-бітним шифруванням.

Ключові слова: *контроль доступу, кодер.*

В статье рассмотрено противостояние средств и способов противоправного завладения транспортными средствами или их разукомплектации и средств, которые предупреждают о начале противоправних действий, а также блокируют их завершение. Рассмотрены автомобильные сигнализации без дистанционного управления, с управлением по радиоканалу и использованием статического и динамического кодов; основные принципы кодирования сигнала – Keeloq Code Hopping; подверженность радиоуправляемых автомобильных сигнализаций действиям радиосканеров и граберов. Приведены функциональные и технические характеристики современной дистанционно управляемой автомобильной сигнализации с многоканальным управлением и 128-битным шифрованием.

Ключові слова*: контроль доступу, кодер.*

У роботі висвітлено питання щодо використання сучасних технологій, які застосовуються в системах охоронної сигналізації автотранспорту. Вивчено ряд недоліків охоронних систем. Проведено ознайомлення з системами контролю доступу та їх надійністю на практиці.

Якщо проаналізувати охоронні системи для автомобілів, то можна помітити чітку паралель в історичному розвитку: система захисту – методи (засоби) її подолання. Першою системою захисту автомобіля від протиправного заволодіння був звичайний механічний замок на його дверях. Зважаючи на те, що на відкриття простих механічних замків злодію іноді достатньо лічених секунд, були розроблені системи автосигналізації, завданням яких було (є) попередження власника автотранспортного засобу про спробу незаконного заволодіння. Однак і такі системи не зупинили викрадачів автотранспорту. Викрадачі навчились нейтралізовувати автосигналізацію шляхом відключення живлення від неї (живлення від акумуляторної батареї автомобіля).

Для зручності використання авто-сигналізації на ринку з'явились охоронні системи з дистанційним керуванням (постановкою та зняттям з охорони). Для того щоб відключити таку сигналізацію дистанційно, не пошкоджуючи автомобіль, зловмисникам потрібно знати або "підібрати" таємну ефірну посилку. Дуже скоро стали відомі робочі частоти брелоків, а також те, що цей тип сигналізацій використовує один кодовий сигнал. Кількість можливих комбінацій кодових посилок у сигналі складала 512, а потім збільшились до 2^{24}. Для зламу таких систем з'явились так звані сканери. Сканер – це цифровий радіопередавач, який шляхом випромінювання в ефір кодових посилок, що послідовно змінюються, може "підібрати" правильну посилку й таким чином ввімкнути/вимкнути сигналізацію. Для захисту від сканерів була введена функція антисканування, яка при прийомі хибного коду в форматі атакованої сигналізації блокує прийом кодових посилок від сканера на деякий час. Враховуючи досить велику кількість комбінацій посилок 2^{24}, можна зробити висновок про необхідність витрати дуже великого обсягу часу для подолання таких систем. Наприклад, при 0,5 хвилинній паузі необхідно витратити 2^{23} хвилин для перебору усіх можливих комбінацій.

Для подолання систем охорони обладнаних функцією антисканування були розроблені пристрої, що отримали назву – грабери. Перші грабери – це комбіновані пристрої, що включали в собі: приймач цифрової кодової посилки, блок пам'яті для її збереження та передавач. Таким чином, грабер не "підбирає" кодову посилку – він її перехоплює з ефіру, коли власник автомобіля ставить на охорону чи знімає сигналізацію з охорони, запам'ятовує її, а потім може в будь-який час відтворити в ефірі. Для захисту від перших граберів почали використовувати різні команди для постановки та зняття сигналізації з охорони. На брелоці з'явилась ще одна кнопка. Але виходячи з того, що кодова посилка несе в собі інформацію про номер натиснутої кнопки на брелоці, програмне забезпечення граберів вдосконалили до можливості розрізнення посилок.

Для виключення можливості повтору записаної кодової посилки, був розроблений динамічний (стрибаючий, плаваючий) код, який змінює кодову посилку при кожному натисканні на кнопку брелока. У цьому випадку грабери доповнились ще одним блоком – генератором радіозавади. Вдосконалення призвело до роботи по такому алгоритму: під час появи в ефірі першої кодової комбінації від брелока автосигналізації грабер випромінює в ефір радіозаваду, яка заважає приймачу автосигналізації правильно ідентифікувати посилку. Зважаючи на те, що грабер "знає", який сигнал і коли був випромінений як завада, він фільтрує записану інформацію та запам'ятовує першу кодову посилку. Далі грабер знову стає в режим прийому. Якщо в ефірі з'являється друга кодова посилка, все повторюється:

постановка завади – запис інформації. Таким чином, записавши достатню кількість кодових посилок (при цьому необхідно звернути увагу на те, що власник автомобіля повинен декілька разів послідовно натиснути на кнопку брелока), грабер у проміжку між натисненням на кнопку брелока надсилає в ефір першу записану команду – сигналізація стає в режим "охорона". Після того, як власник автомобіля віддаляється на достатню відстань, зловмисник, використовуючи грабер, надсилає в ефір другу записану кодову комбінацію та знімає автомобіль з охорони.

Подальший розвиток сигналів для обміну інформацією між брелоками та сигналізаціями призвів до появи таких методів:

– подвійний динамічний код D-2, сутність якого: кожному брелоку, окрім розрядного номера, присвоюється ще й індивідуальний закон зміни коду. Це індивідуальне правило записується в кодер один раз при програмуванні брелока, в ефірі більше не з'являється й радіоперехопленню не доступно;

– подвійний динамічний код D-квадрат: сигнали брелока кодуються унікальним подвійним динамічним кодом, завдяки якому при кожному натисненні на кнопку брелока змінюється не тільки сам код, але й алгоритм кодування;

– технологія DID: застосовується у транспондерах-мітках, завдяки яким охоронна система розпізнає власника;

– динамічний код Time Code: закодований сигнал, що випромінюється, містить у собі інформацію з міткою про час. Ця інформація індивідуальна для кожної мітки. Основний блок приймає радіосигнал, визначає мітку як "свою" або "чужу" й одночасно аналізує інформацію про час. Якщо мітка визначена як "своя", але час прийому не відповідає часу прийому радіосигналу від цієї мітки, то сигналізація ігнорує мітку та готує процедуру "протирозбою". Щоб нейтралізувати подібну систему, необхідно отримати копію мітки, до того ж залишається відкритим питання синхронізації "часу" копії з сигналізацією [1; 6].

Автомобільна сигналізація – це цілий охоронний комплекс, який для повідомлення власника автомобіля про спробу угону використовує не тільки звуковий сигнал, але й передає інформацію про стан автомобіля по радіоканалу (використовуючи GSM (SMS повідомлення) зв'язок), про місцезнаходження (технологія GPS із використанням радіозв'язку між автомобілем та брелоком автосигналізації), дозволяє дистанційно відчиняти/зачиняти будь-яку із дверей, запускати двигун тощо.

Якщо розглянути ринок автомобільних охоронних систем та пристроїв загалом, то їх можна розділити за типом та ціновим класом.

Протиугоні системи бувають чотирьох типів:

– механічні (блокування валу керма, капота, коліс автомобіля, коробки переміни передач та інше);

– електронні (пейджери, імобілайзери та інше);

– електронно-механічні (імобілайзери в поєднанні з електронним замком капота, електромеханічне блокування дверей тощо);

– бензоклапани (для установки на карбюраторні й інжекторні двигуни).

Розглядаючи охоронні системи за ціновими показниками, можна зробити розподіл на три класи:

– недорогі сигналізації (Pantera XS100, Jaguar GX200, Cenmax X200, Mister X, Mongoose iq250);

– середній клас сигналізацій (Alligator LX 430/730, Pantera SLK, Mongoose AMG 750, Meritec Master);

– високий клас – цей клас систем має всі можливі функції зазначених вище класів, які зібрані в одну систему. У систему можуть бути додані такі функції, як: дистанційний запуск двигуна автомобіля на відстані від 500 до 1000 метрів, запуск по таймеру, контроль температури в салоні, використання бездротових реле блокування запалення, сповіщення при виході із зони досяжності передавача автомашини, супутникове спостереження та відправка координат місцезнаходження автомобіля. До цього класу охоронних систем можна віднести Pandora DX-90BT, Starline B96 2 CAN+2 LIN GSM/GPS, Starline A96 2 CAN+2 LIN GSM/GPS з 128-бітним шифруванням [2; 3].

Щодо функцій авто-сигналізацій, то це стандартний набір:

– блокування запалення;

– датчик на відчинення дверей, капота, багажника;

– датчик на удар – "шок сенсор" (деякі системи комплектуються датчиком на об'єм (ультрасонік або мікрохвильовий сенсор) або датчик на розрізання скла склорізом);

– сирена до 128 дБ (сирени поставляються в комплекті сигналізацій у чотирьох варіантах:

– автономні сирени із внутрішнім джерелом живлення;

– неавтономні сирени без джерела живлення;

– моноблочні автономні системи (SIRIO 777, LAZERLINE, COBRA, SIKURA, META та інші);

– світлова сигналізація габаритними вогнями;

– режим відлякування – "паніка";

– "тиха" постановка на охорону;

– можливість підключення до центрального замка.

Брелоки

Попередником сучасних брелоків, що використовуються для керування охоронною системою автомобіля, можна вважати передавач кодових посилок дротяного типу. Цей передавач за своїми функціональними можливостями нагадує швидше кодовий замок, який зараз встановлюється на дверях багатоповерхівок, і відрізняється від нього лише вбудованим таймером для затримки подачі сигналів керування на елементи охоронної системи. Затримка дозволяла власнику автомобіля до або після набору коду відчинити або зачинити двері автомобіля без вмикання сигналів тривоги. При цьому найчастіше водій має поспішити, щоб встигнути вийти з автомобіля, або встигнути на панелі керування вимкнути сигналізацію, в іншому випадку спрацює сирена. Панель керування сигналізацією, зазвичай була вбудована в приладову дошку. Крім того, процедуру натискання кнопок на панелі було добре видно зі сторони, особливо якщо скористатися біноклем або підзорною трубою – при великому бажанні цей простий оптичний прилад зловмиснику цілком доступний. Таким чином, з'явилася ідея застосування радіоканалу для дистанційного керування охоронною сигналізацією.

Однією з проблем було забезпечення стабільності передачі керуючого коду при мінімальній потужності (порядку 1 мВт) сигналу й прийнятному радіусі дії.

Також необхідно було отримати мінімальні габарити й вагу самого пристрою передачі коду (брелока) з тим, щоб він розміщувався в долоні та кишені. При цьому необхідно було врахувати розмір елемента живлення (батареї) та його енергоємності. Нарешті через кілька років був здобутий патент на радіопере-

давальний пристрій з петльовою антеною на друкованій платі, яка дозволила передавати постійну кодову посилку на достатню відстань. Ще через кілька років було запатентовано сигналізацію з розширеним діапазоном функціональних можливостей. Поштовхом до цього була поява на ринку дешевих мікрочипів багатоканальних малогабаритних швидкісних мікропроцесорів. До алгоритму роботи сигналізації були введені сигнали підтвердження постановки на охорону: звукові та світлові, які полегшили життя власнику автомобіля. Тому наступним вдосконаленням була розроблена функція, яка дозволяла власнику автомобіля самому вирішувати питання про необхідність користування світловим або звуковим сигналом.

Несприятлива кримінальна обстановка послужила поштовхом до розробки функції "Паніка". За допомогою світлових і звукових сигналів власник міг при розбійному нападі скористатися своїм автомобілем як додатковим засобом залучення уваги оточуючих. Знову ж таки, з ростом кількості каналів мікропроцесора з'явилась можливість збільшити кількість як охоронних, так і сервісних функцій. Відповідно зростала і кількість кнопок на брелоці, що, у свою чергу, вело до його модернізації. Наприклад, використовуючи брелок з двома кнопками, можна задіяти до трьох каналів, з трьома – до шести, а з чотирма – до десяти каналів. Але і такої кількості каналів зв'язку не вистачало, особливо на елітних системах. Необхідність поєднати мініатюрність і багатофункціональність потребує іншого підходу для вирішення проблеми. Таким чином, розроблено алгоритм керування за принципом револьверних систем – мінімальна кількість кнопок, але максимальна кількість каналів. У цьому випадку використовують додаткові канали (кнопки) для переходу на другий, третій і т.д. рівень запрограмованих охоронних і сервісних функцій сигналізацій. Для достатньо простих, середніх за кількістю функцій систем до цього часу застосовують брелоки з двома кнопками, але провідні фірми, наприклад Clifford, у своїх найбільш елітних моделях притримуються варіантів з чотирма кнопками. Для користувачів таке рішення здається успішним, оскільки запам'ятати призначення кнопок неважко, але, крім цього, велика кількість виробників стали наклеювати зі зворотної сторони багатокнопочних брелоків ярлички з підказками.

З часом для значного зниження вірогідності несанкціонованого доступу до системи охорони почали використовувати кодові посилки. Перші брелоки мали код, який складався з 8 або 16 розрядів і у більшості випадків встановлювався шляхом перерізання доріжок на платі або DIP – перемикачем. Згодом з метою підвищення таємності (тобто для виключення вірогідності повтору кодових комбінацій) й у зв'язку з необхідністю передавати більшу кількість інформації каналом зв'язку довжину файла з кодом довелося збільшити. Але це зростання не могло бути нескінченним – час передачі обмежено, тому збільшується вірогідність спотворень інформації під впливом зовнішніх електромагнітних завад. Для збільшення таємності була введена базова інформація з алгоритмом кодування та схема перетворення інформації в брелоках від центрального блоку охоронної системи, що дає такі переваги.

По-перше, підвищується рівень захищеності системи, оскільки тепер коди не знає ніхто – ні виробник, ні особа, що встановлювала сигналізацію, ні сам користувач.

По-друге, виникає можливість стирання з пам'яті кодів втрачених або вкрадених брелоків.

По-третє, брелоку можна надати відчуття індивідуальності, тобто конфігурувати його "бібліотеку" охоронних і сервісних функцій під конкретного користувача, наприклад під кожного члена родини.

Але дійсно революційним кроком у підвищенні криптостійкості посилки, що передається, стала поява одного з найдосконаліших на той час принципів кодування сигналу – Keeloq Code Hopping.

Взаємодія брелоків з охоронними системами авто-сигналізацій

Характеризуючи роботу брелоків, не можна не зупинитися на таких параметрах, як спосіб передачі, частота й потужність випромінювання: саме ними можна визначити дальність дії, стійкість до завад від електромагнітних випромінювань та енергоспоживання.

Спочатку в усіх брелоках моделей сигналізацій для передачі сигналу використовувалася амплітудна модуляція (АМ), точніше її цифровий варіант (ASM), як найбільш простий і дешевий метод. Більшість брелоків мають схеми передавача, багато чим схожі зі схемою генератора *Колпитця* та відрізняються один від одного лише елементом стабілізації частоти (резонатор поверхневих акустичних хвиль, ПАХ-резонатор або кварцевий резенатор). Згодом почала використовуватися частотна модуляції (ЧМ), або її цифровий варіант, для досягнення кращої захищеності від завад [4].

Якщо до способів передачі даних у світі існує єдиний підхід, то у виборі частотного діапазону відслідковується деяке "розходження". Це пов'язано з нормативами, які встановлені у багатьох країнах. У свій час Україна взяла приклад з європейських держав, в яких для подібних пристроїв був введений діапазон частот 433,05–434,75 МГц з шириною смуги частот 1,74 МГц.

На сьогодні можна виділити декілька реперних частоти, біля яких виробники охоронних систем встановлюють несівну частоту: 310+/-10, 370, 434 і 447, 868, 915 МГц. Відразу зазначимо, що ширина 20 МГц для частоти 310 МГц – це не похибка, а розкид значень для брелоків певних виробників. Невелике відхилення від реперних значень може бути викликане як похибкою вимірювання, так і особливістю схеми генератора. Для живлення схеми передавача найчастіше використовуються елементи живлення на 12 В типу Alkaline 23 A, які дозволяють працювати при досить великих споживаннях струму. У цих же моделях, які розроблялися з метою мінімізації енерговитрат, частіше використовуються літієві елементи. Це служить гарантією, що користувачу не доведеться проводити заміну елемента живлення частіше ніж один раз на 2–3 роки (для односторонньої сигналізації).

Для захисту автомобільної сигналізації від застосування кодграбберів і підвищення надійності передачі інформації виробники сучасних сигналізацій відмовляються від амплітудної модуляції (АМ), точніше її цифрового варіанта (ASM), як найбільш простого і дешевого методу на користь частотної модуляції (FM), в тому числі вузько смугової (NFM). Прикладом такого рішення може бути виріб KGB GX-3 (5,6).

Опис

Автомобільна охоронна система KGB GX-3 ґрунтується на основі запатентованої технології здвоєного діалогового коду, за якої радіокоманди брелока дублюються на двох різних каналах. При цьому система в режимі реального часу самостійно

обирає один із каналів, якість прийому якого краща. Ця технологія має майже абсолютну стійкість до різних видів електронного злому і код-граббінгу. Для створення цього коду були застосовані індивідуальні 128-бітні ключі шифрування, важливою особливістю яких є можливість їх зміни при кожному наступному перезапису брелока в системі.

Автомобільна охоронна система KGB GX-3 має додаткові керуючі FLEX-канали з можливістю інтелектуального програмування в режимі сервісних налаштувань. Застосування цих каналів не потребує під'єднання додаткових зовнішніх пристроїв для здійснення складних задач, котрі виконуються штатними системами за командою охоронної сигналізації.

Здвоєний діалоговий код (DUPLEX DIALOG)
Досконалий захист від завад (8192 каналів)
Швидкодія системи (час відгуку 0,25 сек)
Керування штатним брелоком автомобіля (Режим SLAVE)
Контроль з будь-якої точки світу (Bilarm GPS/GSM)
Функція "Комфорт"
Автоматичне замикання дверей при натисканні гальма
Дистанційне вимірювання температури в салоні автомобіля
Постановка системи на охорону з двигуном, що працює на холостому ходу
Турботаймер
Діалогові брелоки в комплекті (1 з РК-дисплеєм + 1 без дисплея)
Виходи для додаткових блокувань двигуна
Кількість незалежних зон охорони: 7
Можливість позонового відключення датчиків системи
Вихід 1-го радіокерованого каналу для керування замком багажника чи додатковими приладами
Вихід 2, 3, 4-го радіокерованого каналу для керування додатковими приладами
Сервісний режим Valet
Можливість під'єднання додаткового датчика
Можливість під'єднання CAN модуля
Сумісність з автоматичною і ручною трансмісією

ХАРАКТЕРИСТИКИ

Бренд **KGB**
Країна-виробник – Тайвань
Партномер KGB GX-3
Тип – протиугінний пристрій, автосигналізація, іммобілайзер
Тип зв'язку. Радіозв'язок
Робоча частота, 434 МГц
Дальність зв'язку, 600 м (режим керування); 1200 м (режим оповіщення)
Тип сповіщувача. Світло-звуковий
Протиугінні функції. Режим "паніка", Режим Anti-HiJack
Безшумне ввімкнення режиму охорони.

ОСНОВНІ ХАРАКТЕРИСТИКИ

Здвоєний діалоговий код (DUPLEX DIALOG): Так
Досконалий захист від завад (8192 каналів): Так

Рекордна швидкодія системи (час відгуку 0,25 сек): Так
Керування штатним брелоком автомобіля (Режим SLAVE): Так
Контроль з будь-якої точки світу (Bilarm GPS/GSM): Так
Сповіщення про ввімкнення передпускового підігрівача: Так
Попередження про розряд батарейки брелока передавача: Так
Функція "Комфорт": Так
Автоматичне замикання дверей при натисканні гальма: Так
Дистанційне вимірювання температури в салоні автомобіля: Так
Постановка системи на охоронну з двигуном, який працює на холостому ходу: Так
Турботаймер: Так

ДОДАТКОВІ ХАРАКТЕРИСТИКИ

Діалогові брелоки в комплекті (1 з РК-дисплеєм + 1 без дисплея): Так
Частота радіоканалу: 434 МГц
Радіус дії в режимі керування: 600 м
Радіус дії в режимі оповіщення: 1200 м
Виходи для додаткових блокувань двигуна: Так
Режим "Паніка": Так
Обхід несправної зони при постановці на охорону з указанням зони чи тригера: Так
Пам'ять на 1 чи 2 останніх спрацювання системи із зазначенням зони/тригера: Так
Кількість незалежних зон охорони: 7
Режим пасивного блокування двигуна / іммобілайзер: Так
Функція антипограбування: Так
Вимкнення охорони в 2 етапи: Так
Безшумні постановка/зняття системи з охорони: Так
Можливість позонового відключення датчиків системи: Так
Самодіагностика при ввімкненні режиму охорони: Так
Вихід 1-го радіокерованого каналу для керування замком багажника чи додатковими приладами: Так
Вихід 2, 3, 4-го радіокерованого каналу для керування додатковими приладами: Так
Сервісний режим Valet: Так
Функція виклику власника автомобіля: Так
Функція пошуку автомобіля: Так
Можливість під'єднання додаткового датчика: Так
Можливість під'єднання CAN модуля: Опціонально.
Автоматичне замикання/відчинення дверей при ввімкненні/вимкненні запалення: Так
Сумісність з автоматичною і ручною трансмісією: Так
Інформація про електронний злам названої сигналізації у відритих джерелах відсутня.

Висновки:

Постійний розвиток технічних систем контролюю доступу до транспортних засобів відбувається на тлі появи нових засобів несанкціонованого зламу протоколів шифрування та пристроїв для протиправних дій. Впровадження інтелектуальних систем контролю захисту та наукових досягнень у створенні протоколів обміну

даними дозволяє підвищити стійкість від зламу дистанційно керованих систем з радіоканалом та посягань на транспортні засоби.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Когда автомобильная охранная система не может быть эффективной. URL: ugona.net/article/ugon-paukom-kak-zashchititsia-368.html (дата звернення 25.10.2018).
2. Тестируем контроль канала связи на современных сигнализациях. URL: ugona.net/article/ugon-glushilkoi-testiruem-kontrol-kanala-sviazi-359.html (дата звернення 26.10.2018).
3. Агент Эксперт. Пандора Эксперт. Старлайн Эксперт. URL: ugona.net/catalog/alarm/starline/expert-3513.html (дата звернення 26.10.2018).
4. Основные способы защиты. URL: ugona.net/article/testiruem-bezopasnost-podzemnogo-parkinga-i-shtatku-mersedes-gls-355.html (дата звернення 27.10.2018).
5. Методы используют на практике угонщики. URL: ugona.net/article/test-shtatnoi-okhrannoi-sistemy-bmw-x6-f16-353.html (дата звернення 25.10.2018).
6. Бэкдор, backdoor – программа получения повторного доступа. URL: ugona.net/article/schema-ugona-nissan-kashkai-kakikh-ozhidat-ugroz-351.html (дата звернення 26.10.2018).

REFERENCES

1. Kogda avtomobilnaia okhrannaia sistema ne mozhet byt effektivnoi. “When the car security system can not be effective”. URL: ugona.net/article/ugon-paukom-kak-zashchititsia-368.html (date of application: 25.10.2018) [in Russian].
2. Testiruiem kontrol kanala sviazi na sovremennykh sihnalizatsiyakh. “We test the control of the communication channel on modern alarms”. URL: ugona.net/article/ugon-glushilkoi-testiruem-kontrol-kanala-sviazi-359.html (date of application: 26.10.2018) [in Russian].
3. Agent Ekspert. Pandora Ekspert. Starlayn Ekspert. URL: ugona.net/catalog/alarm/starline/expert-3513.html (date of application: 26.10.2018) [in Russian].
4. Osnovnymi sposobami zashchity. “The main methods of protection”. URL: ugona.net/article/testiruem-bezopasnost-podzemnogo-parkinga-i-shtatku-mersedes-gls-355.html (date of application: 27.10.2018) [in Russian].
5. Metody ispolzuiut na praktike uhonshchiki “Methods are used in practice hijackers”. URL: ugona.net/article/test-shtatnoi-okhrannoi-sistemy-bmw-x6-f16-353.html (date of application: 25.10.2018) [in Russian].
6. Bekdor, backdoor – programma polucheniya povtornoho dostupa. “Backdoor, backdoor – re-access program”. URL: ugona.net/article/schema-ugona-nissan-kashkai-kakikh-ozhidat-ugroz-351.html (date of application: 26.10.2017) [in Russian].

UDC 629.331.047

V.A. Bilohurov,
Senior Researcher, State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0003-1896-0782,
K.V. Zaichko,
Postgraduate, Head of the Department, State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-5987-3197,
D.S. Nazarok,
Senior Researcher, State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0002-3000-4534

DEVELOPMENT OF ACCESS CONTROL SYSTEMS FOR VEHICLES

The paper deals with the confrontation between means and methods of illegal possession of vehicles or their disassembly, and means, which prevent the beginning of

unlawful actions, and also hinder their completion. The subjects of consideration were mechanical devices, which blocked the opening of the door, hood, trunk of the vehicle, blocked the steering shaft, shaft gearbox to prevent theft. Automobile alarms without remote control and their vulnerability to the attacker are considered, possible ways to bypass signaling.

With the development of threats to the property of citizens in the market began to appear means and technology in the field of protection against robbery. Over time, certain stages of development take place in the development of technology. The appearance of movable property such as motor vehicles has, to a certain extent, accelerated the development of protection. One of the areas of protection technology can be the protection of domestic and industrial premises, the protection of motor vehicles and etc.

In the early stages of development, locking devices with physical keys were widely used. The history of the use of padlocks has almost a century history.

The next stage in the development of access systems can be considered the emergence of alarms, which were included in the case of unauthorized entry into the vehicle. It should be referred to as mechanical and electromechanical devices with sirens and capacitive sensors, sensors for opening contacts or breaking the glass (vibrations) of the vehicle. The further direction in improving both ergonomic properties and increasing the stability from the influence of intruders can be considered the introduction of automotive signaling remote action.

The article deals with the codes of increased stability: the double dynamic code D-2, the double dynamic code D-square, DID technology used in transponders-tags, through which the security system recognizes the owner. The dynamic code Time Code, in which the signal is encoded Radiant, contains information with a time label. The basic principles of signal coding are defined - Keeloq Code Hopping. The means of breaking alarms using the radio scanner, grader is considered.

The functional and technical specifications of the modern remotely controlled car alarm system with multichannel control (8192 channels) and increased immunity from breaking code (DUPLEX DIALOG) and possibility of control from any point of the world (Bilarm GPS / GSM) are presented.

Keywords: access control, encoder

Отримано 01.11.2018
Рецензент Марченко О.С., к.т.н.