УДК 004.94 DOI 10.36910/6775.24153966.2021.71.7

В. М. Лазебний
Український науково- дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
ORCID ID: 0000-0002-2597-8203

ВПЛИВ РОЗРОБОК НОВИХ ЗАМКІВ (ЗАМИКАЮЧИХ ПРИСТРОЇВ) НА КІЛЬКІСТЬ ЗЛОМІВ

У статті досліджується вплив розробок замикаючих пристроїв на загальну кількість зломів. Визначено проблематику захисту домогосподарств, встановлено роль захисних пристроїв у загальній системі ефективного захисту. Запропоновано чотири категорії захисту домогосподарств: повна відсутність безпеки; рівень безпеки менше базової (встановлено один пристрій); основний рівень безпеки (встановлено віконні та дверні замки); рівень безпеки посилений (комплексний захист). Сформовано поняття замикаючого пристрою. Підкреслено, що сучасні розробки замикаючих пристроїв ґрунтуються на електронній базі. До новітніх розробок варто віднести: електрозамки, соленоїдні замки, замки з електроблокуванням, електромагнітні замки, електромеханічні замки, кодові замки, біометричні замки і деякі інші різновиди замків, які працюють від електрики або пов'язаних з електронікою. Досліджено принцип дії електронних замикаючих пристроїв, який засновано на здатності даного пристрою сприймати за допомогою датчиків і зчитувачів сигнали від певних носіїв інформації. Наведено конструкцію типового електронного замикаючого пристрою з детальним описом алгоритму функціонування. Запропоновано структурну схему замикаючого пристрою на основі мікроконтролера та обґрунтовано принцип дії. Розкрито функціональну складову замикаючого пристрою на батарейках та інтегрованим Wi-Fi на базі бездротового мікроконтролеру і драйвера двигуна постійного струму з наведенням структурної схеми. Здійснено детальний опис можливих варіантів злому наведених пристроїв та виконано аналіз впливу нових замків на кількість зломів. Наголошено, що розробка сучасних замків рухається швидкими темпами, з кожним роком відбувається модернізація кожного попереднього варіанту, додаються нові елементи та механізми захисту. Проте, в той же час, злочинці та хакери вишукують новітні методи впливу на замикаючі пристрої. Зазначено, що одним з пріоритетних напрямків захисту є комбінований захист, який у сукупності, дає більш ефективний захист та безпеку.

Ключові слова: *замок, злом, крадіжка, замикаючий пристрій, криптографія, напад, майно, сенсор, мікроконтролер.*

В.Н. Лазебный

ВЛИЯНИЕ РАЗРАБОТОК НОВЫХ ЗАМКОВ (ЗАПИРАЮЩИХ УСТРОЙСТВ) НА КОЛИЧЕСТВО ВЗЛОМА

В статье исследуется влияние разработок запирающих устройств на общее количество взломов. Определены проблематику защиты домохозяйств, установлена роль защитных устройств в общей системе эффективной защиты. Предложено четыре категории защиты домохозяйств: полное отсутствие безопасности; уровень безопасности меньше базовой (установлена одно устройство) основной уровень безопасности (установлен оконные и дверные замки) уровень безопасности усиленный (комплексная защита). Сформировано понятие запирающего устройства. Подчеркнуто, что современные разработки запирающих устройств основаны на электронной базе. К новейшим разработкам следует отнести: электрозамка, соленоидные замки, замки с электроблокировкой, электромагнитные замки, электромеханические замки, кодовые замки, биометрические замки и некоторые другие разновидности замков, которые работают от электричества или связанных с электроникой. Исследована принцип действия электронных запирающих устройств, основанный на способности данного устройства воспринимать с помощью датчиков и считывателей сигналы от определенных носителей информации. Приведены конструкцию типичного электронного запирающего устройства с подробным описанием алгоритма функционирования. Предложена структурная схема запирающего устройства на основе микроконтроллера и обоснованно принцип действия. Раскрыто функциональную составляющую запирающего устройства на батарейках и интегрированным Wi-Fi на базе беспроводного микроконтроллера и драйвера двигателя постоянного тока с указанием структурной схемы. Осуществлено детальное описание возможных вариантов взлома приведенных устройств и выполнен анализ влияния новых замков на количество взломов. Отмечено, что разработка современных замков движется быстрыми темпами, с каждым годом происходит модернизация каждого предыдущего варианта, добавляются новые элементы и механизмы защиты. Однако, в то же время, преступники и хакеры выискивают новые методы воздействия на запирающие устройства. Отмечено, что одним из приоритетных направлений защиты является комбинированный защита, в совокупности, дает более эффективную защиту и безопасность.

Ключевые слова: *замок, взлом, кража, запирающее устройство, криптография, нападение, имущество, сенсор, микроконтроллер.*

V. Lazebnyi

INFLUENCE OF DEVELOPMENT OF NEW LOCKS (LOCKING DEVICES) ON THE NUMBER OF BREAKS

The article investigates the influence of locking device developments on the total number of breakages. The problems of household protection are determined, the role of protective devices in the general system of effective protection is established. Four categories of household protection are proposed: complete insecurity; security level is less than the basic one (one device is installed); basic level of security (installed window and door locks); the level of security is strengthened (complex protection). The concept of a locking device is formed. It is emphasized that modern developments of locking devices are based on electronic base. The latest developments include: electric locks, solenoid locks, locks with electroblocking, electromagnetic locks, electromechanical locks, combination locks, biometric locks and some other types of locks that run on electricity or related to electronics. The principle of operation of electronic locking devices is investigated, which is based on the ability of this device to receive signals from certain media with the help of sensors and readers. The design of a typical electronic locking device with a detailed description of the operation algorithm is given. The structural scheme of the closing device on the basis of the microcontroller is offered and the principle of action is substantiated. The functional component of the battery-operated locking device and integrated Wi-Fi based on a wireless microcontroller and a DC motor driver with a block diagram are revealed. A detailed description of possible options for breaking these devices and analyzes the impact of new locks on the number of breaks. It is emphasized that the development of modern locks is moving rapidly, every year there is a modernization of each previous version, new elements and protection mechanisms are added. However, at the same time, criminals and hackers are looking for the latest methods of influencing locking devices. It is noted that one of the priority areas of protection is combined protection, which together provides more effective protection and security.

Key words: *lock, burglary, theft, locking device, cryptography, attack, property, sensor, microcontroller.*

Постановка проблеми. На сьогодні, в умовах тривалої економічної кризи, одними з найбільш поширених і суспільно небезпечних різновидів злочинної діяльності є крадіжки чужого майна. Беззаперечно, кожен власник формує дієву систему захисту власного майна, проте у своїй більшості, крадіжки відбуваються в умовах неочевидності і в ході їх розслідування виникають значні труднощі в отриманні відомостей, про особу, що вчинила злочин, і обставин, які спричинили його вчинення. Одним з найбільш небезпечних різновидів крадіжок чужого майна є крадіжки з помешкань або сховищ, оскільки вони часто пов'язані з підготовкою до злочинного посягання і подолання перешкод. Такі крадіжки скоюються особами, що мають значний злочинний досвід і кваліфікацію. Найбільш поширеним способом протидії вчиненню крадіжок, що використовується простими громадянами, є установка міцних, або навіть броньованих дверей, оснащення їх найсучаснішими, надійними і складними замикаючими пристроями. Загалом безпека залишається на розсуд власника, на сьогодні не існує еквівалентної вимоги щодо охорони домогосподарств.

Аналіз останніх досліджень і публікацій. Дослідженню питання зломів приміщень при встановленні на них замикаючих пристроїв присвятило власні праці чимало як зарубіжних так і вітчизняних вчених.

І. К. Російський [1] розкрив тактику огляду приміщень магазинів при розслідуванні крадіжок. Автором зосереджено увагу на основних організаційних і тактичних прийомах проведення огляду на підготовчому та робочому етапах. Зазначено об’єкти, на які потрібно звертати увагу при огляді, інформацію, що може бути отримана при їх дослідженні, а також правила їх вилучення та зберігання.

Використання спеціальних знань підчас розслідування грабежів і розбоїв розкрив П. Ю. Кравчук [2]. Автором розкрито типи запираючих пристроїв та механізми їх встановлення на об’єктах.

Стосовно криптографічного шифрування варто відмітити роботу Д. М. Курбанмурадова, В. Ю. Соколова та В. М. Астапеню [3]. Науковці підійшли до питання реалізації протоколу шифрування XTEA на базі безпроводових систем стандарту IEEE 802.15.4. У роботі вирішене завдання безпечності передачі даних в системах типу IEEE 802.15.4 на пристроях Pololu Wixel, наведені приклади апаратно-програмної реалізації шифрування і розшифрування різними пристроями на одній платформі. Запропоновані підходи можуть бути використані при розробці, впровадженні та експлуатації безпроводових корпоративних, промислових та персональних систем.

В. Ю. Корольов, М. І. Огурцов та О. М. Ходзінський [4] проаналізували загрози для сучасних криптографічних алгоритмів, викликані реалізацією алгоритмів Гровера і Шора на квантових комп'ютерах (КК). Дослідили криптографічні алгоритми, стійкі до атак за допомогою КК та надано рекомендації до застосування класичних алгоритмів – нові довжини ключів шифрування для СДВ.

Розробку протоколу захищеного обміну даними для спеціальних мереж запропонував М. І. Огурцов [5]. Автор детально описав підходи до шифрування даних що передаються по спеціальних мережах та здійснив обґрунтування криптографічного захисту сигналів з обмеженням доступу.

Із зарубіжних авторів варто відзначити такі роботи як: Chenery, S. and Pease, K. [6], Grimes R.A. [7], Van Dijk, J., Tseloni, A. and Farrell, G. [8], Vollaard, B.A. and van Ours, J.C. [9], Tilley, N., Tseloni, A. and Farrell, G. [10], Murphy, R. and Eder, S. [11], Grove, L.E., Farrell, G., Farrington, D. and Johnson, S.D. [12] та інші.

Основна увага науковців присвячена питанню розробки, модернізації та впровадження новітніх замикаючих пристроїв, однак мало уваги приділено ефективності їх застосування, саме тому питання розгляду впливу розробок нових замків на кількість зломів є актуальним та потребує детального опрацювання.

Постановка завдання. Дослідити вплив розробок нових замків (замикаючих пристроїв) на кількість зломів

Викладення основного матеріалу дослідження. Протизломна безпека домогосподарств існує у різних формах, і є неоднозначні докази про її ефективність: здається, що деякі пристрої ефективніші у запобіганні крадіжок, ніж інші. Можливою причиною очевидних змішаних висновків є те, що пристрої безпеки часто згруповані разом або аналіз, проводиться просто на підставі наявності чи відсутності, скажімо, охоронної сигналізації, мало враховуючи існування інших пристроїв. Це ускладнює точне визначення захисної ролі окремих захисних пристроїв або різних можливих комбінацій.

Із загального переліку захисних пристроїв, що існують на сучасному ринку, найбільш затребуваними та ефективними є охоронна сигналізація, відео спостереження, віконні розумні замки, блокування на двері та інші.

У своїй сукупності, безпека домогосподарств угрупована у чотири категорії:

1) повна відсутність безпеки;

2) рівень безпеки менше базової (встановлено один пристрій);

3) основний рівень безпеки (встановлено віконні та дверні замки);

4) рівень безпеки посилений (комплексний захист).

За свою суттю замикаючий пристрій – це спеціальний виріб, який слугує для замикання об'єктів різного призначення, що має відповідну комбінацію замикаючих елементів, які забезпечують блокування цього пристрою і є такими, що керуються електроприводом, в дію який приводиться певного роду носієм електронної, біометричної та іншої інформації, за допомогою датчика або складальної клавіатури.

Сучасні розробки замикаючих пристроїв ґрунтуються на електронній базі. До новітніх розробок варто віднести: електрозамки, соленоїдні замки, замки з електроблокуванням, електромагнітні замки, електромеханічні замки, кодові замки, біометричні замки і деякі інші різновиди замків, які працюють від електрики або пов'язаних з електронікою. В основі електронних замикаючих пристроїв лежить механізм, який приводиться в дію за допомогою спеціального електронного пристрою. Сутність пристрою залежить від виду замка. Замки, у свою чергу поділяються на панель набору коду, електронний «ключ-таблетка», магнітну картку або картку, оснащену мікрочіпом, біометричний розпізнаючий пристрій, такий як сканер відбитків пальців, а в особливих випадках і сітківки ока або ж пульт дистанційного керування, що передає або інфрачервоний, або радіосигнал.

Принцип дії електронних замикаючих пристроїв заснований на здатності даного пристрою сприймати за допомогою датчиків і зчитувачів сигнали від певних носіїв інформації. В якості

таких можуть використовуватися магнітні картки, штрих-коди або датчики контактної пам'яті, біометричні датчики. Конструкція типового електронного замикаючого пристрою наведена на рисунку 1.

Основними елементами конструкції типового електронного замикаючого пристрою є: виконавчий механізм, приймально-передавальний пристрій, перетворювач частоти, радіоприймальний пристрій.

Принцип складання схеми монтажу і підключення електронного замикаючого пристрою наступний: по-перше, встановлюють приймальний пристрій і блок живлення, який буде подавати напругу на виконавчий пристрій, по-друге, встановлюється кабель, що підводиться до панелі, а від блока живлення до виконавчого пристрою. Однак останнім підключення виконується з петлею до задньої частини радіоприймального пристрою.

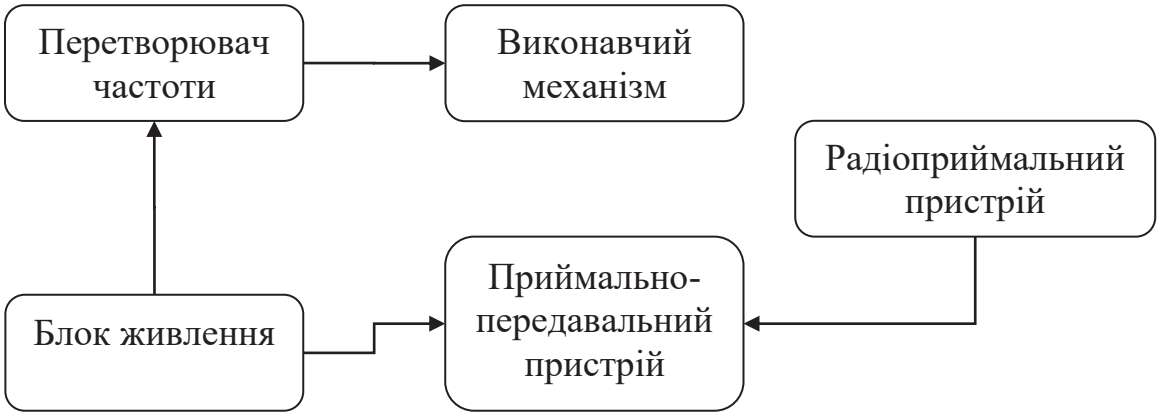

Рис.1 **Конструкція типового електронного замикаючого пристрою**

Один з живильних кабелів розмикається контактом управління панелі, другий – залишається вільним. При такому підключенні виходить, що після натискання кнопки здійснюється управління замикаючим пристроєм. З відеомонітора надходить імпульс на радіоприймальний пристрій, який, в свою чергу, замикає внутрішнє реле і на замок подається напруга – замикаючий пристрій відкривається.

Електронний замок працює наступним чином: в момент знаходження поблизу замку одного з видів ключів, що представляє собою засіб для кодування, від замку надсилається сигнал, частота якого перетворюється ключем і відсилається назад. Сигнал зі зміненою частотної модуляцією надходить в приймаючий пристрій, який налаштовано саме на цю частоту. За умови збігу частот електронний замок відкривається [5]. Одним з найважливіших показників надійності електронного замка є рівень його захищеності від перешкод. Головною умовою ефективного захисту є застосування досить складного виду сигналів, так званих електромагнітних хвиль фазової модуляції. Їх основна перевага – енергетична і структурна скритність. Звичайні моделі електронних замків виготовляються із застосуванням мікросхем, а найбільш сучасні – на основі мікроконтролерів і сенсорів. Структурна схема замикаючого пристрою на основі мікроконтролера наведена на рисунку 2.

Алгоритм роботи замикаючого пристрою на основі мікроконтролера ґрунтується на формуванні блоку імпульсів живлення, при дії яких відбувається ініціалізація змінних. Для зберігання адреси осередків пам'яті з поточною введеною цифрою коду використовується регістр, для кількості спроб введення – пам'ять даних. Потім вимикаються світлодіод і динамік установкою в відповідних бітів порту. Налаштовується таймер, який буде далі використовуватися для формування програмної затримки. Режим – 16-бітний таймер. Далі задається адреса для першої цифри коду і кількість спроб введення.

Введення коду проводиться за допомогою опитування клавіатури і реєстрації натискань клавіш. Клавіатура опитується в нескінченному циклі. При виявленні натискання кнопки, щоб уникнути реєстрації декількох натискань викликається підпрограма формування тимчасової

затримки тривалістю 5 мікросекунд. Після відпускання кнопки відбувається запам'ятовування введеного значення і повернення в цикл опитування клавіатури, якщо ще не всі цифри введені.

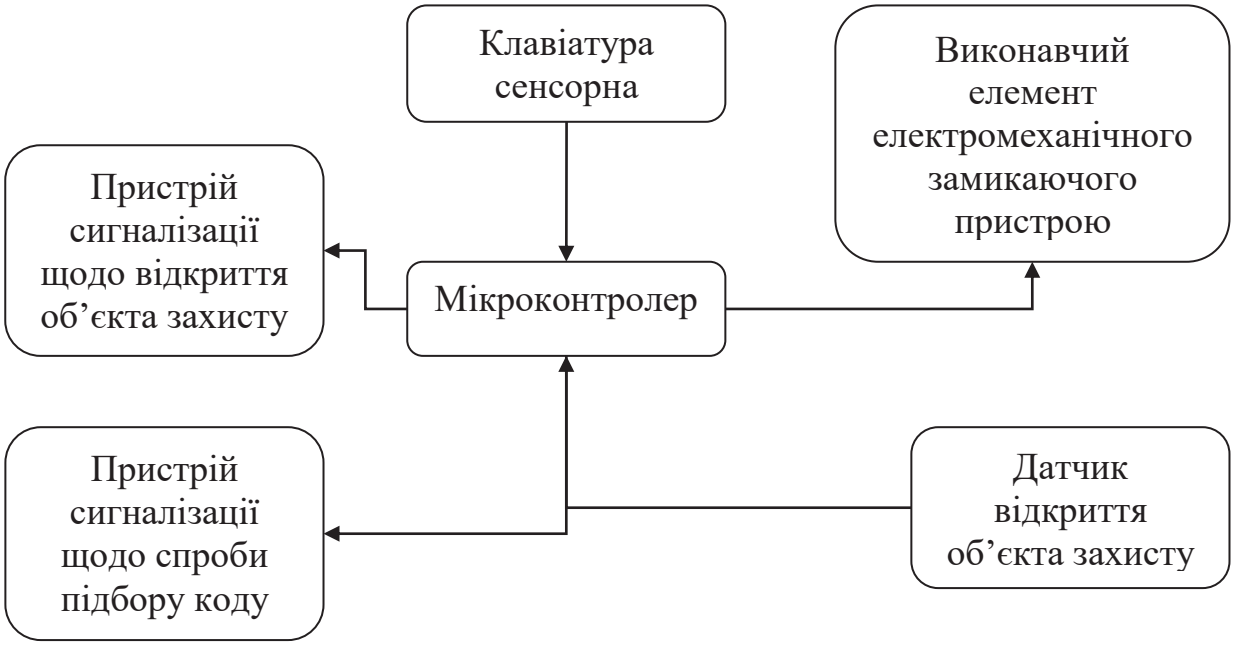

Рис. 2. **Структурна схема замикаючого пристрою на основі мікроконтролера**

У разі введення всіх цифр коду, проводиться послідовна перевірка, починаючи з останньої (code_wrong). У разі, якщо всі спроби введення витрачені, включається звуковий сигнал тривалістю 1 секунд. Для формування затримки використовується підпрограма delay. Під час дії звукового сигналу пристрій не реагує на натискання клавіш. Підпрограма реалізації тимчасової затримки використовує метод програмних циклів. При цьому в певний робочий регістр завантажується число, яке потім в кожному проході циклу зменшується на 1. Так триває до тих пір, поки вміст робочого регістра не стане рівним нулю, що інтерпретується програмою як момент виходу з циклу. Час затримки при цьому визначається числом, завантаженим в робочий регістр, і часом виконання команд, що утворюють програмний цикл.

Однією з найіноваційніших розробок сьогодення є замикаючий пристрій на батарейках та інтегрованим Wi-Fi на базі бездротового мікроконтролеру і драйвера двигуна постійного струму. Структурна схема такою пристрою наведена на рисунку 3.

Замикаючий пристрій на батарейках з інтегрованим Wi-Fi на базі бездротового мікроконтролера і драйвера двигуна постійного струму показує, як створити рішення на основі мікроконтролера (з підсистемою зв'язку по Wi-Fi), який управляє драйвером двигуна електронного інтелектуального замикаючого пристрою. Представлена розробка також демонструє варіант підключення до Wi-Fi-мережі через завдання початкових налаштувань за допомогою смарт Bluetooth і використання послідовної шини даних для зв'язку інтегральних схем за для взаємодії з блоком MEMS-датчиків інерційного вимірювального пристрою.

Від системи потрібні максимальний час автономної роботи і низька ціна обслуговування. В існуючих системах на батарейках вимога енергоефективності часто ускладнює використання нових бездротових інтерфейсів зв'язку, таких як Wi-Fi, BLE або Sub-1GHz. Впровадження бездротових інтерфейсів зв'язку може також викликати проблеми, пов'язані із забезпеченням безпеки системи. Через це вимоги щодо низького енергоспоживання і наявності вбудованих функцій безпеки – були прийняті в якості найбільш пріоритетних для новітніх розробок у сфері замикаючих пристроїв.

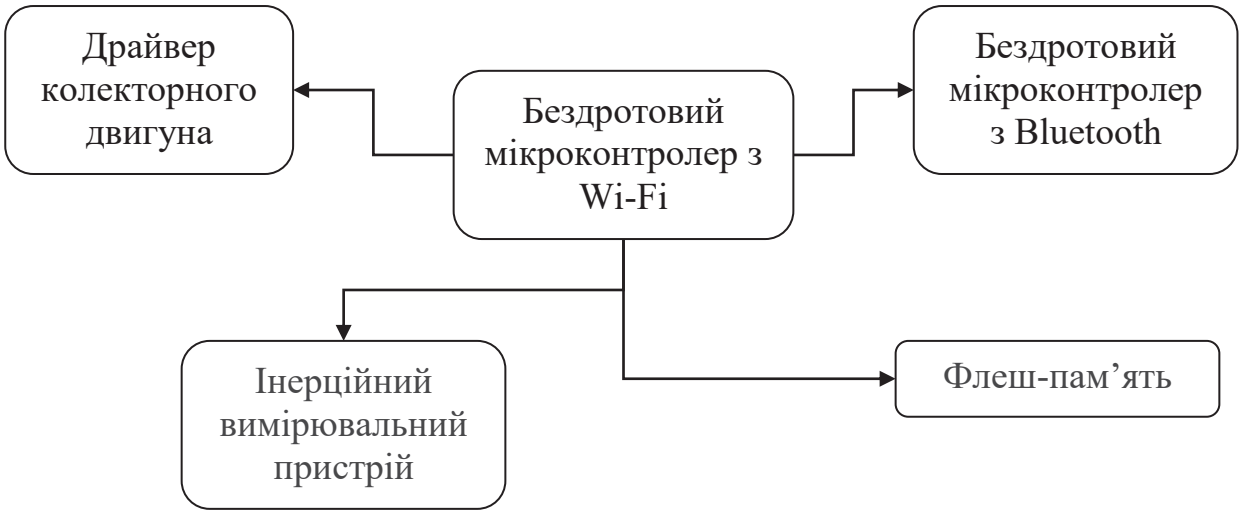

Рис. 3 **Структурна схема замикаючого пристрою на батарейках та інтегрованим Wi-Fi на базі бездротового мікроконтролера і драйвера двигуна постійного струму**

Наразі промисловістю випускаються електронні замикаючі пристрої, які мають різні види і конструкції. Кожен із таких пристроїв має певні характеристики, виходячи з принципу їх дії, області застосування, додаткових можливостей і т.д. Проте, варто відзначити, що незалежно від кількості та різноманіття розроблених замикаючих пристроїв, зломи та крадіжки продовжують відбуватися. Порушення механічної справності електронного замикаючого пристрою полягає в умисному впливі на конструктивні елементи замикаючого пристрою, що забезпечують функціонування механічної складової при наявності такої.

Руйнівний вплив інструментами можна розділити: на ударний (молоток, кувалда, сокира, перфоратор, а також інші масивні предмети); важільний (лом, монтування, плоскогубці, лещата, домкрати); ріжучий (різаки, ножі, ножиці, кусачки, кліщі та ін.); знаряддя комбінованого впливу, наприклад, ударно-ріжучі [2]. Електронний замикаючий пристрій в цілому або його конструктивні елементи піддаються впливу сильнодіючих хімічних речовин, з метою руйнування або ослаблення механічної складової пристрою.

Створення імпульсів високої напруги виводить з ладу інтегральну мікросхему, електронного замикаючого пристрою, подаючи на нього імпульси струму вище допустимих. При цьому використовуються імпульсні джерела енергії з напругою від кількох кіловольт та мегавольт, з імпульсними струмами від ампер та сотень кілоампер. Тривалість імпульсу – частки мілісекунд і наносекунди, частота повторення імпульсу – від одиниць та тисяч герц. Імпульсні джерела напруги включають в себе, як правило, накопичувач енергії, систему множення (трансформації) напруги, систему комутації і управління. У якості накопичувача енергії в них найчастіше використовуються ємнісні і індуктивні накопичувачі.

При відмиканні електронних замикаючих пристроїв найбільш часто використовується вплив на криптостійкість і створення електромагнітних завад. Сенс впливу на криптостійкість виражає основне призначення криптографії – захистити або зберегти в таємниці необхідну інформацію. Криптографія дає засоби для захисту інформації, і тому вона є частиною діяльності із забезпечення безпеки інформації. У разі відмикання електронних замикаючих пристроїв вплив на криптостійкість передбачає використання дешифровальних пристроїв (декодерів) з метою спрощення і зчитування коду електронного замикаючого пристрою і відмикання останнього.

Суть відмикання електронних замикаючих пристроїв шляхом створення електромагнітних завад полягає у створенні електромагнітного поля за допомогою різного роду випромінювачів радіочастотного діапазону, які впливаючи на механізм електронного замикаючого пристрою виключають можливість розпізнавання замком сигналів, що подаються користувачем з ключа або карти.

Слід також зазначити, що крім наведених у класифікації способів злому і відмикання електронних замикаючих пристроїв існують також комбіновані способи подолання даної перешкоди.

Вплив розробок нових замків (замикаючих пристроїв) на кількість зломів розглянемо на основі трьох наведених замикаючих пристроїв та варіантів можливого впливу на працездатність. До розгляду приймемо:

1) Типовий електронний замикаючий пристрій
2) Замикаючий пристрій на основі мікроконтролера
3) Замикаючий пристрій на батарейках та інтегрованим Wi-Fi на базі бездротового мікроконтролера і драйвера двигуна постійного струму

Результати дослідження наведемо у таблиці 1.

Таблиця 1

Результати дослідження

Вид злому	Типовий електронний замикаючий пристрій	Замикаючий пристрій на основі мікроконтролера	Замикаючий пристрій на батарейках та інтегрованим Wi-Fi на базі бездротового мікроконтролера і драйвера двигуна постійного струму
Порушення механічної справності	+	+	+
Руйнівний вплив інструментами	+	+	+
Впливу сильнодіючих хімічних речовин	+	+	+
Створення імпульсів високої напруги	+	+	-
Вплив на криптостійкість	-	+	+
Створення електромагнітних завад	-	+	-
Комбінування видів злому	+	+	+

Варто відзначити, що розробка сучасних замків (замикаючих пристроїв) рухається швидкими темпами, з кожним роком відбувається модернізація кожного попереднього варіанту, додаються нові елементи та механізми захисту. Проте, в той же час, злочинці та хакери вишукують новітні методи впливу на замикаючі пристрої. Одним з пріоритетних напрямків захисту є комбінований захист, який у сукупності, дає більш ефективний захист та безпеку.

Висновки і перспективи подальших досліджень. У роботі досліджено види замикаючих пристроїв та види злому сучасних замків. Вплив розробок новітніх замикаючих пристроїв на кількість зломів характеризується зменшенням кількості останніх за рахунок розробок надійних методів криптографії та обов'язкового поєднання / комбінування різнорідних замикаючих пристроїв на базі єдиного об'єкта захисту.

Перспективи подальших досліджень ґрунтуються на розробці комбінованого способу захисту приватного домогосподарства, здатного максимально мінімізувати можливість злому.

Література:

1. Російський І. К. Тактика огляду приміщень магазинів при розслідуванні крадіжок. *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право*. 2017. № 3-4. С. 113-116.

2. Кравчук П. Ю. Використання спеціальних знань під час розслідування грабежів і розбоїв : дис. ... канд. юрид. наук : 12.00.09 ; Східноєвроп. нац. ун-т ім. Л. Українки. Ірпінь, 2015. 185 с.

3. Курбанмурадов Д. М., Соколов В. Ю., Астапеня В. М. Реалізація протоколу шифрування XTEA на базі безпроводових систем стандарту IEEE 802.15.4. *Кібербезпека: освіта, наука та техніка.* 2019. №2 (6). С. 32-45.

4. Корольов В.Ю., Огурцов М.І., Ходзінський О.М. Багаторівневе державне впізнавання об'єктів та аналіз застосовності пост-квантових криптографічних алгоритмів для захисту інформації. *Кібернетика та комп'ютерні технології*. 2020. – № 3. – С. 74-84.

5. Огурцов М.І. Розробка протоколу захищеного обміну даними для спеціальних мереж. *Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. праць. Кам'янець-Подільський національний університет ім. Івана Огієнка*, 2019. Вип. 19. С. 108–113. https://doi.org/10.32626/2308-5916.2019-19.108-113

6. Chenery S., Pease K. Understanding Domestic Burglary in Leeds, Safer Leeds Executive Reprt. Unpublished. Applied Criminology Associates. April 2013.

7. Grimes R.A. Cryptography Apocalypse. Preparing for the Day When Quantum Computing Breaks Today's Crypto. John Wiley & Sons, Hoboken. 2020. p. 272. https://doi.org/10.1002/9781119618232

8. Van Dijk J., Tseloni A., Farrell G. The International Crime Drop: New Directions in Research. Basingstoke, UK: Palgrave Macmillan, 2012.

9. Vollaard B.A. van Ours J.C. (Does regulation of built-in security reduce crime? Evidence from a natural experiment. *The Economic Journal*, 2011. Vol.121(552). P. 485–504.

10. Tilley, N., Tseloni, A. and Farrell, G. (2011) Income disparities of burglary risk: Security availability during the crime drop. *British Journal of Criminology*. Vol. 51(2). P. 296–313.

11. Murphy R., Eder S. Acquisitive and other property crime. In: Crime in England and Wales 2009/10: Findings from the British Crime Survey and police recorded crime. *Home Office Statistical Bulletin*. 2010. Vol. 12/10. P. 79–107.

12. Grove L.E., Farrell G., Farrington D., Johnson, S.D. Preventing Repeat Victimization: A Systematic Review. The Swedish National Council for Crime Prevention (BRA: Brottsförebyggande rådet). Stockholm, Sweden: BRA, 2012.