Також причепна система має дешевшу ціну у порівнянні із повноцінними автомобілями, обладнаними для перевезення ВНП, і тому у випадку несанкціонованого спрацювання понесе менші збитки державі.

Загалом, використання причепних систем для перевезення ВНП має широке застосування у розвинених країнах світу. Також використання таких систем призведе до розумного підходу та безпеки проведення транспортування вибухонебезпечних предметів, і може зберегти людські життя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСНС: в Україні заміновані 30% території, за площею – це дві Австрії URL: https://www.ukrinform.ua/rubric-ato/3617335-dsns-v-ukraini-zaminovani-30-teritorii-za-ploseu-ce-dvi-avstrii.html]

2. Інструкція з організації та проведення робіт з розмінування місцевості на території України підрозділами та спеціалізованими підприємствами МНС, затверджена наказом МНС від 20.09.2010 № 791;

3. Спеціальні транспортні засоби для забезпечення робіт з розмінування та перевезення вибухонебезпечних предметів: довідкове видання / упор.: М. Г. Вербенський, В. О. Криволапчук, М. П. Будзинський, В. П. Бакал та ін. Київ, 2021. 90 с.

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету №4
Харківського національного університету внутрішніх справ

ВИКЛИКИ ТА ПЕРСПЕКТИВИ ПОКРАЩЕННЯ КІБЕРБЕЗПЕКИ І ЗАХИСТУ ВІД ВИКРАДАННЯ СУЧАСНИХ АВТОМОБІЛІВ

Вступ. У зв'язку з широким використанням інформаційних технологій, кібератаки та спроби несанкціонованого втручання та фізичного викрадення автомобіля, стають все більш загрозливими. Такі кібератаки часто виходять за рамки кібербезпеки і несуть загрозу фізичного характеру. Їх всебічне

проникнення фактично призвело до появи не тільки фінансових загроз, а й дій, пов'язаних зі здоров'ям, і самим життям людей. Технології захисту з кожним новим поколінням все більш удосконалюються, і автомобіль стає все більш складним та комп'ютеризованим [1].

Викладення основного матеріалу. Автомобільна кібербезпека – це виклик сучасності для виробників автомобілів. Згідно міжнародному стандарту інженерії комп’ютерної безпеки дорожніх транспортних засобів ISO/SAE 21434:2021, що призначений допомогти виробникам [2], кожен комунікаційний інтерфейс і компонент може бути потенційною точкою атаки для кіберзлочинців.

На сьогодні в автомобільній індустрії кібербезпека забезпечується як апаратними, так і програмними рішеннями, але потрібно пройти довгий шлях, перш ніж усі електронні блоки керування (ЕБК) в автомобілях будуть захищені від активності кібератак. Кібербезпека в автомобільному будівництві значно складніша, ніж на смартфонах і персональних комп’ютерах, з двох основних причин:

а) існують десятки ЕБК у кожному автомобілі, з’єднані множиною електронних шин і відповідають за різні функції та характеристики, навіть у одному і тож самому автомобілі (Volkswagen) кількість ЕБК значно різниться в залежності від комплектації;

б) існує множина потенційних точок доступу як розташованих всередині автомобіля, так і віддалених, зокрема: OBDII, USB та SD порти, безключовий доступ, Bluetooth і Wi-Fi, вбудований модем, датчики, інфотейнмент або застосунок для смартфонів, а також множина підключень із використанням телеметричних та інших хмарних систем, що мають доступ до систем автомобіля.

Питання кіберзахисту мають пріоритетне значення, але серед них особняком стоять питання захисту автомобілів від угону. Сучасні автомобілі - це дуже складні технічні комплекси, виробники охоронних систем постійно впроваджують нові опції, щоб забезпечити високий рівень їх захисту. Як абсолютно вірно, відзначає, експерт з інформаційної безпеки компанії DQS Хольгер Шмекен, краще використовувати

комбінацію з кількох захисних систем - як механічних, так і електронних [3].

Сьогодні автомобіль часто містить більше 40 модулів, з'єднаних за допомогою controller area network (CAN) шині, таких як спідометр, тахометр, різні термометри і датчики тиску. Інформація з них дозволяє отримати дані про швидкість, прискорення, тиск у шинах, стан дороги, відстань до інших учасників руху та стан водія [4]. CAN-шина - це двопровідна, послідовна, асинхронна шина з рівноправними вузлами та придушенням синфазних перешкод, з гарним співвідношенням "ціна/продуктивність". Вона дуже багато успадковує від локальних комп'ютерних мереж, але тільки в дещо урізаному вигляді. Тому, що насамперед ставиться висока швидкість, а зовсім не захищеність [5].

До методів захисту CAN-шин автомобілів від стороннього втручання можна віднести наступні:

1. Захист фізичними замками: це може бути захист проводів спеціальними кронштейнами які запобігають вирізанню проводів, чи демонтажу спеціальних блоків пам'яті (наприклад, EEPROM), які захищають важливі дані системи автомобіля.

2. Використання шифрування даних, що передаються по CAN-шині автомобіля, це запобіжить їх використання сторонніми особами.

3. Використання фільтрів для блокування небажаних повідомлень на CAN-шинах.

4. Використання контрольних сум для перевірки цілісності повідомлень на CAN-шині.

5. Використання аутентифікації для перевірки автентичності повідомлень на CAN-шині.

6. Використання фізичних забезпечувальних засобів: наприклад, маркування проводів спеціальними мітками, які забезпечують ідентифікацію та унеможливлюють їх підрізання чи підміну.

7. Відключення можливості створення бездротових підключень до CAN-шини.

Висновки. Аналіз фактів угону автомобілів показує, що викрадачі постійно вигадують нові і нові методи крадіжки

автомобілів. Тому важливо максимально ускладнити процес злому, щоб злодій не захотів витрачати свій час і пішов шукати легший та доступніший об'єкт для крадіжки. Завжди до захисту транспортного засобу підходити треба комплексно. Найнадійніший спосіб убезпечити нове авто сьогодні, це встановлення додаткових систем безпеки, як механічних, так і електронних, а також паркування авто тільки в паркінгах, що охороняються. Комплексне використання механічних та електронних систем надає значно більше впевненості у безпеці автомобіля. Як показує практика, не можна бути повністю впевненим у тому, що автомобіль не зможуть або не будуть викрадати. Але застрахуватися від цього необхідно кожному автовласнику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Світличний В.А. Технічні методи захисту автомобіля від угону. Новітні технології розвитку автомобільного транспорту (16-19 жовтня 2018 р., м. Харків), Харківський національний автомобільно-дорожній університет. Харків : ХНАДУ, 2018. С. 177-180.

2. The Mission of SAE International is to advance mobility knowledge and solutions. URL: https://www.sae.org/

3. Автомобільна кібербезпека: нові обов’язкові правила. DQS | Audits und Zertifizierung | Simply leveraging Quality. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/avtomobil'na-kiberbezpeka-novi-obov’yazkovi-pravila (date of access: 30.10.2023).

4. Розумні і небезпечні: що загрожує власникам високотехнологічних автомобілів | Блог 1GB.UA. Блог 1GB.UA. URL: https://blog.1gb.ua/umnые-y-nebezopasnые-chto-ugrozhaet-vladelczam-vыsokotehnologychnыh-avtomobylej/ (date of access: 30.10.2023).

5. Canis Labs CAN Security. Canis Labs Home. URL: https://canislabs.com/cansecurity/ (date of access: 30.10.2023).