4. Сараєва І. Метод діагностики герметичності камери згорання бензинового двигуна автомобіля. Monografia pod redakcja naukowa Kazimierza Lejdy – Pzeszow, 2017. – S. 85-93.
5. Сараева И.Ю., Цапко С.С. Определение предельно-допустимых значений технического состояния цилиндра и поршня эмпирическим способом на автомобиле// Slovak international scientific journal №36, Bratislava, Slovakia. - 2019. С 36-43. (IIJIF, SIS, GIF, ISI, DIIF)
6. Сараева И.Ю., Дибров В.К. Закономерность распределения случайной величины компрессии в двигателях внутреннего сгорания/ **Scientific discussion** №38. Praha, Czech Republic. - 2019. С 48-52. (RB, SIS, DIIF).

Світличний Віталій Анатолійович к.т.н., доцент, Харківський національний університет внутрішніх справ, vit.svet@ukr.net

КІБЕРБЕЗПЕКА СУЧАСНОГО АВТОМОБІЛЯ

Сучасний автомобіль - високотехнологічна машина, що надає широкі можливості управління своїми компонентами для забезпечення більшої фізичної безпеки і комфорту. Збільшення кількості електронних пристроїв в сучасних автомобілях з провідним і безпровідним підключенням неминуче призводить до зростання вразливостей, а значить до зниження безпеки і ефективності експлуатації транспортного засобу.

Сучасні розумні автомобілі можуть багато чого: виходити в Інтернет, завантажувати звідти карти місцевості та іншу корисну інформацію, обмінюватися даними з сервісним центром і віддалено проходити профілактику. Наприклад в Європі починаючи з квітня 2018 року всі нові автомобілі що продаються, зобов'язані мати на борту систему ECall яка спрацьовує при дорожньо-транспортній пригоді і відправляє в центр екстреної служби 112 пакет інформації, який включає в себе мінімальний набір даних: дата і час активації, географічні координати, маршрут, дані про транспортний засіб і провайдера зв'язку, Одночасно автоматично встановлюється телефонний зв'язок з салоном автомобіля. Також можлива передача додаткової інформації з бортового комп'ютера автомобіля. Таким чином, обмін інформацією здійснюється в режимі реального часу 24/7/365, і потенційно автомобіль доступний невідомим вам людям або програмами. Всі блоки управління, вся топологія мережі, правила маршрутизації, завантажувачі, оновлення - все як на долоні. Крім того, ще баги і уразливості операційних систем автомобілів. Використовується кілька систем в основному це Windows, Linux, QNX, Android Найбільш поширеними є QNX і Linux, але аналітичні звіти пророкують велике зростання частки Android. Як відомо будь який софт вимагає оновлень апгрейдів і автософт - не виняток. Якщо в дорогих моделях автомобілів процедура технічно відпрацьована і доступна за замовчуванням, то в більш дешевих варіантах розумних автомобілів багато подібних можливостей заблоковані (захищені спеціальною цифровим підписом), і за їх включення потрібна додаткова платня.

Однак, на просторах даркнета розташоване безліч форумів і торгових майданчиків, на яких можна купити найрізноманітніші пристосування, програми, спеціальні модулі, які оновлюють софт, покращують роботу, обнуляють пробіг або перезавантажують подушки безпеки після аварії, і заощадити на техобслуговуванні. Або засоби діагностики і розблокування платних функцій, піратські навігаційні пакети, та інші неліцензійні аксесуари. Коштує це - в десятки разів дешевше, ніж пропонують офіційні виробники. Ці пристосування дозволяють обнулити пробіг на машинах Renault, BMW, Mercedes, Ford, Fiat та інших. Проблема полягає в тому, що після підключення такий пристрій отримує доступ до всієї системи управління автомобіля, а через смартфон до конфіденційних даних власника, рахунками, паролів і тому подібне.

Автомобіль - річ дорога, і до його безпеки потрібно підходити не менш ретельно, ніж до безпеки банківського рахунку. Зрозуміла позиція автовиробників і розробників, які намагаються своєчасно випускати на ринок додатки з новими можливостями для зручності власників машин. Однак думаючи про безпеку сучасних автомобілів не варто обмежуватися безпекою інфраструктури (серверів управління), каналами взаємодії авто і інфраструктури. Варто також звернути увагу на сторону клієнта, зокрема на додатки, які в даний момент знаходяться у користувачів. Зараз його занадто просто обернути проти його власника, і це, можливо, зараз найвужче місце, на яке можуть бути націлені зловмисники.

Кіберзагроза вже перейшла з теоретичної площини в практичну. На форумах в даркнета періодичні зустрічаються оголошення про покупку і продаж облікових записів для додатків, що працюють з підключеними автомобілями. Причому платять за них вельми щедро - набагато більше, ніж за дані вкрадених кредитних карт.

На жаль, в питанні того, щоб уберегти свій автомобіль від кіберзлочинців, потрібно розраховувати тільки на себе. Хоча вперше розумний Jeep зламали ще в 2015 році, виробники як і раніше приділяють занадто мало уваги закриттю вразливостей, і багато загрози не втрачають актуальності і зараз. Поки ситуація не змінилася, автовласникам варто пам'ятати, які заходи безпеки вони можуть прийняти самостійно, щоб зменшити ризики. Виходячи з цього дамо кілька порад спрямованих на забезпечення кібербезпеки сучасного автомобіля:

Користуйтеся тільки офіційними додатками і аксесуарами. Скупий платить двічі;

Постійно оновлюйте прошивку автомобіля на сертифікованому сервісі. Якщо для вашої моделі автомобіля вийшла нова прошивка - то це не просто так: швидше за все, вона виправляє якісь проблеми;

Перевіряйте мобільні додатки для контролю автомобіля надійним антивірусом. Так ви не пустите на смартфон непрошеного гостя, який вкраде ваші реєстраційні дані для перепродажу на чорному ринку.

Таким чином, підбиваючи підсумки сказаного вище, можна зробити висновок про те, що кібербезпека стає новим виміром якості автомобілів.