РЕФЕРАТ

Магістерська дисертація: X с., X рис., X табл., X додатків, X джерел.

Актуальність. Сучасні авто пропонують величезну кількість цифрових можливостей. Починаючи з систем безпеки, цифрового помічника і закінчуючи комфортом, авто стають все більше частиною життя людини та бізнесу. До 2020 року очікується приблизно 220 млн. авто, які будуть обладнані мережевими системами. Але разом з новими можливостями з'являються і супутні ризики. Підвищені можливості мережевих систем (Bluetooth, Wi-Fi, 4G, GPS) значно збільшують можливість маніпулювати частинами системи. Сучасні автомобілі привертають увагу кіберзловмисників або хакерів, для яких автомобіль принципово не відрізняється від стаціонарного комп'ютера, банкомата чи смартфона. Тепер недостатньо забезпечити нормальну роботу усіх компонентів автомобіля та захищати водія разом з пасажирами від ДТП. Тому є нагальна необхідність провадження системи виявлення атак для вбудованих мережевих систем автомобіля.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконувалась на кафедрі автоматизованих систем обробки інформації та управління Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського» в рамках теми «Створення засобів імітаційного моделювання дискретно-подійних систем» (Державний реєстраційний номер 0117U000923).

Мета дослідження – підвищення безпеки авто за рахунок створення системи виявлення атак.

Для досягнення мети необхідно виконати наступні **завдання:**

- зробити огляд роботи електронних компонентів управління у складі автомобіля;
- надати опис типових архітектур систем виявлення атак;
- обрати архітектуру нейронної мережі та метода навчання;
- проаналізувати здійснення атак на ЕКУ автомобіля та їх результати;

– побудувати модель загроз на основі здійснених атак;

– створити поверхні атак для ЕКУ автомобіля та надати кількісну оцінку;

– надати ознаки для моделювання ЕКУ;

– змоделювати ЕКУ та дані, що використовуються при нормальному функціонуванні та при здійсненні так;

– сформулювати загальні алгоритми здійснення атак та ознак їх здійснення;

– розробити архітектуру системи виявлення атак;

– створити програмну реалізацію системи виявлення атак;

– виконати аналіз отриманих результатів.

Об'єкт дослідження – інформаційна безпека електронних компонентів управління автомобіля та протидія загрозам.

Предмет дослідження – модель загроз та поверхня атак ЕКУ автомобіля.

Методи дослідження, застосовані у даній роботі, базуються на методах машинного навчання, моделях категоризації загроз та експертних оцінок.

Наукова новизна одержаних результатів полягає у створенні моделі загроз на основі раніше виявлених атак саме на компоненти автомобіля, оцінка поверхні атак з врахуванням наслідків втручання в роботу автівки, а не лише втрати даних. Були запропоновані параметри моделювання електронних компонентів управління, ознаки виявлення аномальної поведінки в мережі автомобіля для навчання нейронної мережі та виконано виявлення анормальної поведінки нейронною мережею.

Публікації. Матеріали роботи опубліковані у двох наукових статтях «Аналіз загроз для електронних компонентів управління автомобіля в мережі CAN» (науковий журнал «INNOVATIVE SOLUTIONS IN MODERN SCIENCE»), «Оцінювання поверхні атак електронних компонентів управління автомобіля в мережі CAN» (науковий журнал «Науковий огляд») та у збірці матеріалів науково-практичній конференції «Інформатика та обчислювальна техніка-ІОТ-2018» [1].

АВТОМОБІЛЬ, ЕЛЕКТРОННІ КОМПОНЕНТИ УПРАВЛІННЯ, СИСТЕМА

ВИЯВЛЕННЯ АТАК, МОДЕЛЬ ЗАГРОЗ, ОЦІНКА ЕКУ, ПОВЕРХНЯ АТАК, МАШИННЕ НАВЧАННЯ.