Серед перспективних функцій – повна реставрація старих фотографій, видалення пилу і подряпин зі знімків, зменшення шумів на зображеннях, зроблених камерами низької якості, і навіть перетворення поганих фотографій на професійні. Також розробники обіцяють функції, що дозволять видаляти окуляри з фотографій, а ще – створювати художні малюнки на основі зображень, відкриваючи величезні можливості для творчості.

Це лише деякі приклади того, як нейрофільтри здатні змінити підхід до редагування зображень і спростити роботу як для початківців, так і для професіоналів. Майбутнє виглядає надзвичайно захопливим для тих, хто працює з графікою.

Література

1. https://ru.wikipedia.org/wiki/Нейронная_сеть
2. images(https://www.ellegirl.ru/articles/kak-povtorit-firmennyi-makiyazh-ariany-grande- so-strelkami/) (https://zen.yandex.ru/media/id/5cae10d37ce49000b3f7462f/eto-ne-defekt-plenki-realnye-fotografii-na-kotoryh-prisutstvuiut-prizraki-5cb3fcc635fb3300b328a71a) (https://www.goodfon.ru/wallpaper/priroda-gory-les-zima-nebo.html) (https://www.cosmo.ru/stars/krupnim-planom/ot-50-i-starshe-samye-effektnye-modeli-v-vozraste/) (https://ru.depositphotos.com/stock-photos/%D0%B1% D0% B5% D0%B7-%D0%BC%D0%B0%D0%BA%D0%B8%D1%8F%D0% B6%D0%B0.html)

КІБЕРБЕЗПЕКА В АВТОМОБІЛЬНОМУ ЗВ'ЯЗКУ

Мельник С.О., студент МК 51-20
Науковий керівник – ***Попова А.В.,*** доц., к.т.н.
Харківський національний автомобільно-дорожній університет

Тема кібербезпеки та електромобілів є надзвичайно актуальною в сучасному світі. Щодня питання кібербезпеки набуває все більшого значення. Сьогодні багато з нас зберігають величезні обсяги даних у своїх гаджетах, автомобілях та інших пристроях.

Всі ці дані про користувачів зберігаються на серверах компаній або в хмарних сховищах. Компанії, яким ми довіряємо наші дані, зазвичай інформують нас про те, для чого ці дані використовуються і як довго вони будуть зберігатися. Проте, навіть за таких умов, жодна компанія не може повністю гарантувати безпеку від витоків інформації.

Кібербезпека стає особливо важливою, коли мова йде про автомобілі, зокрема електромобілі, які повністю залежать від комп'ютерних систем. Відо-

мо, що через збої в комп'ютерних системах траплялися аварії, які призводили до трагедій. Це змушує задуматися про рівень безпеки таких транспортних засобів.

Ілон Маск, засновник компанії Tesla, яка виробляє екологічно чисті електромобілі, обладнує свої машини повністю цифровими панелями управління та передовими технологіями. Більше того, ці автомобілі можуть підключатися до відкритих мереж для оновлення програмного забезпечення в реальному часі. Це означає, що ваш автомобіль може автоматично зв'язуватися з іншими транспортними засобами, гаджетами та навіть з елементами навколишнього середовища. Схема за якою це працює, виглядає так:

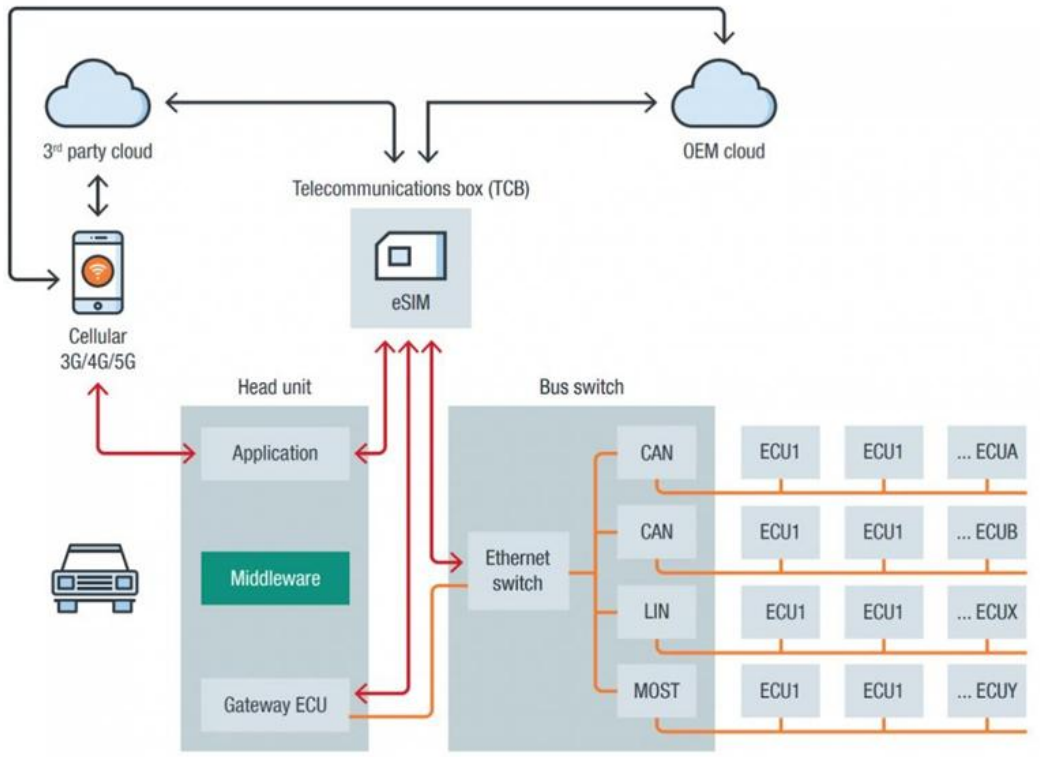

Figure 2. The cloud-connected ecosystem of a connected car

Таким чином, виникає значна проблема, яка стосується не лише автомобілів Tesla, а й інших брендів, що виробляють електрокари. Якщо хтось добре обізнаний у методах обходу захисту даних, то зламати систему стає відносно легко, що може призвести до серйозних наслідків. Втручання в такі системи є незаконним. Наприклад, у відкритому доступі можна знайти таблиці, які показують конкретні загрози, що стосуються серверів, котрі керують автомобілями під час руху.

Враховуючи надану інформацію, можна зробити висновок, що внутрішній сервер можна використовувати як інструмент для атак на транспортні засоби та викрадання даних. Якщо внутрішній сервер виходить з ладу, це вплине на функціональність автомобіля. Дані, що належать транспортному засобу, що

зберігаються на цих серверах, можуть бути втрачені або скомпрометовані (порушення конфіденційності).

Крім того, важливо знати про можливі внутрішні та зовнішні атаки, такі як: Зловживання правами доступу персоналом (внутрішні атаки), несанкціонований доступ до серверів через Інтернет, несанкціонований фізичний доступ до серверів.

Серверний сервер. Атаки на внутрішні сервери та порушення їх роботи необхідно розглядати як потенційну загрозу. Зверніть особливу увагу на інсайдерські атаки, коли співробітники можуть зловживати своїми правами доступу. Такі атаки можуть призвести до втрати даних у хмарних службах, несанкціонованого доступу до серверів через Інтернет, фізичного доступу до серверів або порушення цілісності інформації через ненавмисний обмін даними.

Top-level threat	Threat Example	D	R	E	A	D	Rating
1. Back-end servers used as a means to attack a vehicle or extract data	1.1 Abuse of privileges by staff (insider attack)	3	3	2	2	2	High
	1.2 Unauthorized internet access to the server	3	2	2	2	2	Medium
	1.3 Unauthorized physical access to the server	3	3	2	2	2	High
2. Services from back-end server being disrupted, affecting the operation of a vehicle	2.1 Attack on back-end server stops it functioning	3	2	2	2	2	Medium
3. Vehicle related data held on back-end server being lost or compromised (data breach)	3.1 Abuse of privileges by staff (insider attack)	3	3	2	2	2	High
	3.2 Loss of information in the cloud	3	2	2	2	2	Medium
	3.3 Unauthorized internet access to the server	3	2	2	2	2	Medium
	3.4 Unauthorized physical access to the server	3	3	2	2	2	High
	3.5 Information breach by unintended sharing of data	3	1	2	2	3	Medium

Як потенційні загрози варто враховувати атаки на внутрішні сервери та зупинку їхньої роботи. Особливу увагу слід звернути на інсайдерські атаки, коли працівники можуть зловживати своїми правами доступу. У результаті таких атак можлива втрата даних у хмарних сервісах, несанкціонований доступ до серверів через Інтернет, фізичний доступ до серверів або порушення цілісності інформації через ненавмисний обмін даними.

Якщо зловмисник отримує привілейований або фізичний доступ до вашого сервера, захист стає надзвичайно складним і може призвести до повної компрометації вашої системи. Хоча деякі сервери могли стати менш уразливими через різні системні оновлення, конфіденційні сервери можуть піддаватися широкому доступу через Інтернет.

Навіть у разі витоку даних у хмарі використання може бути складним, а потенційна шкода залежатиме від типу викраденої інформації та характеру її подальшого використання. Типи кібератак, які слід розглянути, включають DoS, DDoS, MITM, фішинг, фішинг, атаки з викупом, злом паролів, впровадження SQL і заміну DNS.

DoS- і DDoS-атаки полягають у перевантаженні системи запитами, що робить її недоступною для законних користувачів.

Розподілена DDoS-атака виконується проти кількох заражених комп'ютерів, контрольованих хакером. Ці атаки призводять до тимчасового припинення роботи вашого веб-сайту або служби. Атаки MITM дозволяють зловмиснику перехоплювати зв'язок між двома сторонами, часто без їх відома. Щоб захистити себе, ви можете використовувати надійне шифрування або VPN. Фішингові атаки відбуваються під виглядом законних електронних листів для отримання конфіденційної інформації. Ви можете запобігти таким атакам, ретельно перевіряючи свої електронні листи та посилання. У найближчі роки актуальність кіберзагроз зросте, особливо у зв'язку з розробкою електричних і безпілотних автомобілів, які необхідно захищати від потенційних кіберзагроз. Машинне навчання та алгоритми глибокого навчання вже використовуються для виявлення аномалій і захисту цих систем.

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СУЧАСНІЙ СИСТЕМІ ОСВІТИ

Бугай А.В., студент МК-41-21
Науковий керівник – ***Костікова М.В.,*** доц., к.т.н.
Харківський національний автомобільно-дорожній університет

Вступ.

Сучасні технології в освіті дозволяють здобувати знання дистанційно, в більшому обсязі та з меншими витратами часу і коштів. З'явилися нові способи взаємодії між викладачами та студентами. При виборі навчального закладу більше уваги приділяється якості освіти, ніж близькості закладу до місця проживання.

Вплив інформаційних технологій на освіту

Інтернет вніс свої корективи в освіту. Зміни торкнулися як методів навчання, так і підходів до організації навчального процесу.

Система освіти вступає у фазу інтеграції з глобальним інформаційним простором. Це уможливило використання сучасних методів навчання, які стали більш комфортними та доступними.