Полковников Владислав Павлович,
курсант 222 учебной группы 2 факультета,
ВУНЦ ВВС «ВВА» в г.Челябинске

Прохоренко Кирилл Денисович,
курсант 222 учебной группы 2 факультета,
ВУНЦ ВВС «ВВА» в г.Челябинске

Стасюкевич Александр Едосиевич,
преподаватель 1 кафедры филиала,
ВУНЦ ВВС «ВВА» в г.Челябинске

СОВРЕМЕННЫЙ АВТОМОБИЛЬ. НОВОЕ СРЕДСТВО СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация: В данной статье рассматривается новое средство сбора персональных данных – современный автомобиль. Рассматриваются способы сбора данных. Выявляются цели и задачи сбора данных. Рассказываются методы самозащиты от сбора персональных данных. Изучаются последствия утечки данных.

Ключевые слова: автомобиль, персональные данные, датчики, автоконцерны, злоумышленники, информация, смартфон, система, маркетинговые фирмы, выгода, сбор данных.

Современный автомобиль – это не просто средство передвижения, а скорее компьютер на колёсах. Около половины его стоимости составляет электроника и софт: сенсоры, контроллеры, компьютерные компоненты и управляющее ПО. Большая часть населения нашей планеты пользуются данным видом транспортных средств. Практически в каждой семье имеется один автомобиль, а в некоторых и больше одного [1].

К сожалению, вслед за производителями телевизоров и другой бытовой техники автоконцерны тоже открыли для себя новый источник доходов – сбор данных о своих пользователях. Современный автомобиль – это настоящий комбайн по сбору персональных данных.

Эксперты компании Mozilla проверили автомобили 25-ти крупнейших брендов – и ни один не смогли назвать безопасным. Абсолютно все они собирают и используют данные пользователя в чрезмерном количестве и страдают от уязвимостей, нарушая критерии безопасности, установленные для этого тестирования. Восемьдесят процентов брендов признают, что могут делиться персональными данными водителей с поставщиками услуг, брокерами данных и другими компаниями [4] Семьдесят процентов утверждают, что могут продавать персональные данные водителей на сторону. Что характерно, текущее законодательство не обязывает компанию отчитываться, кому конкретно и с какой целью она предоставила или продала персональные данные. Семнадцать из двадцати пяти автомобильных брендов получили дополнительный минус в графе «послужной список» за утечки, взломы и нарушения, угрожающие приватности водителей.

Современный автомобиль буквально напичкан датчиками – начиная с сенсоров в двигателе и ходовой, показывающих, например, температуру двигателя, угол поворота руля или давление в шинах, и заканчивая куда более интересными, такими как видеокамеры по периметру машины и в салоне, микрофоны, датчики присутствия рук на руле, встроенные видеорегистраторы и многое другое. Собранная информация используется в различных целях.

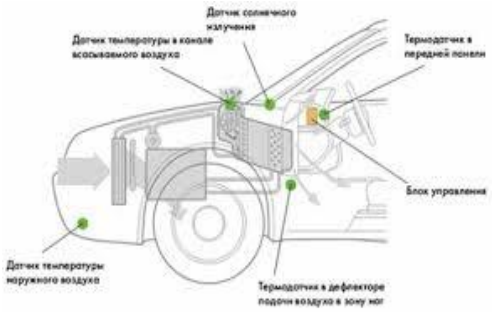

Рис.1. Датчики, встроенные в современный автомобиль

Данные от сенсоров и камер помогают предупредить водителя о возможных опасностях на дороге, а также могут автоматически активировать системы помощи, такие как экстренное торможение [3].

Навигационные системы, анализируя данные о движении, могут предлагать альтернативные маршруты, избегая пробок и сокращая время в пути. Кроме того, системы мультимедиа могут адаптироваться к предпочтениям водителя и пассажиров.

Информация о состоянии автомобиля позволяет своевременно выявлять неисправности и проводить профилактическое обслуживание, что способствует увеличению срока службы.

Собранные данные могут быть использованы для анализа поведения водителей и тенденций на рынке, что позволяет производителям улучшать свои продукты и разрабатывать новые решения.

Все датчики объединены в общую систему, поэтому головной компьютер автомобиля получает всю эту информацию централизованно. Плюс все современные автомобили оснащены GPS, модулем сотовой связи, Bluetooth и Wi-Fi. Наличие сотовой связи и GPS во многих странах продиктовано законом (для автоматического вызова помощи при ДТП), но производители охотно используют эту функцию для удобства водителя – и своего. Можно прокладывать маршрут на экране автомобиля, дистанционно диагностировать поломки, заблаговременно заводить машину [5] И, конечно, мостик «датчики и камеры → компьютер автомобиля → сотовая сеть» создает постоянный канал сбора информации: куда вы едете, где и сколько времени стоите на парковке, насколько резко крутите руль и газуете, пользуетесь ли ремнями безопасности и так далее.

Дополнительный сбор информации ведется с водительского смартфона при его подключении к бортовой системе автомобиля для совершения звонков, прослушивания музыки, навигации и прочих удобств [2] А уж если на смартфоне установлено мобильное приложение от автопроизводителя для управления функциями автомобиля, то данные можно передавать со смартфона даже тогда, когда водитель вообще не в машине.

Ну а информацию о пассажирах помогают собирать камеры и микрофоны, точки доступа Wi-Fi и функции Bluetooth [1] С их помощью легко узнать, кто постоянно ездит в машине вместе с водителем, где и когда садится и выходит, каким смартфоном пользуется и так далее.

Также современные таксопарки используют специальные приложения для просмотра местонахождения водителя, его личной информации и информации о транспортном средстве. Всё это было создано для улучшения качества сервиса такси. Но данная функция очень опасна не только для самого водителя, но и для пассажира. Взломав приложение, происходит утечка информации, персональных данных [2] Многие таксопарки для подтверждения личности, запрашивают документы, в основном это паспортные данные. В случае водителя: паспорт транспортного средства, свидетельство о регистрации транспортного средства, права на управление транспортным средством, а также текущее состояние автомобиля в виде фотографий.

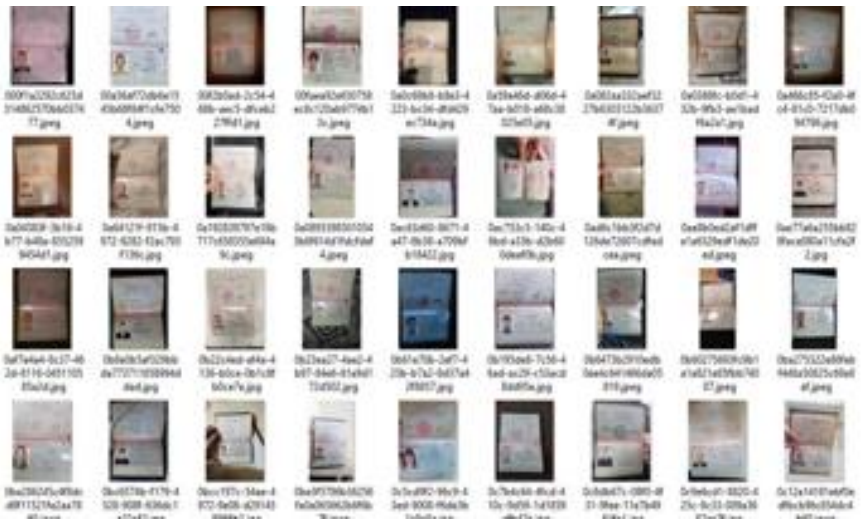

Рис.2. Пример утечки паспортных данных водителей популярного таксопарка

Злоумышленник имеет возможность просмотра маршрутов, которыми пользовался клиент таксопарка. С помощью этой информации возможно определить место работы клиента такси. Если человек в одно и то же время приезжает на определенный адрес, и уезжает через определенное время,то с вероятностью 85% это является его местом работы. Заказывая такси в рестораны, парки, театры, злоумышленник может определить свободное время и места проведения отдыха. Также возможно определить информацию о том находится ли человек в городе проживания или уехал. К примеру, если человек заказал маршрут от дома к аэропорту, а обратного не заказывал, то с вероятностью 67% человек улетел на отдых или в командировку.

Зачем эта информация производителям автомобилей? Чтобы заработать больше денег. Кроме анализа для «улучшения качества продуктов и услуг», данные могут быть перепроданы, а функции – перенастроены для большей выгоды производителя.

Продавцы страховок, например, покупают информацию о стиле вождения конкретного водителя, чтобы более точно прогнозировать вероятность ДТП и корректировать стоимость страховки. Уже в 2020 году этой неоднозначной функцией прямо на заводе были оснащены 62% автомобилей, в 2025 году рост этого показателя достиг 91%.

Маркетинговые фирмы также охотно пользуются подобными данными и таргетируют рекламу, ориентируясь на доходы, семейное положение и социальный статус владельца авто.

В военных целях сбор информации о водителе, является средством разведки. Современные автомобили всё чаще встречаются на территориях воинских частей, местах проведения испытаний, учений, а также в ходе боевых действий. Полученные данные с автомобиля будь то изображение или записанная речевая информация, могут использоваться для получения информации о составе войск, их боевой готовности, боевых планах. А в случае боевых действий потеря информации может привести к выявлению мест расположения войск.

Но как же повысить безопасность данных в автомобилях? В первую очередь необходимо улучшить кибербезопасность. Разработка и внедрение современных методов шифрования и аутентификации данных поможет защитить информацию от несанкционированного доступа. Регулярные обновления программного обеспечения также играют важную роль в устранении уязвимостей.

Следующий аспект – это прозрачность в сборе данных. Производители должны информировать пользователей о том, какие данные собираются, как они используются и с кем могут быть поделены. Чёткие и доступные условия использования данных помогут повысить доверие клиентов.

Не стоит забывать про контроль доступа. Внедрение строгих протоколов контроля доступа к данным, включая многофакторную аутентификацию, может значительно уменьшить риск несанкционированного доступа.

Обучение пользователей играет не маловажную роль. Если владельцы машин знают о рисках, связанных с использованием подключённых к интернету автомобилей, то это поможет защитить их личные данные [3].

Ещё один аспект – это функции анонимизации. Внедрение технологий, позволяющих анонимизировать собираемые данные, может помочь защитить личность пользователей, сохраняя при этом ценность информации для анализа.

Ну и, наконец, партнёрство с экспертами в области безопасности. Сотрудничество с компаниями и исследовательскими учреждениями, специализирующимися на кибербезопасности, может обеспечить доступ к передовым решениям и технологиям.

Сбор информации в автомобиле – это важный аспект, который влияет на безопасность персональных данных его владельца. Несмотря на существующие вызовы, технологии продолжают развиваться, открывая новые возможности для улучшения автомобильной индустрии и повышения качества жизни людей. Важно продолжать работу над вопросами конфиденциальности и безопасности, так как от утечки персональных данных не застрахован никто из нас. С развитием технологий, таких как искусственный интеллект сбор информации в автомобилях будет только увеличиваться. Ожидается, что автомобили станут еще более «умными», способными самостоятельно анализировать и обрабатывать информацию в реальном времени.

Список литературы:

1. Иванов, С. А. (2020). "Безопасность данных в современных автомобилях: вызовы и решения." Автомобильный журнал, 12 (3), стр. 45-52.

2.Петров, А. В. (2019). "Сбор и обработка персональных данных в автомобилях: правовые аспекты." Журнал права и технологий, 8 (2), 34-40.

3. Зайцева, Л. Н. (2020). "Проблемы безопасности данных в умных автомобилях." Научный вестник, 10 (5), 100-105.

4. Чистяков, П. В. (2022). "Технологии защиты данных в автомобилях: современные решения." Технические науки и инновации, 9 (2), 15-22.