Проблемы обеспечения информационной безопасности высокоавтоматизированных транспортных средств

Д.И.Правиков, Е.А.Пономарева, В.П.Куприяновский

***Аннотация* — В статье проводится анализ положений принятой в Российской Федерации Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования. Рассмотрены нормативные документы, определяющие развитие искусственного интеллекта как инновационной технологии. Описаны угрозы информационной безопасности современных автомобилей, показано, что с созданием беспилотного транспорта количество угроз увеличится. Проведен обзор требований к информационной безопасности беспилотных транспортных средств, сформированный на основании практики специалистов по информационной безопасности, а также соответствующих международных стандартов. Сделан вывод о необходимости детализации положений Концепции с учетом общемировых подходов к обеспечению информационной безопасности автомобилей и беспилотных устройств на их основе.**

***Ключевые слова*—Беспилотные транспортные средства, требования по безопасности.**

I. Введение

В ноябре 2019 г. опубликована информация о том, что Сбербанк, "Яндекс", Mail.ru Group, "Газпром нефть", МТС и Российский фонд прямых инвестиций создают альянс для развития искусственного интеллекта (ИИ) в России, о чем было объявлено на конференции "AI Journey 2019"[1]. В целом ИИ в России можно охарактеризовать как динамично развивающуюся область, которая получила государственную поддержку, оформленную законодательно. Так, Президент Российской Федерации В.Путин подписал указ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», которым утверждается Национальная стратегия развития ИИ до 2030 г. Уровень разработок и их практическая направленность подтверждается федеральным законом от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».

Одним из последних нормативных документов является Распоряжение Правительства Российской Федерации от 25 марта 2020 г. № 724-р, которым утверждена Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования (далее - Концепция). В указанном документе особое внимание привлек раздел «Информационная безопасность высокоавтоматизированных транспортных средств», анализ которого является предметом настоящей статьи.

В ходе анализа не только рассмотрены актуальные угрозы информационной безопасности автомобилей и других автотранспортных средств, но и приведен краткий обзор стандартов, описывающих требования к ним по информационной, так и иным видам безопасности.

II. Анализ концепции и угрозы информационной безопасности автотранспорта

A. Угрозы информационной безопасности автотранспорта

Если провести анализ вопроса информационной безопасности автомобильного транспорта, то он уже достаточно давно является предметом не только анализа, но и разработки решений по безопасности. В первую очередь это связано с тем, что для управления современным автомобилем используются электронные блоки, которые могу быть уязвимы с точки зрения информационной безопасности [1]. В различных работах, доступных в открытом доступе, приведены примеры успешного проведения телекоммуникационных атак на системы современных автомобилей[2]. Появление беспилотного автомобильного транспорта только усугубило проблему обеспечения информационной безопасности [2]. В результате к проблемам, которые

Статья получена 20 мая 2020.

Д.И Правиков, РГУ нефти и газа (НИУ) им. И.М.Губкина (e-mail: dip@gubkin.pro).

Е.А.Пономарева, АО «Лаборатория Касперского» (e-mail: Evgeniya.Ponomareva@kaspersky.com).

В.П. Куприяновский, РУТ (МИИТ) (email: v.kupriyanovsky@rut.digital).

1 https://www.interfax.ru/business/683445

2 https://habr.com/ru/post/373457/

были связаны с функционированием современных автомобилей, добавились проблемы, связанные с ними как с беспилотным транспортом. Как следствие это усложнило понимание вопросов информационной безопасности и связанных с ними соответствующих требований.

С внедрением V2X-систем задача обеспечения кибербезопасности будет усложняться, т.к. появится больше элементов в экосистеме и новые участники процесса взаимодействия с автомобилем. На рис.1 приведена общая схема экосистемы V2X с перечнем наиболее актуальных киберугроз.

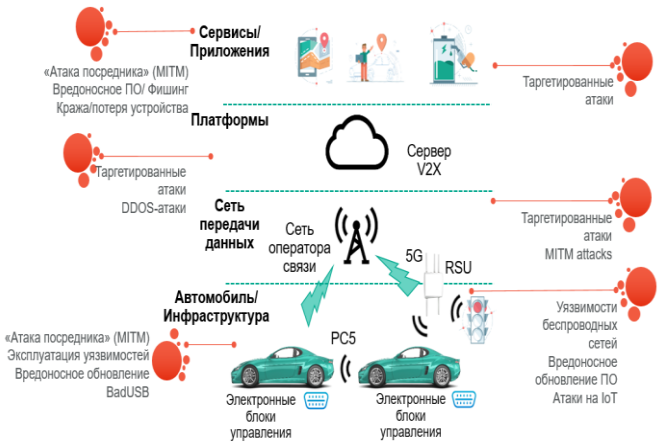

Рис. 1. Актуальные угрозы информационной безопасности автотранспорта

Фактически, злоумышленник имеет множество возможностей для получения несанкционированного доступа к системе. Например, автопроизводители фокусируются на разработке средств обеспечения кибербезопасности внутри автомобиля, но, при этом, разработке приложений, которые с ним взаимодействуют, с точки зрения информационной безопасности не уделяется должного внимания. Исследования показали, что у разработчиков приложений нет понимания текущих угроз для мобильных платформ, как при проектировании приложений, так и при создании инфраструктуры[3].

B. Анализ Концепции

В Концепции заложено интересное сочетание требований по безопасности, которое нуждается в определенной детализации и трактовке.

Первое, с чего начинается анализируемый раздел Концепции, это требование по однозначной физической идентификации пользователей беспилотных транспортных средств. Вот, например, на текущий момент пользователь услуг такси или общественного транспорта не обязан себя идентифицировать, фактически они перевозят анонимного пассажира, от которого требуется только оплатить поездку. Для беспилотного транспорта принимается совершенно другая концепция — перевозка анонимных пользователей не допускается. Сейчас в Концепции предполагается, что потенциальный пассажир предъявляет биометрические данные. При этом используется термин не идентификация, а именно аутентификация, т. е. проверка подлинности представленных данных, судя по всему, должна проводиться до момента начала поездки. Тогда, в перспективе, система оператора беспилотного транспорта должна быть подключена к единому федеральному информационному регистру, содержащем сведения о населении Российской Федерации, законопроект о котором Государственная дума 17 апреля 2020 г. приняла во втором чтении.

При этом в Концепции сразу оговаривается, что полученные персональные данные не должны быть доступны третьим лицам, следовательно, должен быть предусмотрен комплекс мер по обеспечению информационной безопасности начиная с их ввода (предъявления) в системе беспилотного транспорта и заканчивая обработкой и хранением в системе оператора беспилотного транспорта. Как минимум это подразумевает, что оператор беспилотного транспорта будет являться оператором персональных данных.

Вторым существенным требованием в Концепции является воспрепятствование подавлению или перехвату управления беспилотником. Говоря другими словами, нельзя допустить подавления функции управления или допустить возможность угона. Функцию подавления управления обсудим чуть ниже, а сейчас рассмотрим требование воспрепятствования перехвата управления беспилотным автомобилем. Здесь возможны два варианта реализации этого замысла. В первом случае злоумышленник имеет возможность подключиться к CAN-шине беспилотного автомобиля. Значит, разъем не только должен быть защищен физически, но и иметь такую систему защиты, которая сигнализирует о попытках несанкционированного физического доступа к нему. Второй вариант подразумевает исключение возможности подключения к каналу взаимодействия беспилотника к центру управления, т. е., говоря другими словами, должен различать факт проведения атаки MITM по беспроводному каналу связи. Вместе с тем, в концепции присутствует упоминание о минимизации рисков, что означает применение риск-ориентированного подхода к перехвату управления. Говоря другими словами, Концепция, тем не менее, закладывает вероятность риска перехвата управления беспилотным автомобилем, что на статистическом объеме означает принятие возможного ущерба, связанного с их угоном.

Что обращает на себя внимание при анализе указанного раздела Концепции, это одновременное использование терминов «информационная безопасность» и «кибербезопасность». При этом последний термин употребляется в контексте того, что информационная безопасность обеспечивается «не только за счет дополнительных систем защиты, но и на основе максимального исключения принципиальной

3 https://securelist.ru/a-study-of-car-sharing-apps/90804/

возможности вмешательства, физической невозможности управления движением извне, например передачи дистанционного управления внешнему оператору только посредством ручного переключателя». В данном случае подход интересно сравнить с подходом к обеспечению комплексной безопасности АСУ ТП, включающем в себя функциональную безопасность, операционную (промышленную - в терминах российской нормативной базы) безопасность и кибербезопасность [3]. Судя по всему, требования по функциональной, промышленной, кибербезопасности сохраняются для беспилотного автотранспорта, при этом в части кибербезопасности выделяются требования невозможности перехвата управления.

Следующий ключевой момент в Концепции: «обязательным требованием является своевременное и быстрое уведомление водителей о наличии угроз информационной безопасности. Поскольку устранение угрозы или последствий взлома займет некоторое время, водитель или автоматизированная система вождения должны предпринимать корректирующие действия.» С точки зрения специалистов по информационной безопасности АСУ ТП принята концепция, согласно которой проявление факта поражения системы не отличимо от сбоя в следствии физического износа, поломки и т. п. Выявление кибератаки является следствием анализа инцидента, проводящегося, как правило, апостериори. Результатом атаки может быть, например, отказ тормозной системы. На промышленных предприятиях минимизация последствий инцидента (чем бы он не был вызван) в основном реализуется функцией корректного останова. Значит такая концепция должна быть реализована в беспилотных автомобилях, а дороги на всем протяжении должны быть оборудованы специальными «карманами» по типу «ловушек» на горных дорогах.

C. Нормативные требования по безопасности

Учитывая, что, как указано в Концепции, «отчет о кибербезопасности на основе унифицированных стандартов должен быть одним из документов, необходимых для допуска высокоавтоматизированного транспортного средства к эксплуатации», рассмотрим те стандарты, которые применяются к безопасности автотранспортных средств, указанные, в частности в [4].

Вопросы функциональной безопасности рассматриваются в серии стандартов ISO 26262, которая, судя по имеющимся данным, была существенно обновлена в 2018 г. В данной серии ключевым, с точки зрения понимания формируемых подходов, является стандарт ISO 26262-10 Second edition 2018-12 Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262, в котором представлен обзор других стандартов серии и даются дополнительные пояснения. Вопросы безопасности рассматриваются на основе подходов стандарта 61508 и в плане информационной безопасности, фактически сводятся к корректности и надежности программного обеспечения.

Вопросы промышленной (в данном контексте пожарной) безопасности автотранспорта рассматривались в [5]. Исходя из формирующихся подходов, можно предполагать, что беспилотный автотранспорт должен быть оборудован автоматическими средствами пожаротушения.

Вопросы кибербезопасности рассматриваются в специальных стандартах. Анализ зарубежной нормативной базы показал, что в настоящее время в стадии разработки находится ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering[4]. Структура рассматриваемого стандарта представлена на рис. 2.

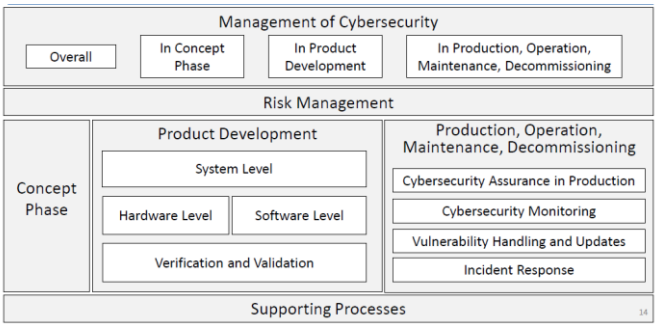

Рисунок 2. Структура стандарта 21434.

В силу того, что данный стандарт находится в процессе разработки, поэтому на текущий момент нельзя провести сопоставление его положений с положениями Концепции.

D. Перспективы развития требований

Развитие систем автономного вождения, электрификация, подключение автомобилей к сети и системы общего использования оказали фундаментальное влияние на индустрию. В настоящий момент в автоиндустрии происходят серьезные изменения в подходах к организации электроники в автомобиле. На рис.3 приведена информация по подходам реализации E/E архитектуры.

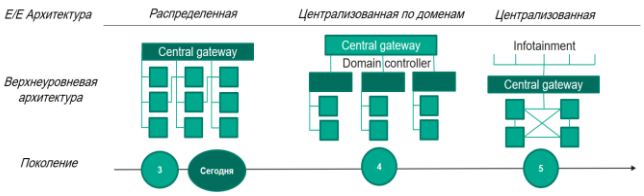

Рисунок 3. Эволюция E/E архитектуры.

В современных автомобилях электроника построена по распределенной архитектуре и используется более 100 различных электронных блоков. Общая тенденция в будущем - объединение электронных блоков по доменам (поколение 4), а далее – централизация и применение высокопроизводительных контроллеров (поколение 5). Фактически, в будущих автомобилях будет значительно

4 https://www.iso.org/ru/standard/70918.html

меньше электронных блоков, но высокая производительность и применение на них технологий виртуализации, позволит запускать на одном контроллере приложения, выполняющие различные задачи и имеющие разные требования по обеспечению функциональной и кибербезопасности.

Централизацию архитектуры будет сопровождать разделение аппаратной и программной платформ. Системы внутри автомобилей будут построены как многоуровневая архитектура с четкими точками абстракции на уровнях операционной системы (ОС) и промежуточного программного обеспечения. Количество строк кода в электронных блоках будет расти, что будет оказывать влияние и на подходы к обеспечению кибербезопасности.

Европейская экономическая комиссия ООН (ЕЭК ООН) подготовила проекты 2 новых положений:

- о единообразных положениях относительно одобрения транспортных средств в отношении систем кибербезопасности и управления кибербезопасностью;
- о процессах обновления программного обеспечения транспортных средств и систем управления обновлениями программного обеспечения.

После принятия данных документов ЕЭК ООН и странами-членами Всемирного форума для согласования правил в области транспортных средств, автопроизводителям потребуется внедрить конкретные практики обеспечения кибербезопасности и обновления программного обеспечения. Согласно проекту документа UNECE WP.29 нормы обеспечения кибербезопасности и обновления программного обеспечения должны включать в себя:

- **Управление рисками кибербезопасности**. Участники рынка должны будут обеспечивать комплексное управление рисками, и выявлять их не только в транспортных средствах, но и в смежных компонентах экосистемы, которые могут оказывать влияние на безопасность. Необходимо будет принимать меры по снижению таких рисков;
- **«Безопасность-по-дизайну».** Автопроизводители должны будут разрабатывать безопасные транспортные средства с самого первого шага, применяя самые современные методы в разработке аппаратного и программного обеспечения, а также обеспечивать гарантии, что транспортные средства и смежные компоненты экосистемы спроектированы, изготовлены и испытаны с точки зрения кибербезопасности и любые киберриски снижаются должным образом;
- **Обнаружение и реагирование.** Производители транспортных средств должны иметь возможность обнаруживать технические уязвимости и проблемы безопасности, которые могут повлиять на безопасность или защиту транспортного средства;
- **Безопасные и надежные обновления.** Автомобильные игроки должны иметь возможность реагировать на любое обнаруженное событие безопасности и предоставлять обновления программного обеспечения для устранения проблем безопасности.

III. Предложения по проработке Концепции

Можно сделать вывод о том, что защита только одного из элементов экосистемы «подключенного» автомобиля не обеспечит защиту в целом. В связи с этим, требуется комплексный подход к решению задачи. В обеспечении кибербезопасности беспилотного транспорта можно выделить следующие ключевые аспекты, на которые необходимо обращать внимание при проектировании и создании систем:

- **Кибербезопасность внутри автомобиля** – автономные автомобили используют данные в режиме реального времени от различных датчиков и электронных блоков управления;
- **Аутентификация водителя** – при предоставлении различных сервисов мобильности требуется аутентификация водителя/пользователя;
- **Мониторинг состояния автомобиля** – необходимо осуществлять сбор данных о состоянии систем автомобиля. Во время неправильных настроек у злоумышленника есть большие возможности получить доступ к компонентам транспортного средства, которые могут быть дополнительно использованы для получения доступа ко всей сети;
- **Обеспечение безопасности внутренних и внешних коммуникаций** - доверие и конфиденциальность являются основными проблемами в случае меж- и внутриавтомобильной связи. Межавтомобильная связь относится к настройке V2X, которая состоит из автомобилей разных производителей. Атаки в любом из этих режимов оказывают значительное влияние на надежность сети;
- **Обеспечение безопасности инфраструктуры** – уязвимости в мобильных приложениях и платформах, осуществляющих сбор и анализ данных с ТС и элементов дорожной инфраструктуры, могут привести к отправке в беспилотный автомобиль скомпрометированных данных, на основе

которых он может принять некорректные решения;

- **Управление траффиком и детекция аномалий** - управление трафиком включает в себя вопросы, связанные с управлением скоростью, информацией о трафике, информацией о маршрутизации, совместной навигацией. Кроме того, поведение водителя, автомобильные аномалии и сетевые вторжения являются другими факторами, влияющими на основные функции автомобильной системы. Достаточно безопасные механизмы могут помочь решить эти проблемы и выявить потенциальные аномалии до их атаки.

IV. Практические шаги

A. Технические предложения

Обеспечение кибербезопасности не ограничивается только этапом производства транспортного средства, она должна быть обеспечена на всем жизненном цикле автомобиля, т.к. уязвимости могут быть обнаружены в любой момент времени.

Какие же практические шаги можно предпринять?

1. Проведение аудитов безопасности и тестов на проникновение с целью выявления уязвимостей существующих систем, а также для проектирования системы обеспечения кибербезопасности беспилотного автомобиля. При этом, тестировать необходимо не только автомобиль, но и инфраструктуру с которой он взаимодействует (телематическая платформа, мобильные приложения и т.д.);
2. Применение технологий обеспечения кибербезопасности внутри автомобиля. Например, для электронных блоков автомобилей уже сейчас существуют специализированные платформы безопасности и ОС с функционалом безопасной загрузки, обновления и изоляции процессов;
3. Создание инфраструктуры центра сбора и мониторинга событий для оперативного выявления атак и их предотвращения;

B. Организационные предложения

России необходимо становиться частью мирового процесса по многим причинам. Во-первых, мы являемся членом Всемирного форума для согласования правил в области транспортных средств и требования документа UNECE WP.29 также будут затрагивать наш автопром. Во-вторых, российские автопроизводители вынуждены использовать электронную компонентную базу иностранных поставщиков в связи с тем, что российские поставщики пока не могут обеспечить полный набор необходимых комплектующих. В-третьих, все-таки иностранные компании пока являются драйвером развития технологий автопромышленности.

Что можно сделать уже сейчас, чтобы стать частью мирового процесса? Например, вступать в различные профессиональные организации, которые объединяют автопроизводителей, поставщиков электроники и разработчиков ПО. Ярким примером является ассоциация AUTOSAR (**AUT**omotive **O**pen **S**ystem **AR**chitecture), ведущая разработку перспективного стандарта открытой архитектуры автомобильной системы AUTOSAR Adaptive Platform. Реализация сервисно-ориентированной архитектуры (SOA) в высокопроизводительных контроллерах домена и шлюзах, как раз будет использоваться рядом автопроизводителей и поставщиков электроники в будущих автомобилях. Кстати, членами AUTOSAR уже стали и компании из России. По тематике V2X также существуют отдельные ассоциации 5GAA, CAR2CAR, European Automotive-Telecom Alliance (EATA).

V. Заключение

Таким образом, утвержденная Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования фактически инициирует процесс более активного участия Российской Федерации в глобальных процессах обеспечения информационной безопасности автомобильного транспорта, а также беспилотного транспорта, построенного на его основе.

Библиография

[1] Калинцев Н.Н., Михайлов Д.М. Аппаратно-программный комплекс обнаружения жучков в инфраструктуре автомобиля. // Спецтехника и связь. - 2014. - стр. 41 — 43.
[2] Беляев К.М. Романов А.А. Кибернетическая безопасность беспилотного транспорта. // Технико-технологические проблемы сервиса. - 2018. - № 2(44) — стр. 37 — 42.
[3] Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУ ТП. // Вопросы кибербезопасности. - 2015. - № 2 (10). - стр. 56 – 59.
[4] Покусаев О.Н., Куприяновский В.П., Катцын Д.В., Намиот Д.Е. Онтологии и безопасность автономных (беспилотных) автомобилей. // International Journal of Open Information Technologies. - 2019. -
[5] Копылов С.Н., Кущук В.А., Полтавец Д.В. Пожарная безопасность автотранспортных средств. // Технологии гражданской безопасности. - 2009. - т. 6 № 1-2. - стр. 88 — 93.
[6] McKinsey&Company. Automotive software and electronics 2030. Mapping the sector's future landscape. – 2019. – стр. 9 – 11.
[7] McKinsey&Company. Cybersecurity in automotive. Mastering the challenge. – 2020. – стр. 6, 10.

Problems of ensuring information security of highly automated vehicles

Dmitry Pravikov, Evgeniya Ponomareva, Vasily Kupriyanovsky

***Abstract* - The article analyzes the provisions of the Concept of road safety adopted in the Russian Federation with the participation of unmanned vehicles on public roads. Regulatory documents defining the development of artificial intelligence as an innovative technology are considered. Threats to the information security of modern cars are described. it is shown that the number of threats will increase with the creation of unmanned transport. The review of requirements for information security of unmanned vehicles, formed on the basis of the practice of information security specialists, as well as relevant international standards, is conducted. It is concluded that it is necessary to detail the provisions of the Concept, taking into account global approaches to ensuring information security of cars and unmanned devices based on them.**

***Keywords* - Driverless vehicles, safety requirements.**

REFERENCES

[1] Kalintsev N.N., Mikhailov D.M. Apparatno-programmniy kompleks obnaruzenia zuchkov v infrastructure avtomobilia. // Speztechnika I svyaz. - 2014. - pg. 41 — 43.

[2] Belyaev K.M., Romanov A.A. Kiberneticheskaya bezopasnot bespilotnogo transporta. // Tehniko-tehnologicheskie problemy servisa. - 2018. - № 2(44) - pg. 37 — 42.

[3] Gordeychik S.V. Missionersky podhod k kiberbezopasnosty ASU TP. // Voprosy kiberbezopasnosti - 2015. - № 2 (10). - pg. 56 – 59.

[4] Pokusayev O.N., Kupriyanovsky V.P., Katchyn D.V., Namiot D.E. Ontologyy i bezopasnost avtonomnyh (bespilotnyh) avtomobiley. // International Journal of Open Information Technologies. - 2019. – vol. 7, no. 2.

[5] Kopylov S.N., Kushuk V.A., Poltavez D.V. Pozarnaya bezopasnost avtotransportnyh sredstv. // Tehnologyy grazdanskoy bezopasnosty. - 2009. - т. 6 № 1-2. - pg. 88 — 93.

[6] McKinsey&Company. Automotive software and electronics 2030. Mapping the sector's future landscape. – 2019. – pg. 9 – 11.

[7] McKinsey&Company. Cybersecurity in automotive. Mastering the challenge. – 2020. – pg. 6 - 10.