Разработка модели угроз кибербезопасности электронных блоков управления в автомобиле

К.И. Тахаутдинова, Т.А. Маркина

***Аннотация*—В исследование приводится процесс разработки модели угроз кибербезопасности электронных блоков управления в автомобиле. Рассматриваются проблемы в области обеспечения информационной кибербезопасности автомобилей и направления в решении этих проблем. Приводится сравнительный анализ стандартов и нормативных документов в области кибербезопасности автомобилей. Отдельно рассматриваются построение модели нарушителя и составление банка угроз, как наиболее важные этапы в построении модели угроз. В результате работы разработана модель угроз кибербезопасности автомобилей, в которой определены возможные внутренние (3 нарушителя) и внешние (4 нарушителей) нарушители, также разработан банк угроз безопасности информационной безопасности автомобилей, включающий в себя 206 угроз и произведена классификация угроз банка угроз на разделы. Для обеспечения кибербезопасности информационной системы автомобиля были разработаны общие рекомендации.**

***Ключевые слова*— Кибербезопасность автомобилей, модель угроз, модель нарушителя, угрозы информационной системы автомобиля.**

I. Введение

Современные автомобили обладают огромным количеством компьютеров и мультимедийных систем, которые активно взаимодействуют с облачными сервисами, другими автомобилями и дорожной инфраструктурой. Это добавляет к существующим опасностям риски, связанные с киберугрозами. Каждый электронный блок управления автомобилем, такой как блоки управления двигателем, трансмиссией, системой безопасности, навигации, кондиционирования и другие, может содержать различные компоненты, которые могут быть уязвимыми из-за недостатков в программном обеспечении. Недостатки в безопасности автомобиля могут быть использованы злоумышленниками для удаленного доступа и контроля над автомобилем, что может привести к серьезным последствиям, например отключению системы безопасности или изменению маршрута, что может привести к аварии.

Статья получена 13 июня 2023.

К.И. Тахаутдинова, Университет ИТМО (e-mail: karina.takhautdinova@mail.ru).

Т.А. Маркина, Университет ИТМО (e-mail: markina_t@itmo.ru).

В нашей стране все больше развивается отечественный автопром. Правительство РФ выпустило распоряжение. № 4261-р «Об утверждении Стратегии развития автомобильной промышленности Российской Федерации до 2035 г» [1].

Реализация Стратегии обеспечит конкурентоспособность российской автомобильной промышленности и возможность экспорта технологий на глобальном уровне за счет создания производств инновационного транспорта - электромобилей, гибридных автомобилей, включая автомобили на водородных топливных элементах, и автономных автомобилей.

Сегодня в автомобильной индустрии кибербезопасность должна обеспечивается как аппаратными, так и программными решениями. Организациям необходимо разработать стандарты и регламенты, которые регулировали бы кибербезопасность, что дополнительно поспособствует развертыванию киберзащитных решений во всех подключенных автомобилях. На данный момент существует несколько международных стандартов, однако при перспективном развитии российского автопрома необходимо также иметь собственные руководящие документы в области кибербезопасности автомобилей, которые бы описывали возможные угрозы и потенциальных нарушителей. Возникает необходимость в разработке модели угроз.

В ходе статьи рассматриваются проблемы в области обеспечения информационной кибербезопасности автомобилей и направления в решении этих проблем. Приводится сравнительный анализ стандартов и нормативных документов в области кибербезопасности автомобилей. Отдельно рассматриваются построение модели нарушителя и составление банка угроз, как наиболее важные этапы в построении модели угроз.

II. Элементы и угрозы безопасности автомобилей

С развитием подключенных автомобилей возникают новые вызовы в области информационной безопасности. Поскольку автомобили становятся все более связанными с внешними сетями и устройствами, они становятся более уязвимыми к кибератакам и злоумышленникам. Использование новых технологий производителями автомобилей также привлекает злоумышленников, которые хотят овладеть этими технологиями и без

достаточной защиты информационных систем автомобилей страдают сами производители этих автомобилей.

Несанкционированный доступ к системам автомобиля может привести к угону автомобиля, нарушению приватности владельца, а в некоторых случаях даже к физической опасности для пассажиров.

Как отмечено в [2] при изучении аспектов безопасности подключенного устройства по его физическому расположению можно выделить различные области. Первая область — это, группы элементов, которые расположенных внутри транспортного средства, а именно электронные блоки управления, автомобильная сеть и коммуникационный шлюз. Следующая область — это использование мобильных устройств для связи и управлением автомобилем, которые могут принадлежать не только владельцу транспортного средства, но и сервису или даже стороннему пользователю в случае каршеринга. Третья область — это использование облачной инфраструктуры, поскольку нельзя быть точно уверенным, что не возникнут проблемы на стороне поставщика облачных услуг. Помимо этого, протокол, аутентификация, авторизация, шифрование и защита данных играют важную роль в общей безопасности системы.

Каждый из электронных блоков отвечает за определенные функции в автомобиле и может содержать различные компоненты, такие как микроконтроллеры, датчики, актуаторы, память и интерфейсы для связи с другими блоками управления. Электронные блоки управления (ЭБУ) заменили механические и аналоговые модули. Даже самые простые автомобили имеют не менее 30 ЭБУ, а более дорогие модели содержат более 100 ЭБУ, соединённых между собой лабиринтом разнообразных цифровых шин — Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), Ethernet.

Электронные блоки управления автомобилем, могут ошибочно считаться «безопасными», так как они находятся внутри транспортного средства и до них нельзя добраться напрямую, однако они подвержены нескольким угрозам.

Источников для угроз может быть несколько: разработчики могут оставить различные бэкдоры из-за отладки, невнимательности, или намеренно. Существуют также и другие скрытые угрозы для электронных блоков управления. Один из них заключается в сложном устройстве и функциональности электронных блоков управления, которые не закрывают все возможные уязвимости. Ещё одна проблема заключается в том, что сам ЭБУ обеспечивает диагностический доступ.

Другая проблема связана с целостностью команд. Сам ЭБУ должен применять правила для переопределения команд подключенной автомобильной системы в зависимости от состояния транспортного средства, чтобы избежать опасных ситуаций.

III. Проблемы обеспечения информационной безопасности автомобилей и направления в решении этих проблем

С развитием технологий и прогрессом в автомобильной индустрии возникает все больше проблем, связанных с обеспечением информационной безопасности автомобилей.

В статье «Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges» [3] авторы Саймон Паркинсон, Пол Уорд, Кайл Уилсон и Джонатан Миллер говорят от том, что системы взаимодействия автомобилей основаны на технологиях, которые все еще находится в стадии развития и не подвергались значительному конкурентному давлению. Академические исследования являются основным стимулом для выявления уязвимостей и повышения безопасности технологии, также есть несколько случаев использования уязвимостей злоумышленниками. Однако со все большим увеличением автоматизации и коммуникационных технологий в транспортных средствах, увеличится интерес к обнаружению уязвимостей, так как киберпреступность на транспортных средствах становится финансово мотивированной.

Цепочка поставок в транспортной отрасли такова, что многие технологии (аппаратное обеспечение, программное обеспечение и инфраструктура) используются без должного понимания последствий для безопасности. Например, электронный чип, используемый в блоке управления, может иметь уязвимость, о которой производитель не знает. Это может привести к выявлению уязвимостей, которые неизвестны производителю, но являются легкой добычей для злоумышленников. Производители транспортных средств часто передают на аутсорсинг проектирование и разработку компонентов и систем, что приводит к изоляции производителей и возможному отсутствию дополнительных мер безопасности. Также возможно, что у некоторых производителей может отсутствовать копия исходного кода блока управления, используемого в их автомобилях, что не позволяет им проводить дополнительный аудит.

В своей статье «Проблемы обеспечения информационной безопасности высокоавтоматизированных транспортных средств» [4] авторы Д.И.Правиков, Е.А.Пономарева, В.П.Куприяновский анализируют 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. Авторы подчёркивают, что в указанном документе особое внимание привлек раздел «Информационная безопасность высокоавтоматизированных транспортных средств», в Концепции [5] указывается, что для обеспечения безопасности необходимо использовать средства защиты информации, которые обеспечат целостность и конфиденциальность передаваемых

данных. Также предлагается использовать криптографические методы защиты, которые защитят от перехвата и подмены данных.

Согласно концепции, процесс разработки автомобиля также должен сопровождаться «отчетом о кибербезопасности на основе унифицированных стандартов». Это должен быть один из документов, необходимых для допуска высокоавтоматизированного транспортного средства к эксплуатации. Из этого следует, что для того, чтобы сосредоточиться на разработке и внедрении надежных систем защиты необходимо также разрабатывать стандарты в области кибербезопасности автомобилей. Нормативно-правовая база в области кибербезопасности автомобилей существует, но она не всегда соответствует современным вызовам и угрозам кибербезопасности. Например, в США был принят закон о кибербезопасности автомобилей, который требует от производителей устанавливать защиту от хакерских атак и уведомлять владельцев об уязвимостях в системах безопасности. Однако, многие другие страны еще не приняли подобные законы.

Киберпреступность на транспорте стала наиболее распространенным видом преступлений в последнее время. В новостях все чаще появляются сообщения о краже личных данных пользователей каршеринговых сервисов, продаже незаконно полученных транспортных карт и взломе электросамокатов, что угрожает безопасности транспорта.

В своей работе «Основные направления обеспечения кибербезопасности на транспорте» [6] Шашкин А. А. рассматривает основные направления, по которым стоит работать не только контролирующим органам, но и самим организациям и обществу в целом для того, чтобы обеспечить кибербезопасность на транспорте. Среди основных направлений по обеспечению кибербезопасности в транспорте Шашкин А. А. выделяет следующие действия:

1) Для более точного понимания механизма совершения преступления и составления плана расследования необходимо проводить оперативные исследования и компьютерно-технические экспертизы, анализировать заключения экспертов и использовать их как доказательства в судебном процессе. Специалисты, обладающие специальными знаниями и навыками в данной области, играют ключевую роль в этом процессе.

2) Для предотвращения мошенничества необходимо проводить профилактические мероприятия с населением, включая беседы и расклейку листовок. Однако для транспортных организаций, которые не предоставляют свои данные, необходимо проводить проверки на наличие соответствующих систем безопасности и всех необходимых лицензионных документов для обеспечения соответствующего уровня защиты.

3) Для обеспечения безопасности в транспортной сфере необходимо постоянно контролировать техническую оснащенность организаций и предотвращать кибератаки, которые могут привести к человеческим жертвам.

4) Важным фактором является улучшение программного обеспечения с помощью компетентных специалистов и профессионального оборудования, а также контроль со стороны правоохранительных органов.

5) Необходимо совершенствовать законодательную базу, связанную с кибербезопасностью на транспорте, разрабатывать методики и базы данных угроз кибербезопасности автомобилей.

6) Важно противодействовать потенциальным преступникам, проверяя лиц, которые отбыли наказание за киберпреступления.

7) Для более эффективного раскрытия и предотвращения киберпреступлений на транспорте необходимо совершенствовать материально-техническую базу правоохранительных органов.

В результате рассмотренных взломов автомобилей, проблем обеспечения информационной безопасности автомобилей можно сделать вывод о том, что необходимо усилить меры безопасности в производстве и эксплуатации автомобилей. Это может быть достигнуто путем улучшения процессов разработки и тестирования, внедрения стандартов безопасности и повышения осведомленности пользователей о возможных угрозах. Также важно установить более тесное сотрудничество между производителями автомобилей, поставщиками компонентов и специалистами по информационной безопасности, чтобы обеспечить целостность цепочки поставок и защитить автомобили от возможных угроз. В целом, безопасность автомобилей должна быть приоритетом для всей отрасли, чтобы обеспечить безопасность жизни и здоровья людей на дорогах.

IV. Сравнение стандартов в области кибербезопасности автомобилей

Стандарты в области кибербезопасности автомобилей являются неотъемлемой частью развития автомобильной промышленности и обеспечивают безопасность управления транспортными средствами. Они определяют требования к защите от кибератак, а также к проектированию, разработке и эксплуатации автомобилей.

Одним из наиболее значимых стандартов в области кибербезопасности автомобилей является ISO/SAE 21434[7]. Этот стандарт был разработан совместно Международной организацией по стандартизации (ISO) и Сообществом инженеров автомобильной промышленности (SAE) и определяет требования к процессам, методам и инструментам, используемым для обеспечения кибербезопасности автомобилей.

Кроме того, существуют и другие стандарты, например, SAE J3061 [8], который определяет методологию для управления кибербезопасностью в автомобильной промышленности.

Стандарт NHTSA Cybersecurity Best Practices [9] — это набор рекомендаций и лучших практик в области кибербезопасности, разработанный Национальным управлением безопасности дорожного движения (NHTSA) в США. Эти рекомендации предназначены для автопроизводителей и других участников автомобильной отрасли, чтобы помочь им защитить транспортные средства от кибератак и обеспечить безопасность пассажиров.

Ещё один стандарт — это NIST SP 800–53 (National Institute of Standards and Technology Special Publication 800–53) [10], который предоставляет каталог средств контроля безопасности и конфиденциальности для федеральных информационных систем и организаций.

Следующий документ — UN Regulation No. 155 [11], это правила Организации Объединенных Наций о единообразных положениях, касающихся официального утверждения транспортных средств с точки зрения кибербезопасности и обновлений их программного обеспечения. Еще один международный регламент, разработанный ООН — это W.29, который определяет требования к безопасности автомобилей. Он устанавливает стандарты для различных систем и компонентов автомобилей, включая системы торможения, управления двигателем и электроники. Стандарт W.29 также содержит рекомендации по использованию средств защиты и методов тестирования, чтобы обеспечить безопасность автомобилей и защиту от кибератак [12]. Этот стандарт является важным шагом в обеспечении безопасности информации в автомобилях и используется во многих странах по всему миру.

В России существуют несколько стандартов и законов, которые регулируют вопросы кибербезопасности в общем. Один из основных документов в области кибербезопасности - Федеральный закон "Об информации, информационных технологиях и о защите информации", который содержит требования к защите персональных данных и обеспечению кибербезопасности в целом [13].

Также стоит отметить, что в России существует Федеральный закон "О техническом регулировании", который устанавливает требования к безопасности продукции. Этот закон определяет процедуры сертификации и декларирования соответствия, которые позволяют обеспечить безопасность на рынке [14].

Существует также ГОСТ Р ИСО/МЭК 27001–2021 [15] — это стандарт, который устанавливает общие требования по созданию, внедрению, поддержке и постоянному улучшению системы менеджмента информационной безопасности. Он является российским национальным эквивалентом международного стандарта ISO/IEC 27001.

ISO/SAE 21434, SAE J3061, NIST SP 800–53 и UN Regulation No. 155 — это стандарты, которые описывают требования к кибербезопасности автомобилей. Несмотря на то, что все они имеют общую цель - обеспечение безопасности автомобилей от кибератак, каждый стандарт имеет свои особенности и принципы. Федеральный закон "Об информации, информационных технологиях и о защите информации" и Федеральный закон "О техническом регулировании" – российские законы для обеспечения безопасности.

Федеральный закон "Об информации, информационных технологиях и о защите информации" устанавливает правила и требования к обработке, хранению и передаче информации, а также охрану прав субъектов персональных данных. Закон также содержит положения о кибербезопасности, включая требования к защите информации от несанкционированного доступа и разглашения информации.

Федеральный закон "О техническом регулировании" определяет правила и требования к производству, реализации и эксплуатации технической продукции, включая автомобили. Он содержит положения о безопасности транспортных средств и требования к их технической безопасности.

Оба закона имеют отношение к кибербезопасности, но Федеральный закон "Об информации, информационных технологиях и о защите информации" более ориентирован на защиту информации и персональных данных, а Федеральный закон "О техническом регулировании" - на обеспечение безопасности транспортных средств в целом. В целом, эти законодательные акты являются важными для обеспечения информационной безопасности в Российской Федерации, однако, как и любые другие законы, они могут иметь недостатки и требовать дополнительных усовершенствований и изменений в соответствии с изменяющейся ситуацией в области информационной безопасности.

Хотя многие эти стандарты и нормативные акты содержат руководящие принципы и наилучшие практики для повышения кибербезопасности в автомобильной промышленности, они также имеют некоторые ограничения и проблемы. Например, Рекомендации NHTSA по кибербезопасности — это руководящий документ, который не имеет силы закона и не является нормативным актом. Защита информации не является основным направлением стандартов, применимых к исследованиям, в которых используется личная информация. NIST SP 800–53 дает общее представление об охвате контроля по отношению к другим системам и стандартам. UN Regulation No. 155 применяется только к транспортным средствам и обновлениям их программного обеспечения, и неясно, как они будут применяться на практике. Регламент WP.29 состоит из двух основных директив по кибербезопасности автомобилей. В первом документе основное внимание уделяется кибербезопасности и системам управления кибербезопасностью (CSMS). Второй регулирующий документ касается процессов обновления программным обеспечением и систем управления такими обновлениями (SUMS). Новая регулирующая норма ООН об универсальных предпосылках к обновлениям программ и системам управления обновлениями программ применяется к

автомобилям, работа которых зависит от обновления ПО [12].

Таким образом, хотя эти стандарты и нормативные акты важны для повышения кибербезопасности в автомобильной промышленности, они также имеют некоторые ограничения и проблемы, которые необходимо решить.

Исходя из анализа стандартов в области кибербезопасности автомобилей можно сделать вывод о том, что существует ряд международных стандартов, которые регулируют вопросы кибербезопасности электрических и электронных систем, устанавливаемых на автомобильном транспорте. Например, стандарт ISO/SAE 21434 посвящен вопросам обеспечения кибербезопасности электрических и электронных систем, устанавливаемых на автомобильном транспорте. Кроме того, стандарт ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001) определяет подходы к оценке и управлению рисками в организации, включая вопросы информационной безопасности. Однако, совершенные и изощренные методы нападения на информационные системы постоянно развиваются, поэтому поиски способов борьбы с ними не прекращаются никогда.

Данные стандарты не описывают угрозы, с которыми могут столкнуться производители и пользователи автомобилей, а в основном дают лишь рекомендации по обеспечению кибербезопасности. Однако существует множество угроз, которые могут возникнуть в области кибербезопасности автомобилей, и которые не описаны в стандартах. С учетом развития российской автопромышленности необходимо разрабатывать российские стандарты в области кибербезопасности автомобилей, которые описывали бы возможных нарушителей (модель нарушителя) и возможные угрозы для автомобилей, а также учитывали бы особенности технологий и устройств, используемых в автомобилях. Возникает необходимость в разработке модели угроз.

V. Разработка модели угроз

Разработка модели угроз является важным этапом в обеспечении кибербезопасности. В современном компьютерном сообществе атаки на информацию стали обыденной практикой, и злоумышленники используют как ошибки в написании и администрировании программ, так и методы социальной психологии и проблемы аппаратным оборудованием для получения желаемой информации. Цель разработки модели угроз заключается в выявлении потенциальных угроз и уязвимостей в информационной системе автомобилей, а также в разработке мер по их предотвращению и устранению. В данном контексте разработка модели угроз является неотъемлемой частью стратегии обеспечения кибербезопасности. Неотъемлемой частью построения модели угроз является разработка модели нарушителя

A. Разработка модели нарушителя

Построение модели нарушителя подразумевает рассмотрение возможных внутренних и внешних нарушителей, категорию нарушителей, а также согласно «Методика моделирования угроз безопасности информации» [16] рассматривается возможный потенциал нарушителя. На основе знаний о возможных нарушителях информационных систем был сформирован список возможных нарушителей, а также адаптирован под информационную систему автомобиля. Для каждого из видов нарушителей определена возможная мотивация совершения противозаконных действий.

На информационную систему автомобиля могут воздействовать два вида нарушителей: внешние нарушители и внутренние нарушители.

В таблице 1 представлены предлагаемые возможные нарушители для информационной системы автомобиля.

Таблица 1 – Возможные нарушители.

№ п/п	Вид нарушителя	Тип нарушителя	Идентификатор
1	Конкурирующие разработчики автомобилей	Внешний	НА1
2	Лица, имеющие санкционированный доступ на территорию, где располагается оборудование информационной системы автомобиля, но не имеющие доступа к ресурсам	Внутренний	НА2
3	Посторонние физические лица	Внешний	НА3
4	Пользователь автомобиля	Внутренний	НА4
5	Бывшие работники компании, разрабатывающий автомобиль	Внешний	НА5
6	Обслуживающий персонал автомобилей (механик, мойщики автомобилей и т. д.)	Внешний	НА6
7	Персонал разработчиков информационной системы автомобиля	Внутренний	НА7
8	Бывшие владельцы автомобиля	Внешний	НА8

Возможными внешними нарушителями информационной системы автомобиля являются конкурирующие организации, которые разрабатывают автомобили. Такого рода нарушители являются нарушителями с высоким и со средним потенциалом. Их возможной мотивацией является получение конфиденциальной информации о технологиях и разработках конкурента, а также нанесение ущерба его репутации и бизнесу. Взлом автомобиля может позволить конкурентам получить доступ к деталям производства, планам разработки, а также к информации о клиентах и продажах. Кроме того, конкуренты могут использовать взломанный автомобиль для проведения шпионских операций или для уничтожения имущества конкурента.

Следующими внешними возможными нарушителями со средним и низким потенциалом являются посторонние физические лица. В эту категорию лиц могут входить также и исследователи безопасности. Возможной мотивацией являются получение денежных

средств от продажи украденного автомобиля или получение выгоды от полученных данных с автомобиля.

Также внешними нарушителями могут являться бывшие работники компании, разрабатывающий автомобиль. Они являются нарушителями с низким потенциалом. Возможной мотивацией таких нарушителей может быть причинение имущественного ущерба путем мошенничества или иным противозаконным путем, еще одной возможной не исключающей мотиваций может быть месть за ранее совершенные действия. Также мотивация может быть связана с финансовыми причинами или желанием получить конкурентное преимущество в отношении других производителей.

Бывшие владельцы автомобиля являются нарушителями с низким потенциалом. Их возможной мотивацией может быть месть новому владельцу за какие-либо обиды, неприятности или желание получить доступ к личной информации нового владельца, хранящейся в системах автомобиля.

Способности внешних нарушителей зависят от используемых в информационной системе автомобиля средств защиты информации. Способности внутренних нарушителей зависят от действующих разграничительных мер по доступу к охраняемой информации.

Пользователи автомобиля, которые не являются его владельцами, являются возможными нарушителями с низким потенциалом. Возможной мотивацией таких нарушителей может быть причинение имущественного ущерба; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия также могут являться причиной угроз для автомобиля.

Лица, имеющие санкционированный доступ на территорию, где располагается оборудование информационной системы автомобиля, но не имеющие доступа к ресурсам и обслуживающий персонал автомобилей (механик, мойщики автомобилей и т. д.) могут являться возможными нарушителями с низким потенциалом. Возможной мотивацией может быть причинение имущественного ущерба путем обмана или злоупотребления доверием; непреднамеренные, неосторожные или неквалифицированные действия.

Для осуществления угроз нарушители могут использовать различные методы для достижения своих целей. Внутренние нарушители для достижения своих целей могут использовать различное оборудование организации не по назначению, которое также используется в организации по назначению. Также нарушителями могут использоваться различные программные и технические средства, которые находятся в свободной продаже в интернете или в магазинах. Помимо этого, нарушителями может использоваться пиратское программное обеспечение для достижения своих целей.

Из анализа нарушителей, для информационной системы определен нарушитель со среднем потенциалом.

B. Разработка банка угроз

Для обеспечения безопасности информационных систем и защиты от киберугроз необходимо проводить анализ возможных угроз и разрабатывать меры по их предотвращению. Для этого можно использовать банк угроз, который представляет собой систематизированный список потенциальных угроз безопасности информации, их описание и причины реализации, а также учитывающий возможных нарушителей. В данном контексте банк угроз является неотъемлемой частью стратегии обеспечения кибербезопасности и позволяет эффективно выявлять и устранять уязвимости в информационных системах.

Исходя анализа статей: «Как взламывают подключенные автомобили и что с этим делать» [17], «Хакеры выявили массу уязвимостей у современных автомобилей» [18], «Взлом автомобилей: удаленный доступ и другие вопросы безопасности» [19], и «Уязвимость в протоколе CAN, затрагивающая почти все современные автомобили» [20] были составлены предлагаемые угрозы для информационных систем автомобилей.

За основу для банка угроз был взят «Банк данных угроз ФСТЭК России» [21], однако, данный банк угроз был модифицирован и дополнен предлагаемыми угрозами, чтобы соответствовать информационным системам транспортных средств.

На данный в банке угроз ФСТЭК Российской Федерации находится 222 угрозы. Этот банк угроз периодически обновляется и пополняется, поэтому очень важно периодически пересматривать список угроз безопасности информационным систем.

Из банка были исключены угрозы, которые является неприменимыми к рассматриваемой информационной системе автомобилей. Из списка рассматриваемых были исключены следующие угрозы:

— угрозы, связанные с системами распределенных вычислений (грид-системами), так как такие технологии не применяются в рассматриваемой информационной системе;

— угрозы, связанные с большими данными, так как такие технологии не применяются в рассматриваемой информационной системе;

— угрозы, связанные с виртуальными машинами, так как такие технологии не применяются в рассматриваемой информационной системе;

— некоторые угрозы, связанные с суперкомпьютерами, так как такие технологии не применяются в рассматриваемой информационной системе и бортовые компьютеры автомобилей имеют гораздо меньшие мощности по сравнению с суперкомпьютерами;

— некоторые угрозы, связанные с мобильными устройствами, так как не все перечисленные угрозы для

мобильных устройств могут оказать влияние на информационные системы автомобилей.

После исключения неприменимых угроз в банке угроз осталось 187 угроз. Далее было необходимо произвести корректировку наименования угроз, описания угроз и объектов воздействия, чтобы они соответствовали транспортным средствам. Таким образом, было необходимо адаптировать банк угроз к специфике транспортных средств, учитывая особенности их компонентов и систем безопасности. Это позволит более эффективно выявлять и устранять уязвимости в информационных системах автомобилей и других транспортных средствах.

В итоговом банке угроз оказалось 206 угроз безопасности.

Банк угроз содержит угрозы, которые могут быть реализованы в разных типах автомобилей. Некоторые автомобили уже сейчас используют подключение к интернету, облачные технологии и управляются с помощью приложения на смартфоне, а другие обходятся без этих технологий. Для удобства составления модели угроз для определенных видов автомобилей было принято решение разделить банк угроз на разделы.

Проанализировав угрозы банка данных угроз ФСТЭК и новые выявленные угрозы для информационных систем автомобиля были составлены разделы для классификации банка угроз. На разделы угрозы были поделены с учетом описания угрозы и объекта воздействия конкретной угрозы. В таблице 4 представлены названия разделов банка угроз.

Таблица 2 – Список разделов банка угроз

№	Название раздела
1	Угрозы, связанные с использованием облачных технологий
2	Угрозы, связанные с использованием машинного обучения и ИИ
3	Угрозы, связанные с нарушением аутентификации и авторизации
4	Угрозы, связанные с нарушением безопасности сети, телекоммуникаций, подключения к Интернет, использованием беспроводных технологий и gps
5	Угрозы, связанные с использованием вредоносного программного обеспечения и эксплойтов, дискредитированных приложений или программ
6	Угрозы, связанные с нарушением безопасности программного обеспечения и операционных систем
7	Угрозы, связанные с проблемами средств защиты или их отсутствием
8	Угрозы, связанные с физическим доступом

Разделение банка угроз на соответствующие разделы позволяет систематизировать и классифицировать угрозы, что упрощает их анализ и позволяет принимать соответствующие меры по предотвращению их реализации.

C. Рекомендации по устранению угроз

Для обеспечения кибербезопасности информационной системы автомобиля были разработаны рекомендации, такие как:

1) Правильно использовать пароли и PIN-коды для доступа к автомобильной системе. Выберите случайный набор символов и цифр для каждого автомобиля, и не используйте одинаковые пароли для разных устройств.

2) Установка обновлений и патчей системы. Производите регулярные проверки системы автомобиля на наличие обновлений и загружайте их сразу же после выхода, чтобы обеспечить максимальную защиту от новых угроз.

3) Использование антивирусных и антивредоносных программ для защиты устройства от заражения. Существуют специализированные решения, которые специально разработаны для повышения безопасности автомобильной системы.

4) Ограничение доступа к автомобильному приложению через Wi-Fi и Bluetooth соединение, если это возможно. Определите список устройств, которым разрешен доступ к сети автомобиля, и следите за обновлением списка.

5) Регулярное обновление паролей Wi-Fi и Bluetooth соединения для установления взаимодействия между автомобильной системой и подключенными устройствами.

6) Блокирование доступа к удаленным облачным сервисам, которые могут иметь доступ к автомобилю или хранить данные о езде.

7) Систематический аудит и контроль настройки безопасности системы автомобиля, а также регулярное обучение владельцев и пользователей правилам безопасности в автомобиле.

8) Установка системы распознавания лиц и голосовых команд для отслеживания авторизованных пользователей и предотвращения несанкционированного доступа.

9) Использование средств шифрования для защиты передаваемых данных, в том числе служебных сообщений, проводимых по каналам связи.

10) Соблюдение правил поведения во время поездки, включая закрытие дверей, подключение камер наблюдения и активацию приборов блокировки при возникновении подозрительной ситуации. Также необходимо следить за осмысленностью коммуникаций с автомобильными системами и внешним окружением, например при использовании голосовых команд.

VI. Заключение

Таким образом проведен анализ необходимости разработки руководящих документов в области кибербезопасности автомобилей, рассмотрены проблемы в области обеспечения информационной безопасности автомобилей и направления в решении этих проблем, проведен сравнительный анализ стандартов и нормативных документов в области

кибербезопасности автомобилей; разработана модель угроз кибербезопасности автомобилей, в которой определены возможные внутренние (3 нарушителя) и внешние (4 нарушителей) нарушители; разработан банк угроз безопасности информационной безопасности автомобилей, включающий в себя 206 угроз, а также разработаны рекомендации по устранению угроз.

Библиография

[1] Распоряжение Правительства РФ № 4261-р «Об утверждении Стратегии развития автомобильной промышленности Российской Федерации до 2035 г.»: [Электронный источник] – URL: https://www.garant.ru/products/ipo/prime/doc/405963861/.

[2] Tamas Becsi, Szilard Aradi, Peter Gaspar. Security issues and vulnerabilities in connected car systems. – Текст: электронный // Models and Technologies for Intelligent Transportation Systems (MT-ITS) – 2015. – URL: https://www.researchgate.net/publication/281447339_Security_issues_and_vulnerabilities_in_connected_car_systems.

[3] Simon Parkinson, Paul Ward, Kyle Wilson, Jonathan Miller. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challengess. – Текст: электронный // IEEE Journal on Intelligent Transportation Systems. – 2017. – 18(11):1-18 – URL: https://www.researchgate.net/publication/314272204_Cyber_Threats_Facing_Autonomous_and_Connected_Vehicles_Future_Challenges.

[4] Правиков Д.И., Пономарева Е.А., Куприяновский В.П. Проблемы обеспечения информационной безопасности высокоавтоматизированных транспортных средств // International Journal of Open Information Technologies. 2020. №6. URL: https://cyberleninka.ru/article/n/problemy-obespecheniya-informatsionnoy-bezopasnosti-vysokoavtomatizirovannyh-transportnyh-sredstv.

[5] Распоряжение Правительства РФ от 25 марта 2020 г. № 724-р «О Концепции обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования»: [Электронный источник] – URL: https://www.garant.ru/products/ipo/prime/doc/73707148/

[6] Шашкин А. А. Основные направления обеспечения кибербезопасности на транспорте // Цифровой суверенитет и кибербезопасность – М., 2022. – С. 235–239.

[7] ISO/SAE 21434: 2021 «Road vehicles – Cybersecurity engineering: [Электронный ресурс]. – август 2021 – URL: https://www.iso.org/standard/70918.html (дата обращения: 11.11.2022)

[8] SAE J3061:2016 «Cybersecurity Guidebook for Cyber-Physical Vehicle Systems»: [Электронный ресурс]. – 14.01.2016 – URL: https://www.sae.org/standards/content/j3061_201601/.

[9] NHTSA Cybersecurity Best Practices for the Safety of Modern Vechicles: [Электронный ресурс]. – 2020 – URL: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf.

[10] National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53): [Электронный ресурс]. – 2020 – URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[11] UN Regulation No. 155 «Cyber security and cyber security management system»: [Электронный ресурс]. – 2021 – URL: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

[12] Кибербезопасность? Да, теперь и ваша машина в зоне риска: [Электронный ресурс]. –22.06.2021 – URL: https://habr.com/ru/companies/macloud/articles/564054/.

[13] Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации от 27.07.2006: Федеральный закон № 149-ФЗ: [принят Государственной думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года]: [Электронный источник] – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/

[14] Российская Федерация. Законы. О техническом регулировании от 27.12.2002: Федеральный закон № 184-ФЗ: [принят Государственной думой 15 декабря 2002 года: одобрен Советом Федерации 18 декабря 2002]: [Электронный источник] – URL: https://www.consultant.ru/document/cons_doc_LAW_40241/

[15] ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения информации. Системы менеджмента информационной безопасности. Требования: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. № 1653-ст: дата введения 2022-01-01 – Москва: Стандартинформ, 2022. – 22 с.

[16] Методический документ. «Методика моделирования угроз безопасности информации». Проект Федеральной службы по техническому и экспортному контролю России - 2020г. – 54с. – Текст: электронный [Электронный источник] – URL: https://fstec.ru/component/attachments/download/2727.

[17] Как взламывают подключенные автомобили и что с этим делать: [Электронный ресурс]. –11.12.2020 – URL: https://habr.com/ru/companies/trendmicro/articles/532470/.

[18] Хакеры выявили массу уязвимостей у современных автомобилей: [Электронный ресурс]. –16.01.2023 – URL: https://habr.com/ru/companies/cloud4y/articles/710906/.

[19] Взлом автомобилей: удаленный доступ и другие вопросы безопасности: [Электронный ресурс]. –11.13.2022 – URL: https://www.osp.ru/pcworld/2012/11/13018020.

[20] Уязвимость в протоколе CAN, затрагивающая почти все современные автомобили: [Электронный ресурс]. –2018 – URL: https://www.opennet.ru/opennews/art.shtml?num=47039.

[21] Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России: [сайт]. – URL: https://bdu.fstec.ru.

Development of a cybersecurity threat model for electronic control units in a car

K.I. Takhautdinova, T.A. Markina

***Abstract*—The study describes the process of developing a cybersecurity threat model for electronic control units in a car. The problems in the field of ensuring information cybersecurity of cars and directions in solving these problems are considered. A comparative analysis of standards and regulatory documents in the field of cybersecurity of cars is given. Separately, the construction of the intruder model and the compilation of the threat bank are considered as the most important stages in the construction of the threat model. As a result of the work, a model of threats to the cybersecurity of cars was developed, in which possible internal (3 violators) and external (4 violators) violators were identified, a bank of threats to the security of information security of cars was also developed, including 206 threats, and the classification of threats of the threat bank into sections was made. General recommendations have been developed to ensure the cybersecurity of the vehicle's information system.**

***Keywords* — Cybersecurity of cars, threat model, intruder model, threats to the car information system.**

REFERENCES

[1] Decree of the Government of the Russian Federation No. 4261-r "On approval of the Strategy for the development of the automotive industry of the Russian Federation until 2035": [Electronic source] – URL: https://www.garant.ru/products/ipo/prime/doc/405963861 /.

[2] Tamas Becsi, Szilard Aradi, Peter Gaspar. Security issues and vulnerabilities in connected car systems. – Text: electronic // Models and Technologies for Intelligent Transportation Systems (MT-ITS) – 2015. – URL: https://www.researchgate.net/publication/281447339_Security_issues_and_vulnerabilities_in_connected_car_systems.

[3]Simon Parkinson, Paul Ward, Kyle Wilson, Jonathan Miller. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenge. – Text: electronic // IEEE Journal on Intelligent Transportation Systems. – 2017. – 18(11):1-18 – URL: https://www.researchgate.net/publication/314272204_Cyber_Threats_Facing_Autonomous_and_Connected_Vehicles_Future_Challenges.

[4] Pravikov D.I., Ponomareva E.A., Kupriyanovskiy V.P. Problems of ensuring information security of highly automated vehicles // International Journal of Open Information Technologies. 2020. №6. URL: https://cyberleninka.ru/article/n/problemy-obespecheniya-informatsionnoy-bezopasnosti-vysokoavtomatizirovannyh-transportnyh-sredstv.

[5] Decree of the Government of the Russian Federation No. 724-r dated March 25, 2020 "On the Concept of ensuring road safety with the participation of unmanned vehicles on public roads": [Electronic source] – URL: https://www.garant.ru/products/ipo/prime/doc/73707148 /

[6] Shashkin A. A. The main directions of ensuring cybersecurity in transport // Digital sovereignty and Cybersecurity – M., 2022. – pp. 235-239.

[7] ISO/SAE 21434:2021 "Road vehicles – Cybersecurity engineering: [Electronic resource]. – August 2021 – URL: https://www.iso.org/standard/70918.html (date of application: 11.11.2022)

[8] SAE J3061:2016 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems": [Electronic resource]. – 14.01.2016 – URL: https://www.sae.org/standards/content/j3061_201601/.

[9] NHTSA Cybersecurity Best Practices for the Safety of Modern Vechicles: [Electronic resource]. – 2020 – URL: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf.

[10] National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53): [Electronic resource]. – 2020 – URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[11] UN Regulation No. 155 "Cyber security and cyber security management system": [Electronic resource]. – 2021 – URL: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

[12] Cybersecurity? Yes, now your car is at risk: [Electronic resource]. - 22.06.2021 – URL: https://habr.com/ru/companies/macloud/articles/564054 /.

[13] Russian Federation. Laws. On Information, Information Technologies and Information Protection dated 27.07.2006: Federal Law No. 149-FZ: [adopted by the State Duma on July 8, 2006: approved by the Federation Council on July 14, 2006]: [Electronic source] – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.

[14] Russian Federation. Laws. On Technical Regulation of December 27, 2002: Federal Law No. 184-FZ: [adopted by the State Duma on December 15, 2002: approved by the Federation Council on December 18, 2002]: [Electronic source] – URL: https://www.consultant.ru/document/cons_doc_LAW_40241/.

[15] GOST R ISO/IEC 27001-2021. Information technology. Methods and means of providing information. Information security management systems. Requirements: National Standard of the Russian Federation: official publication: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated November 30, 2021 No. 1653-st: date of introduction 2022-01-01 – Moscow: Standartinform, 2022. – 22 p.

[16] Methodological document. "Methods of modeling information security threats". Project of the Federal Service for Technical and Export Control of Russia - 2020 – 54c. – Text: electronic [Electronic source] – URL: https://fstec.ru/component/attachments/download/2727.

[17] How connected cars are hacked and what to do with it: [Electronic resource]. –11.12.2020 – URL: https://habr.com/ru/companies/trendmicro/articles/532470/.

[18] Hackers have revealed a lot of vulnerabilities in modern cars: [Electronic resource]. -16.01.2023 – URL: https://habr.com/ru/companies/cloud4y/articles/710906 /.

[19] Car hacking: remote access and other security issues: [Electronic resource]. -11.13.2022 – URL: https://www.osp.ru/pcworld/2012/11/13018020.

[20] Vulnerability in the CAN protocol affecting almost all modern cars: [electronic resource]. -2018 – URL: https://www.opennet.ru/opennews/art.shtml?num=47039.

[21] Data bank of information security threats of the Federal Service for Technical and Export Control of Russia: [website]. – URL: https://bdu.fstec.ru.