Моделирование работы управляющих поверхностей ЛА (см. рис. 2–7) выполнено в относительных единицах при допущении об идеальности исполнительных механизмов. При этом использовались некоторые значения аэродинамических коэффициентов, приведенные в Приложении III источника [1], в котором указаны аэродинамические характеристики для гипотетического самолета.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Буков В.Н.* Адаптивные прогнозирующие системы управления полетом. – М.: Наука. Гл. ред. физ.-мат. лит., 1987.
2. *Мирошник И.В., Никифоров В.О., Фрадков А.Л.* Нелинейное и адаптивное управление сложными динамическими системами. – СПб.: Наука, 2000.
3. *Колесников А.А.* Синергетическая теория управления. – М.: Энергоатомиздат, 1994.
4. *Колесников А.А., Мушенко А.С.* Синергетическое управление процессами пространственного движения летательных аппаратов // Авиакосмическое приборостроение. – 2004. – № 2. – С. 38-45.
5. Современная прикладная теория управления. Ч. II: Синергетический подход в теории управления / Под. ред. А.А. Колесникова. – М.-Таганрог: Изд-во ТРТУ, 2000.
6. Современная прикладная теория управления. Ч. III: Новые классы регуляторов технических систем / Под. ред. А.А. Колесникова. – М.-Таганрог: Изд-во ТРТУ, 2000.

Статью рекомендовал к опубликованию д.т.н., профессор А.В. Боженюк.

Мушенко Алексей Сергеевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: mushenko.alexey@gmail.com; 347900, г. Таганрог, ул. Чехова, 2; тел.: 88634318090; кафедра синергетики и процессов управления; к.т.н.; старший научный сотрудник.

Mushenko Alexey Sergeevich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: mushenko.alexey@gmail.com; 2, Checkhov street, Taganrog, 347928, Russia; phone: +78634318090; the department of synergetics and control; cand. of eng. sc.; senior scientist.

УДК 656.13:681.518+343.982.3

А.О. Пьявченко

ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К АВТОМОБИЛЬНОЙ ПОДСИСТЕМЕ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ВОДИТЕЛЯ

Рассмотрена необходимость создания высоконадежных, защищенных от несанкционированного доступа автомобильных подсистем идентификации водителя. Приведен краткий обзор по современным методам биометрической идентификации. Указывается на то, что решения в биометрических системах идентификации принимаются на основе вероятностного характера полученной информации. В связи с этим, отмечена необходимость комплексного подхода к решению проблемы создания подсистемы. Определены основные признаки конкурентно-способной автомобильной подсистемы идентификации, базирующейся на принципах интеграции выбранных методов биометрической идентификации с RFID- и DSP-технологиями. Отмечено, что в процессе проектирования подсистемы необходимо учитывать физические и психологические условия ее применения, простоту эксплуатации и обучения.

Автотранспортное средство; подсистема многоуровневой биометрической идентификации; идентификационный код; биодинамическая подпись; DSP- и RFID-технологии; беспроводная и спутниковая связь с диспетчерским пунктом.

A.O. Pyavchenko

FUNCTIONAL REQUIREMENTS TO THE AUTOMOBILE SUBSYSTEM OF BIOMETRIC IDENTIFICATION OF THE DRIVER

The need of creation of a reliable automobile subsystem of identification of the driver protected from unauthorized access is observed. The brief review of modern methods of biometric identification is discussed. That decisions in biometric systems of identification are accepted on the basis of probabilistic nature of the received information is underlined. In this connection, necessity of the comprehensive approach to the decision of a problem of creation of a subsystem is noted. The basic attributes of an automobile subsystem of identification which is based on complex realization of the chosen methods of biometric identification with simultaneous application RFID- and DSP-technologies, are described. It is noted, that during designing a subsystem it is necessary to consider physical and psychological conditions of its application, the simplicity of maintenance and training.

The motor vehicle; subsystem of multilevel biometric identification; identification code; authorization; registration; biological characteristics of the person; DSP- and RFID-technologies; wireless and a satellite communication with a master station.

Практически любая компания, имеющая собственный автопарк, должна производить мониторинг транспорта в силу необходимости контроля угона транспорта, деятельности недобросовестных сотрудников, проверки маршрутов движения транспорта на предмет их оптимальности, учета расхода топлива, оптимизации работы всего автопарка, повышения безопасности его работы [1]. Для решения перечисленных проблем необходимо повсеместное внедрение систем автоматизированного мониторинга автотранспорта GPS/ГЛОНАСС, эффективность которых во многом зависит от надежности встроенных в них автомобильных подсистем идентификации водителей (АПИВ), управляющих отслеживаемыми автотранспортными средствами в конкретные промежутки времени.

В настоящее время наиболее простыми, применяемыми на автотранспорте средствами идентификации, являются запоминаемые коды (числовые последовательности) или вещественные идентификаторы, решение по которым о допуске водителя к эксплуатации автомобиля принимается детерминировано. Ошибки здесь возможны только при аппаратных неисправностях (например, порча носителя кода) или программных сбоях подсистемы идентификации [1, 2, 3]. Тем не менее основным недостатком таких средств идентификации являются их слабая защита от подделки, незащищенность от использования идентификатора другим лицом.

Как показывают результаты анализа современных подходов к проблеме идентификации водителя, степень надежности АПИВ можно увеличить, если при ее построении использовать многоуровневые методы идентификации, аутентификации и авторизации водителя, базирующиеся на результатах последних научно-технических достижений в области биометрии. Биометрия – это использование для идентификации и аутентификации биологических характеристик человека как статических биометрических параметров: отпечатков пальцев, геометрии руки, сетчатки и/или радужной оболочки глаза, геометрической трехмерной формы лица, термограммы лица, ДНК, так и динамических параметров: голоса, формы и динамики сердцебиения, динамики воспроизведения рукописной подписи или рукописного текста и т.п. Решения в биометрических системах идентификации принимаются на основе вероятностного характера полученной информации. В этом случае ошибки в принятии решений неизбежны, и можно говорить только о снижении уровня вероятности появления ошибок. Уровень этих ошибок и будет являться критерием качества системы. Этот критерий, как правило, определяется двумя техническими характеристиками [4]:

- вероятностью несанкционированного допуска, выраженной в процентах числа допусков системой неавторизованных лиц (ошибка FAR (False Accept Rate));
- вероятностью ложного задержания, выраженной в процентах числа отказов в допуске системой авторизованных лиц (ошибка FRR (False Reject Rate)).

Таким образом, подсистема не должна отвергать подлинную личность – не совершать FRR-ошибку, всегда отказывать в допуске фальсифицированной личности, т.е. не совершать FAR-ошибку.

Исследования показывают [2], что величина FAR-ошибки определяет защищенность системы от несанкционированного допуска, и снижение ее величины более важно, чем FRR-ошибки. Пределы, в которых находится эта величина, в настоящее время составляют от 0,0001 до 0,1 %. FRR-ошибка в основном влияет на пропускную способность системы. Если подсистема не допустила водителя с первого раза, то можно ввести данные вторично. Конечно, это приводит к снижению пропускной способности, но зато надежность системы не ухудшается. Пределы, в которых находится величина FRR-ошибки, в современных системах составляют от 0,1 до 1 %. Сортировать и сравнивать описанные выше биометрические методы по величине FRR-ошибок достаточно сложно, так как зачастую имеем большой статистический разброс их значений для одних и тех же методов. Причиной тому является сильная зависимость самих методов от оборудования, на котором они реализованы [1].

По величине FAR-ошибки общая сортировка методов биометрической аутентификации выглядит так (от лучших к худшим): ДНК, радужная оболочка глаза, сетчатка глаза, форма и динамика сердцебиения, отпечаток пальца, термография лица, форма ладони, форма лица, расположение вен на кисти руки и ладони, подпись и, наконец, голос. Метод аутентификации водителя по ДНК является контактным и к тому же в настоящее время он слишком дорог, что в целом делает его неприемлемым для массового применения в составе подсистемы идентификации водителя.

Наиболее интересным и перспективным на наш взгляд, с низким уровнем вероятности подделки является метод биодинамической подписи (Bio-Dynamic Signature (BDS)), основанный на использовании электрокардиографических данных водителя, электрических импульсов нервной системы в целях аутентификации личности водителя. Исследователи компании IDesia [5] обратили внимание на то, что при работе сердца на фоне общих признаков, свойственных другим живым сердцам, проявляются мельчайшие индивидуальные различия, присущие конкретному человеку. Данные индивидуальные различия получили название биодинамической подписи (рис. 1). На основании проведенных исследований разработчиками был сделан вывод об уникальности и постоянстве (независимо от возраста и состояния здоровья) биодинамической подписи.

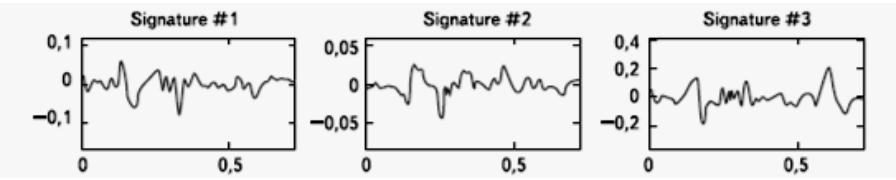

Рис. 1. Образцы биодинамической подписи

Метод биодинамической подписи обладает тем преимуществом, что при его использовании оказывается возможным осуществление экспресс-контроля за общим состоянием сердечно-сосудистой и нервной системы водителя как при аутентификации, так и при управлении автомобилем (если датчики встроить в по-

верхность рулевого колеса автомобиля). К недостатку метода следует отнести его сравнительно низкую помехоустойчивость и довольно длительное время аутентификации – до 8 с в зависимости от требуемого уровня точности [5].

Отпечаток пальца – достаточно дешевый метод идентификации, широко применяемый отечественными производителями автомобильных противоугонных систем. Работают считыватели отпечатков пальцев по следующему принципу: человек прикладывает один из пальцев к рабочему окну (датчику) и запускает процесс сканирования. Дактилоскопический сканер считывает узор папиллярных линий поверхности кожи пальца, корректирует пространственное расположение скана, преобразовывает его в двоичный код и отсылает в DSP-микроконтроллер для предварительной обработки и сравнения по характеристическим признакам, хранящимся в энергонезависимой памяти контроллера [6]. Как правило, процесс сравнения работает в двух режимах (один к одному и один ко многим). В первом случае предъявляемый отпечаток пальца сравнивается с его предполагаемым цифровым шаблоном, хранящимся в базе данных, на предмет идентичности одного к другому. Во втором случае похожий отпечаток пальца ищется в массиве других цифровых шаблонов базы данных, и если похожий отпечаток находится, то это означает, что предъявляемый отпечаток является подлинным. Основным преимуществом дактилоскопического метода является то, что у водителя «идентификатор всегда с собою» и его невозможно потерять. При этом для надежности в считывателях, как правило, имеется возможность зарегистрировать сразу несколько пальцев, начиная с большого, что значительно повышает уровень защиты от НСД. К недостаткам метода следует отнести незащищенность от подделки (от использования муляжа пальца), неустойчивость к загрязнению поверхности датчика, к физическим повреждениям поверхности кожи на «контрольных» пальцах, что весьма вероятно в условиях эксплуатации подержанного автотранспорта. Тем не менее следует указать на успешное применение данного метода в многоуровневых системах защиты совместно с температурными датчиками и датчиками сердцебиения, применение которых позволяет защититься от простых муляжей и решить проблему экспресс-контроля состояния водителя как перед началом его смены, так и в процессе вождения.

Среди методов идентификации также следует обратить внимание на регистрацию микровибраций тела водителя. Дело в том, что незаметно для окружающих и для самих людей их тела подвержены микровибрации [7]. Как и всякая другая вибрация, этот физический процесс имеет волновую природу. Причем частота и диапазон этих волн от вибрации на подсознательном уровне может изменяться в зависимости от внутреннего состояния человека. Микровибрация улавливается по лицу водителя как профессиональными, так и любительскими видеокамерами, которые в свою очередь передают отснятые кадры цифрового видео в буферную память подсистемы идентификации. Затем специальная программа DSP-микроконтроллера, используя полученные в реальном времени кадры, выполняет оценку всего зарегистрированного процесса микровибрации. На этом феномене и может быть создана технология предварительной оценки психологического состояния водителя. Если человек внутренне спокоен и расслаблен, то он излучает волны микровибрации на более низкой частоте. А если человек агрессивен, то он излучает более высокие частоты. Конечно, можно фиксировать и промежуточные уровни состояния водителя. По результату такой обработки, АПИВ может сформировать и выдать водителю рекомендацию отказаться от предстоящей поездки, о чем также путем отправки SMS-уведомления по GSM-каналу должна быть поставлена в известность диспетчерская служба автопарка. Именно за ней окончательное решение об отстранении психически неуравновешенного водителя от предстоящей поездки.

Следует заметить, что наличие в салоне видеокамеры и средств вибрационного анализа лица пользователя с целью проведения экспресс-анализа психологического состояния водителя перед допуском его к работе должно быть опциональным ввиду повышенной сложности реализации и, как следствие, значительного удорожания проекта АПИВ.

Немаловажным фактором является оперативность внесения в бортовой компьютер автотранспортного средства идентификационного кода водителя, его паспортных данных, маршрутных путевых данных, данных о транспортируемом грузе и прочих транзитных документах, необходимых для функционирования GPS-системы мониторинга, а также для сотрудников соответствующих служб контроля и управления (таможни, ГИБДД). Все рассмотренные выше способы аутентификации не позволяют выполнить данную операцию автоматически. Для этой цели, как правило, может быть использована или загрузка памяти бортового компьютера АПИВ напрямую с серверов диспетчерского пункта автопарка посредством беспроводной сети, удовлетворяющей одной из спецификаций стандарта IEEE 802.11 (например, IEEE 802.11g или IEEE 802.11n), или выдача диспетчером водителю предварительно запрограммированной smart-карты. Среди массы разновидностей smart-карт следует выделить карты, выполненные с применением RFID-технологии (идентификационные бесконтактные карты водителей с установленными на них соответствующими RFID-метками). Как правило, это пассивные RFID-карты, имеющие небольшую дальность обнаружения считывателем, устанавливаемым в салоне автомобиля и работающим на частотах 125 МГц (зона действия от 10 см до 3м), 860–930 МГц (зона действия от 10 см до 8м), 2.4–2.483 ГГц (зона действия от 10 см до 20 м). Пассивные карты получают электроэнергию за счет наведения токов во встроенной антенне, которое происходит во время попадания идентификатора в поле действия считывателя. Пассивные идентификаторы обычно меньше по размеру и намного легче активных, они менее дороги (их цена – 10–30 центов), имеют практически неограниченный срок службы и могут храниться совместно с водительским удостоверением. Производство этих карт освоено рядом российских предприятий, как например, Петербургской электротехнической компанией (PERCo), НПК “СоюзСпецАвтоматика”, фирмами АРСЕК, НЕЛК, СШС, ИСТА, МИККОМ, “ААМ Системз”, СОЛИНГ, BioLink, «Лазерные системы» и другими. Многие из разработанных систем способны конкурировать с зарубежными изделиями по техническим характеристикам при меньшей стоимости. К недостаткам такого подхода следует отнести наличие высокой вероятности потери или кражи RFID-карты.

При проектировании АПИВ необходимо помнить, что сама подсистема как функционально завершенный электронный объект, выполненный в отдельном корпусе, в процессе эксплуатации может подвергаться несанкционированному доступу со стороны злоумышленников с целью подмены или уничтожения хранящейся в ее энергонезависимой памяти идентификационных данных и вывода из строя самой подсистемы. Следовательно, подсистема должна быть защищена от копирования используемых идентификаторов с действующим кодом от манипулирования, включая наблюдение, со стороны злоумышленника при ее функционировании в рабочем режиме с целью получения действующего идентификационного кода, от доступа к ее информационным средствам лиц, не прошедших аутентификацию и соответствующую авторизацию. Также АПИВ должна уметь обнаруживать попытки блокировки со стороны злоумышленника ее корректной работы, регламентированной техническими условиями производителя, при которой нарушается работоспособность, ухудшаются параметры, а затем происходит и повреждение самой подсистемы [9]. К таким событиям следует отнести вскрытие корпу-

са, отключение внешнего питания, отключение или замыкание антенны приемника GPS/ГЛОНАСС, отсутствие/пропадание сети GSM, несанкционированное переключение в роуминг, замена/неисправность SIM-карты, аппаратуры доступа к ней, регистрация значения температуры внутри корпуса, регистрация программных запусков и аппаратных сбоев, регистрация повторных запусков с указанием наиболее вероятной возможной причины, регистрация событий нарушения исходных структур программного кода и данных, отслеживание внешних вторжений по линиям передачи данных и т.п. Регистрация подсистемой любых критических событий должна сопровождаться отправкой SMS-уведомления на диспетчерский пункт автопарка. В случае увольнения работника автопарка в соответствии с действующим законодательством АПИВ должна уметь автоматически уничтожать по команде с диспетчерского пункта автопарка биометрические данные этого работника, ранее хранящиеся во встроенной энергонезависимой памяти подсистемы.

Таким образом, АПИВ для сохранения своей конкурентоспособности в условиях выпуска на рынок разнообразных семейств иммобилайзеров (семейства WOODOO («Альтоника», Россия), охранно-противоугонный комплекс BLACK BUG SUPER BT-85W («Автон», Россия)), ужесточения атак со стороны злоумышленников, должна иметь многоуровневую защиту от НСД, основанную на принципах многоуровневой биометрической идентификации с параллельным применением RFID- идентификации при повышенном уровне защиты генерируемого идентификационного кода. Причем, как уже было отмечено ранее, под многоуровневой биометрической идентификацией подразумевается использование биометрического считывателя отпечатков пальцев водителя в комплексе с интегрированными в руль датчиками сердцебиения и температуры.

Разработка АПИВ должна ориентироваться на создаваемые в настоящее время технологии GPS/ГЛОНАСС – мониторинга грузового и пассажирского автотранспорта, вестись с учетом создаваемых перспективных технологических возможностей отечественных производителей, их производственных мощностей и перспективы сертификации будущего продукта как измерительного средства.

Как ожидается, реализация проекта АПИВ, предполагающего комплексное использование в составе подсистемы наряду с RFID- и DSP-технологиями интегральных биометрических считывателей отпечатков пальцев, датчиков сердцебиения и температуры, позволит по сравнению с существующими подходами:

- в более полной мере реализовать преимущества биометрических систем в обеспечении защиты автомобиля от несанкционированного доступа;
- сделать прозрачным контроль со стороны диспетчерского пункта за количеством водителей, имеющих право доступа к управлению автомобилем, и за временем их нахождения за рулем;
- увеличить пропускную способность автопарка при регистрации прибытия/убытия автотранспортов, перевозимого ими груза, учета маршрутных данных и т.д.;
- снизить при наличии в автомобиле центрального замка вероятность несанкционированного запуска двигателя злоумышленником и, как следствие, вероятность последующего угона самого автомобиля.

В заключение, следует отметить, что при построении АПИВ также необходимо учитывать физические и психологические условия применения подсистемы, стоимость и технологичность изготовления ее аппаратуры, а также легкость в обучении и простоту ее использования персоналом (водителями).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Вакуленко А., Юхин Ю.* Биометрические методы идентификации личности: обоснованный выбор // http://www.bytemag.ru/numbers/index.php?ID=11558.
2. Современные биометрические методы идентификации// http://www.polyset.ru.
3. *Ричард Э. Смит* Аутентификация: от паролей до открытых ключей = Authentication: From Passwords to Public Keys First Edition. – М.: Вильямс, 2002. – С. 432.
4. *Крахмалев А.* Многоуровневая идентификация в системах контроля доступа // http://www.alfatv.ru/main.php?lang_id=1&id=13&_cat_id_=41&_ser_=204.
5. Ученые заменили отпечатки пальцев сердцебиением // http://vesti70.ru/news/full/?id =4385.
6. *Пьявченко А.О., Вакуленко Е.А., Качанова Е.С.* Распределенная автоматизированная система идентификации и контроля доступа: вопросы организации // Известия ЮФУ. Технические науки. – 2008. – № 11 (88). – С. 121-125.
7. *Черенков С., Ибрагимов И.* Биометрия на страже безопасности железнодорожного транспорта // Содружество. – Сентябрь 2010 г. – № 18 (273). – С. 15.
8. *ГОСТ Р 51241-2008.* Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

Статью рекомендовал к опубликованию д.т.н., профессор А.М. Белевцев.

Пьявченко Алексей Олегович – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: aop61@mail.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 88634371656; кафедра вычислительной техники; доцент.

Pyavchenko Aleksey Olegovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: aop61@mail.ru; 44, Nekrasovskiy street, Taganrog, 347928, Russia; phone: +78634371656; the department of computer engineering; associate professor.

УДК 681.526

А.Н. Акользин

СИСТЕМА АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ВОДОНАГРЕВАТЕЛЬНЫМ КОТЛОМ

Рассматривается разработка системы автоматического управления водонагревательным котлом, где в качестве топлива используются отходы нефтепродуктов. Перечислены основные виды теплогенераторов, работающих на отработанном масле. Описан процесс модернизации водонагревательного котла для работы на отработанном масле, также показаны требования для разработки системы управления. На рисунке показана разработанная структурная схема системы управления. Описаны особенности работы системы, проблемы, которые возникали в процессе разработки и способы их решений. В ходе проделанной работы была установлена зависимость между подачей воздуха и масла для стабильной работы водонагревательного котла. Также показан и расписан алгоритм работы водонагревательного котла. Из установленной зависимости между подачей воздуха и масла был сделан вывод, что зависимость между подачей воздуха и масла влияет на время работы водонагревательного котла без неисправностей, а также на отдаваемую полезную мощность. Для более тщательной коррекции работы водонагревательного котла было разработано программное обеспечение.

Водонагревательный котел; автоматическое управление.