



Метод защищенной передачи информации для передвижения автономных транспортных средств

Р. Р. Фаткиева^а, канд. техн. наук, доцент, orcid.org/0000-0003-4065-9611, rikki2@yandex.ru

^аСанкт-Петербургский государственный электротехнический университет «ЛЭТИ», Профессора Попова ул., 5, Санкт-Петербург, 197376, РФ

Введение: существующие в настоящее время системы мониторинга и управления состоянием автотранспортных средств, а также методы построения оптимального маршрута передвижения не позволяют моделировать информационные атаки на инфраструктуру транспортных сетей и осуществлять оценку нарушения функционирования автотранспортных средств. **Цель:** разработать метод передачи информационных сообщений с использованием аппарата дискретной ситуационной сети для повышения безопасности передвижения автономных транспортных средств. **Результаты:** разработаны модели построения маршрута и передвижения автономных транспортных средств. По сравнению с традиционными алгоритмами нахождения кратчайших путей оптимальный маршрут передвижения автономных транспортных средств формируется динамически за счет оценки характеристик сегмента пути, встречающегося на маршруте, и времени, которое затрачивается на достижение пункта назначения. Это обеспечивается при помощи предложенного метода передачи информационных сообщений в дискретной ситуационной сети, где корректировка маршрутной информации осуществляется на базе активных и пассивных решателей с формированием информационных сообщений о нарушениях текущей дорожной обстановки и управляющих сообщений для изменения маршрута передвижения. Для повышения безопасности при передаче информационных сообщений разработаны алгоритмы обеспечения конфиденциальности и достоверности переданных сообщений. **Практическая значимость:** результаты исследования могут быть использованы при проектировании и построении систем управления автономными транспортными средствами, а также для моделирования их передвижения в условиях информационных атак. Благодаря возможности программной реализации алгоритма обеспечения достоверности переданных сообщений достигается практический результат защиты от атак отказа в обслуживании.

Ключевые слова – дискретная ситуационная сеть, децентрализованная сеть, информационная атака, функциональная безопасность, оптимизация маршрута передвижения, алгоритм Дейкстры.

Для цитирования: Фаткиева Р. Р. Метод защищенной передачи информации для передвижения автономных транспортных средств. *Информационно-управляющие системы*, 2023, № 6, с. 46–56. doi:10.31799/1684-8853-2023-6-46-56, EDN: QFOYQC

For citation: Fatkueva R. R. Secure data transmission method for the movement of autonomous vehicles. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 6, pp. 46–56 (In Russian). doi:10.31799/1684-8853-2023-6-46-56, EDN: QFOYQC

Введение

Процесс моделирования транспортных сетей позволяет оптимизировать маршруты передвижения и сократить задержки, тем самым улучшить эффективность транспортных операций. «...транспортное моделирование широко применяется в процессе создания новых дорожно-транспортных узлов и процессов передвижения автотранспортных средств и представляет собой создание рабочей модели дорожного движения, соответствующего движению в реальных условиях на автомобильных дорогах. Как правило, имитационное моделирование производится в специализированном программном обеспечении и является быстрым и удобным способом оценки эффективности организации дорожного движения» [1]. Однако существующие на рынке средства не допускают возможности моделировать передачу информационных сообщений для оптимизации маршрута передвижения автономных транспортных средств (АТС).

Применяемые в настоящее время системы для отслеживания и управления состоянием АТС включают методы:

– анализа функционирования датчиков и CAN-шин, а также бортовых диагностических систем [2–6], которые оценивают работу транспортного средства и на основе отклонений от нормальных параметров функционирования в том числе выявляют потенциальные поломки и предсказывают их возникновение [7, 8]. В рамках этого же направления можно назвать и оценку рисков при использовании АТС [9];

– мониторинга и управления АТС и дорожным движением, которые включают использование средств наблюдения, камер и устройств, установленных на автомобилях [10, 11]. Они также позволяют создать цифровую модель функционирования дороги [12, 13], на основе которой выявляются отклонения при помощи машинного обучения или нейронных сетей [14, 15], что способствует прогнозированию уровня трафика и загрузки дорожных сетей;

— оптимизации передачи сообщений, основывающиеся на поиске функций, с минимизацией уровня потерь. Алгоритмы, заложенные в них, используются как в управлении маршрутами автотранспорта, так и в распределении нагрузки между вычислительными ресурсами и сетями [16, 17].

Однако рассмотренные модели и методы не позволяют осуществлять моделирование информационных атак на инфраструктуру транспортных сетей и нарушение их безопасности. В этих условиях необходимость разработки систем обеспечения информационной безопасности обусловлена как ростом числа АТС с одной стороны, так и возрастанием потенциальных уязвимостей к информационным атакам [18–20] за счет увеличения количества компонентной базы (датчиков, коммуникационных модулей, автопилотов и т. д.) с другой стороны, поскольку нарушение безопасности любого из этих компонентов может иметь серьезные последствия, включая аварии и угрозы жизни.

С учетом перспектив развития АТС и их значимости для общества исследования в области моделирования информационных атак и защиты инфраструктуры АТС являются актуальной и неотъемлемой частью обеспечения их безопасности и надежности. Результаты таких исследований могут привести к разработке эффективных мер по предотвращению и защите от информационных угроз в сфере транспортных сетей.

Модель построения маршрута передвижения АТС

С ростом количества АТС их взаимодействие в сетевой инфраструктуре становится все более сложным и требует эффективной оптимизации маршрутов передвижения для обеспечения безопасного движения. Одним из инструментов решения этой задачи является метод моделирования транспортной инфраструктуры на основе дискретной ситуационной сети (ДСС) [21]. Этот метод позволяет отобразить сложные сценарии взаимодействия АТС в виде графа, где вершины представляют узловые точки транспортной инфраструктуры, а ребра — возможные пути связи между ними. В этих условиях требуется осуществить разработку способа оптимизации маршрута передвижения АТС в децентрализованной сети при информационных воздействиях. Тогда можно утверждать, что АТС перемещаются «по неориентированному графу маршрута с определенной скоростью и могут обмениваться информационными сообщениями о текущей дорожной обстановке. Это требует сформировать описание структуры сети, позволяющей осуществлять

передачу информационных сообщений, которые содержат сведения о состоянии АТС и особенностях его функционирования, а также отражают изменение окружающей обстановки при передвижении транспортного средства по неориентированному графу» [21]. С учетом этого для построения маршрута разработаем модель карты, на основании которой формируется маршрут. Одним из вариантов представления карты является граф (сеть), который отвечает следующему виду:

$$K = \langle S, D, Cr, Sl, M \rangle, \quad (1)$$

где S — площадь карты (максимальные параметры графа); D — площадь дорожных покрытий; Cr — множество пересечений (промежуточные вершины графа); Sl — множество решателей (выбор передвижения по графу); M — множество маршрутов передвижения (направление ребер графа).

Алгоритм построения карты можно сформировать в виде шагов.

Шаг 1. Инициализация карты. Карта задается через известные параметры ширины и высоты. В общем виде площадь

$$S = \int_a^b f(x) dx, \quad (2)$$

где $f(x)$ — функция искривления полотна.

Будем считать, что на границах карты допускается формирование стоков и истоков дорог.

Шаг 2. Оценка площади дорожного полотна. При формировании площади дорожного полотна примем также допущение, что оно является прямолинейным, тогда площадь всех дорог, входящих в дорожное полотно, можно представить как сумму площадей всех дорожных полотен, участвующих в формировании маршрута от истока к стоку:

$$D = \sum_{i=1}^N d_i, \quad (3)$$

где D — размер полотна; $d_i = a_i \cdot b_i$, a_i — ширина i -го дорожного полотна, b_i — длина i -го дорожного полотна, ограниченного истоком и стоком; i — идентификатор дороги.

Использование (3) позволяет выявить площадь участков полотна, не задействованных в движении, как разность площадей ($S - D$), что дает возможность осуществить сегментацию участков, не задействованных в движении.

Шаг 3. Построение набора свойств дорожной разметки для каждого d_i -го дорожного полотна:

$$R = (r_1(\text{type}, v), r_2(\text{type}, v), \dots, r_M(\text{type}, v)), \quad (4)$$

где r_i — элемент дорожной разметки; $type$ — вид разметки; v — объем нанесения.

Шаг 4. Нахождение и построение пересечений дорожных полотен, для чего осуществляется:

4.1. Разбиение площади дорожного полотна (3), располагающегося между истоком и стоком, на множество интервалов длиной

$$L = (l_1^{d_i}, l_2^{d_i}, \dots, l_c^{d_i}), \quad (5)$$

где $l_c^{d_i}$ — количество интервалов разбиения для i -го дорожного полотна.

4.2. Вычисление на площади карты (2) контрольной точки K с координатами (x, y) , позволяющей задать координаты i -го интервала относительно данной точки.

4.3. Формирование множества идентификаторов пересечения дорог (перекрестков)

$$Cr = (Cr_1, Cr_2, \dots, Cr_N) \quad (6)$$

с помощью сравнения попадания в границы координат интервалов:

$$Cr_n = d_i \cap d_j = \{l_c^d \mid l_c^d \in d_i \cap l_c^d \in d_j\}. \quad (7)$$

Шаг 5. Нахождение сегмента дорожного полотна, заключенного между идентификаторами пересечения дорог:

$$d_{(Cr_n, Cr_{n+1})} = U_c l_c^d. \quad (8)$$

Это дает возможность построить множество сегментов маршрута и присвоить каждому сегменту весовой коэффициент γ , позволяющий определить свойства сегмента маршрута (например, задержки в пути):

$$C = (d_{(Cr_n, Cr_{n+1})}(\gamma_1), d_{(Cr_{n+1}, Cr_{n+2})}(\gamma_2), \dots, d_{(Cr_{N-1}, Cr_N)}(\gamma_N)). \quad (9)$$

Шаг 6. Назначение уникального идентификатора ID каждому сегменту дорожного полотна: $d_{(Cr_n, Cr_{n+1})}^{ID}$.

Шаг 7. Формирование множества пассивных решателей, для этого:

7.1. Определение координаты нахождения пассивного решателя, в частном случае можно использовать равноудаленное позиционирование пассивного решателя относительно центра дороги.

7.2. Присваивание множеству пассивных решателей уникальных идентификационных номеров:

$$Slp = (Slp_1^{d_i}, Slp_2^{d_i}, \dots, Slp_G^{d_i}), \quad (10)$$

где $Slp_G^{d_i}$ — количество пассивных решателей на d_i -м дорожном полотне.

7.3. Присваивание пассивного решателя подмножеству элементов дорожной разметки r_m из множества R (4):

$$Slp^{d_i} \in r_m. \quad (11)$$

Шаг 8. Формирование множества активных решателей, для этого:

8.1. Определение координаты нахождения активного решателя, который находится в границах пересечения дорог согласно (7).

8.2. Присваивание множеству активных решателей уникальных идентификационных номеров:

$$Sla = (Sla_1^{d_i}, Sla_2^{d_i}, \dots, Sla_g^{d_i}), \quad (12)$$

где $Sla_g^{d_i}$ — количество активных решателей на d_i -м дорожном полотне.

8.3. Присваивание активного решателя подмножеству элементов дорожной разметки r_m из множества R (4):

$$Sla^{d_i} \in r_m. \quad (13)$$

Шаг 9. Построение кратчайших путей в графе (сети). Учитывая в расчете значение весового коэффициента γ (9) при построении сети, основанного на различных известных характеристиках дороги, например: образование пробок, нахождение лежащего полицейского на конкретном участке дороги, — активный решатель формирует решение о дальнейшем движении автомобиля. В частном случае целесообразно рассмотреть построение маршрута с учетом в качестве весового коэффициента времени прохождения пути, тогда:

9.1. Представление множества сегментов дорог в виде графа с учетом введенных весов γ (9), ребер и выделенных вершин.

9.2. Определение первой ближайшей к стоку вершины как вершины истока.

9.3. Выбор подмножества v вершин, принадлежащих множеству V , ближайших к вершине-истоку, с учетом значений веса расстояния $d(\gamma)$. Определение их как непомяченных $v^*(d)$.

9.4. Для найденных вершин расчет времени задержки в них как $t = d/s + z$, где d — расстояние; s — скорость АТС, развиваемая на данном расстоянии; z — временные задержки, вызванные пассивными решателями на указанном пути.

9.5. Среди непомяченных вершин зафиксировать вершину с наименьшим весом, т. е. $v^*(d)$. Дальнейшее рассмотрение начинается с нее, с повторением шагов 9.2–9.5. Зафиксировать ре-

бра из вершины, найденной на шаге 9.2, в вершину, найденную на шаге 9.5. При этом зафиксированную на шаге 9.2 вершину считать помеченной и исключить из рассмотрения.

9.6. В случае если все вершины графа окажутся помеченными, алгоритм свою работу завершает.

Модель передвижения АТС

Передвижение АТС осуществляется с учетом информационных сообщений, полученных от решателей. Найдем близлежащий к АТС решатель из множества доступных решателей (12) за счет выявления максимального сигнала $signal(Sla_n)$, исходящего от решателей, находящихся в подмножестве видимости:

$$Sla = (signal(Sla_1), (signal(Sla_2), \dots, (signal(Sla_g))), \quad (14)$$

или по оценке местонахождения ближайшего решателя исходя из его координат.

Для выявленных решателей совершаем следующие действия:

1. Формируем сообщения об идентификации АТС в сетевой инфраструктуре ДСС. Для этого выделим сообщение M_w , позволяющее определить местонахождение АТС:

$$M_w = \langle t, w, d_{stock}, k \rangle, \quad (15)$$

где t — время появления АТС в истоке; w — уникальный идентификатор АТС отправителя; d_{stock} — место назначения АТС (идентификатор стока); k — координаты нахождения АТС.

2. На основании полученных координат от АТС фиксируем пункт места назначения и задаем функцию передвижения. Решатель осуществляет данную процедуру, проведя следующие мероприятия:

2.1. Построение наикратчайшего пути согласно шагу 9.

2.2. Формирование управляющего сообщения о передвижении АТС для последующей оптимизации маршрута с учетом информации о нарушениях и (или) препятствиях, которые могут произойти на его пути:

$$M_j = \langle w, l \rangle, \quad (16)$$

где M_j — уникальный идентификатор сообщения; l — управляющее сообщение с маршрутом передвижения.

2.3. Построение маршрута передачи сообщений о АТС на основе информации о количестве тактов ДСС с использованием информации, по-

лученной в (2) и (3), и распространение его по ДСС:

$$M_M = \langle w, l, p \rangle, \quad (17)$$

где M_M — уникальный идентификатор сообщения о маршрутизации сообщений; p — технические характеристики АТС.

3. Регистрируем оперативную информацию о прохождении АТМ контрольных точек маршрута. Для этого по маршруту сети АТС передвигается с передачей оперативной информации близлежащему решателю о времени прохождения контрольных точек маршрута для возможности построить новый маршрут с учетом вероятных нарушений в траектории движения:

$$M_{oi} = \langle w, l, oi \rangle, \quad (18)$$

где M_{oi} — оперативная информация о времени прохождения контрольных точек маршрута; oi — время прохождения контрольных точек маршрута АТС.

4. На основании (18) решателем осуществляется коррекция:

— маршрутизации транспортных средств, находящихся в пути, с использованием сообщений согласно (16);

— маршрута передачи сообщений о передвижении автономного наземного транспортного средства между решателями в ДСС.

Метод защищенной передачи информационных сообщений в ДСС

Как было упомянуто ранее, активным решателям известна информация о весах дороги, но ничего не известно о препятствиях, возникающих во время движения на дорогах. Это приводит к тому, что активный решатель не может правильно предложить оптимальный маршрут до получения соответствующей информации о возможных нарушениях передвижения. Тогда для коррекции маршрутной информации АТС формируют информационные сообщения о нарушениях, учитывая текущую дорожную обстановку. Это позволяет скорректировать и выбрать оптимальный маршрут других АТС.

Рассмотрим метод передачи информационных сообщений в ДСС со стороны АТС.

1. Пусть АТС движется с скоростью $V(t)$. При обнаружении препятствий или нарушений движения на дорогах АТС изменяет скорость передвижения с формированием для активного решателя информационного сообщения, содержащего характеристику, подлежащую коррекции (например, в частном случае это скорость или

необходимость перестроиться на соседнюю полосу), и описание сегмента дороги, на котором происходит изменение характеристики функционирования АТС. Для этого сформируем сообщение, аналогичное сообщению (18):

$$M_{oi} = \langle w, l, p(V(t)) \rangle, \quad (19)$$

где l – сообщение о сегменте маршрута на пути передвижения АТС.

Тогда возникает задача минимизации количества сообщений в условиях максимизации скорости:

$$V(M) \Rightarrow \min_n \sum_{i=1}^n M_{oi}, \quad (20)$$

где $V(M)$ – максимальная скорость АТС при получении сообщения; n – количество сообщений для формирования маршрутной информации.

2. Анализ оптимального маршрута передачи информационных сообщений предполагает три случая.

Случай 1 – в системе управления АТС присутствует аппарат для построения топологии сети передачи информационных сообщений. Тогда по запросу от АТС с активного решателя загружается информационное сообщение (17), которое позволяет сформировать граф, хранящий информацию о количестве ребер, которые может обойти сообщение. На основании полученного сообщения выполняется построение и заполнение структур данных в модели передачи данных (матрица смежности, инцидентности с построением матрицы маршрутизации).

Случай 2 – анализ топологии выполнить невозможно. В общем случае сообщение планируется к передаче близлежащему решателю.

Случай 3 – имеется информация о всех активных решателях, которые были пройдены на пути движения АТС, актуальная для тех АТС, которым предстоит пройти препятствие. При данных условиях информационное сообщение формируется для всех пройденных АТС решателей (т. е. информация передается в направлении, противоположном движению АТС).

3. Отправка сформированного пакета всем активным решателям, которые находятся от АТС на расстоянии, не превышающем возможное для получения сообщения.

Теперь рассмотрим метод передачи информационных сообщений в ДСС со стороны активного решателя.

При получении сообщения от АТС на стороне активного решателя возникает две задачи:

– формирование маршрута передачи информационного сообщения о нарушениях в дорожной обстановке для соседних активных решате-

лей с широковещательной рассылкой данного сообщения по найденным маршрутам;

– формирование сообщения для АТС, находящихся в сегменте дороги, под влиянием активного решателя, содержащего управляющее воздействие, для оптимизации маршрута передвижения.

4. Для решения задачи 1 со стороны активного решателя осуществляется:

4.1. Проверка достоверности полученного от АТС информационного сообщения и анализ количества сообщений от данного АТС или соседних АТС, движущихся по данному маршруту, для защиты от атак отказа в обслуживании.

4.2. Формирование таблицы маршрутизации указанного сообщения на основании графа топологии активных решателей при условии достоверности сообщения на шаге 4.1. Это позволяет уменьшить загруженность каналов связи ДСС при передаче информационных сообщений.

4.3. Широковещательная рассылка информационных сообщений о нарушении дорожной обстановки.

5. Для решения задачи 2 со стороны активного решателя осуществляется формирование маршрута передвижения АТС, для этого производится:

5.1. Вычисление всех АТС из множества АТС, находящихся в заданном сегменте дороги, для которых требуется изменение маршрута.

5.2. Изменение весового коэффициента, присвоенного каждому сегменту, или исключение данного ребра в зависимости от вида нарушения дорожной обстановки.

5.3. Перерасчет оптимального кратчайшего пути при помощи алгоритма Дейкстры на основании измененных весовых коэффициентов.

5.4. Формирование для АТС управляющего сообщения с новым маршрутом передвижения.

5.5. Передача активным решателям информации об оптимальном маршруте передвижения для АТС, найденных на шаге 5.1, или широковещательная рассылка для всех АТС.

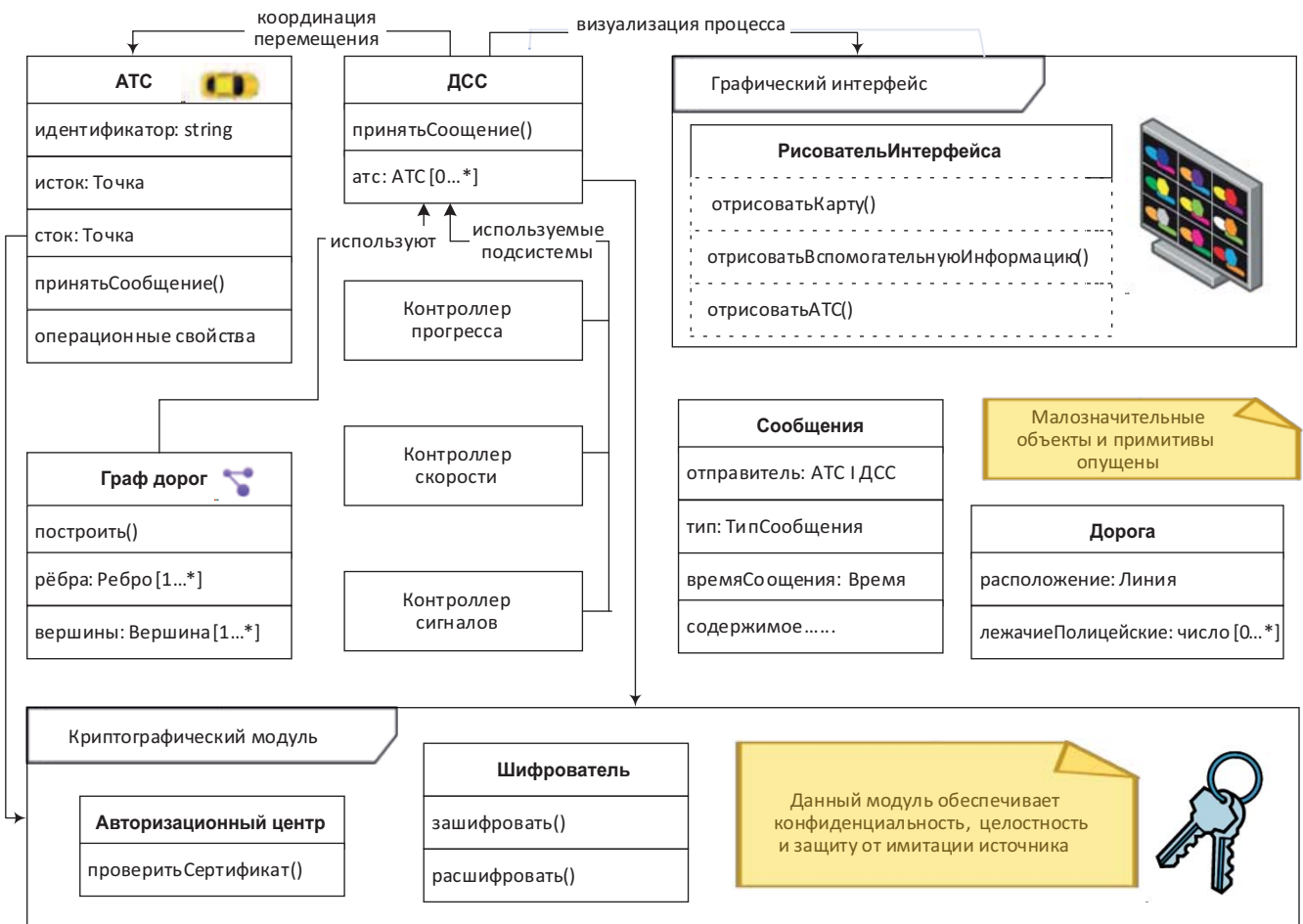
Практическое применение метода

Практическое применение метода защищенной передачи информации для передвижения АТС реализовано в программном комплексе на основе моделирования движения АТС на участке дорожного полотна. АТС движутся из одной точки карты в другую. При этом центральный орган управления АТС отсутствует. Оптимизация движения маршрута идет в определенных узлах данной сети (решателях) и обеспечивается при помощи алгоритма Дейкстры и обмена сообщениями о текущей дорожной обстановке между АТС и решателями. Для разработки програм-

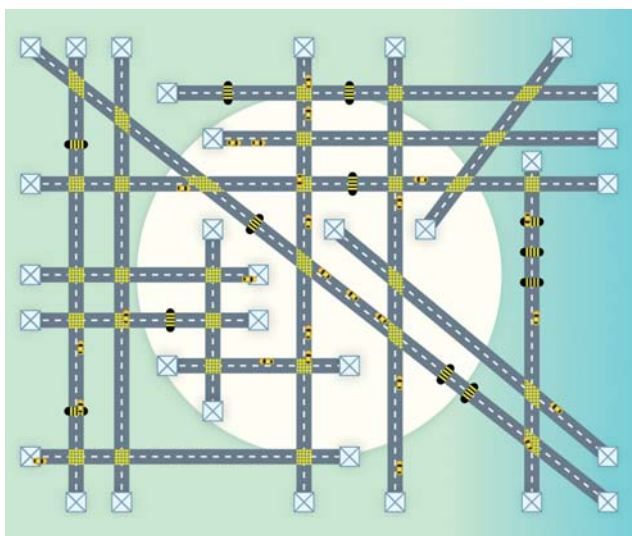
много комплекса был выбран язык программирования TypeScript, для отрисовки карты и создания анимации используются элемент Canvas и библиотеки с открытым исходным кодом React. Программный комплекс оптимизирован, увеличение производительности достигается за счет предварительной индексации данных, которая подразумевает под собой расчет данных из входных параметров. Доступны различные конфигурации окружения для симуляции разнообразных условий улично-дорожной сети. Ядром программы является ДСС-модуль, который работает в дискретные такты и контролирует передвижение АТС, их скорость, а также осуществляет передачу информационных сообщений в каждый рабочий такт. Он обеспечивает работу всей системы при помощи контроллера прогресса, контроллера скорости, контроллера сигналов и криптографического модуля. Архитектура программного комплекса продемонстрирована на рис. 1.

На вход программы поступают данные о множестве дорог и препятствий на них, кото-

рые образуют карту. Структура программы позволяет в любой момент сгенерировать любую другую карту, подав на вход иные параметры. В качестве дальнейшего развития программного комплекса может быть использована процедурно-генерируемая карта. Возможно нанесение двух типов препятствий: пешеходных переходов и лежачих полицейских. Конфигурации заданы по умолчанию, однако их можно модифицировать в процессе работы программы. Они включают в себя загруженность дорог, количество препятствий, количество ребер для передачи информационного сообщения, наличие или отсутствие АТС, включение и отключение режима безопасных сообщений. С учетом их происходит процесс запуска и координация перемещения АТС. После предобработки карты получен граф всех возможных путей следования АТС. Вершинами графа карты являются точки начала и конца каждого перекрестка, стоки и истоки, а участки дороги, находящиеся между вершинами, будут являться ребрами графа (рис. 2).



■ **Рис. 1.** Архитектура программного комплекса
 ■ **Fig. 1.** Architecture of the software package



■ **Рис. 2.** Демонстрация работы программного комплекса
 ■ **Fig. 2.** Demonstration of the software package

Каждый такт основного цикла программы — это такт работы ДСС. В работе основного цикла ДСС использует ядро программы, которое, пользуясь различными контроллерами, координирует передвижение, скорость АТС и контролирует состояние сети в целом. При появлении в сети АТС ему назначается маршрут исходя из стока, в который оно направляется. Каждый такт ДСС проверяет, сколько прошло времени с предыдущего такта, и пересчитывает пройденное АТС расстояние с учетом дорожной обстановки и скоростного индекса карты. Контроллер сигналов (см. рис. 1) координирует перемещение сообщений по сети и реагирует на эти сообщения, внося корректировки в маршрутную информацию и скорость передвижения с учетом обеспечения информационной безопасности АТС. Для этого в каждом АТС предусмотрен криптографический модуль. При включенном криптографическом модуле АТС обмениваются секретным ключом при помощи алгоритма Диффи — Хеллмана. Это позволяет обеспечивать безопасность при перехвате сообщений, т. е. АТС-злоумышленник не сможет использовать информацию о возможных препятствиях, и вектор атаки будет гораздо меньше. Для защиты от атаки отказа в обслуживании проводится анализ трафика. При обнаружении подозрительного трафика, исходящего от какого-либо АТС, активный решатель перестает принимать от него сообщения. Для защиты от модификации данных и имитации источника применен алгоритм электронной цифровой подписи. При запуске АТС по умолчанию получает сертификат условного удостоверяющего цен-

тра, АТС-злоумышленник, напротив, данного сертификата не удостоится.

Для анализа результативности работы разработанного комплекса и проверки достижения поставленной цели повышения безопасности при обмене сообщениями об оптимизации маршрута необходимо оценить уровень функциональной безопасности, достигнутый при разработке. Под функциональной безопасностью в данном программном комплексе подразумевается корректное функционирование системы. Например, за счет уменьшения количества принятых сообщений и увеличения истинности информации. Коэффициент, влияющий на безопасность передвижения:

$$K = \frac{S}{t}, \quad (21)$$

где S — расстояние, пройденное АТС; t — время, затраченное на преодоление расстояния S . Для оценки произведенного эффекта сравним два коэффициента — с использованием и без использования безопасных сообщений:

$$\frac{K_1}{K_2} = \frac{S}{t_s} \div \frac{S}{t_u} \cdot 100 - 100 = \frac{t_u}{t_s} \cdot 100 - 100,$$

где t_u , t_s — время, затраченное на преодоление расстояния S без использования и с использованием безопасных сообщений соответственно.

На первом этапе оценено время в пути АТС с использованием безопасных сообщений и без них. Следует учитывать, что показатели будут равны, если в системе не будут присутствовать АТС-злоумышленники. Поэтому надо проанализировать программный комплекс, внедрив АТС-злоумышленников, приносящих различные информационные угрозы. Фиксирование показателей времени в пути АТС произведено при различных условиях: на коротких и длинных дистанциях, при большей и меньшей загруженности дороги.

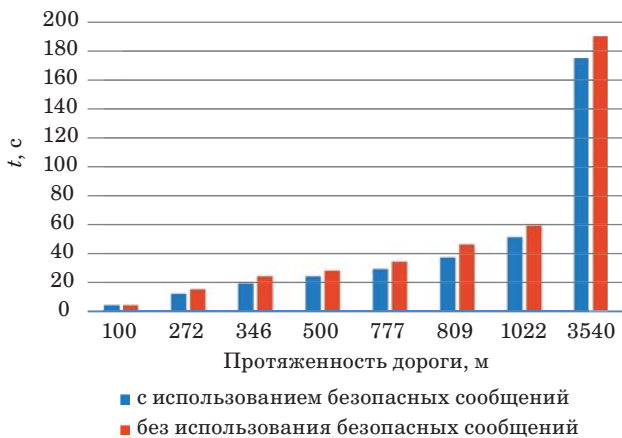
График зависимости времени от протяженности дороги представлен на рис. 3. Данные были получены при неизменной загруженности дороги (табл. 1).

Для оценки загруженности дороги необходимо воспользоваться пространственной характеристикой, определяющей степень стесненности движения, а именно плотность транспортного потока:

$$N_{\text{авт/км}} = \frac{L}{l_d},$$

где

$$l_d = \sum \frac{l_{d_i}}{n}.$$



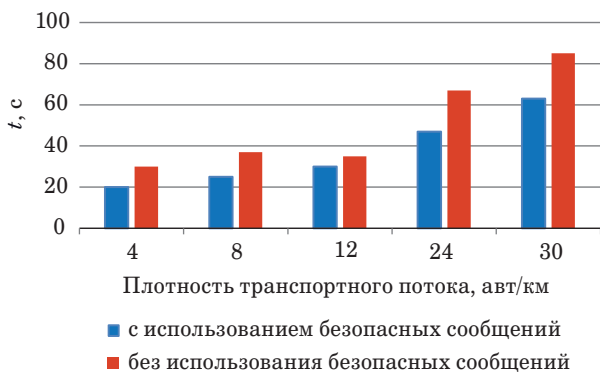
■ **Рис. 3.** Зависимость времени передвижения АТС от протяженности дороги

■ **Fig. 3.** Graph of time dependence on the length of the road

Здесь L — длина оцениваемого участка дороги; $l_{дi}$ — расстояние от начала одного АТС до начала впереди идущего АТС; n — количество участков между двумя АТС на заданной длине дороги.

График зависимости среднего времени в пути от плотности транспортного потока представлен на рис. 4. Данные были получены при направлении АТС по конкретному маршруту следования (табл. 2).

По первой выборке получено, что коэффициент безопасности функционирования (21) увеличился на 13 % при различной протяженности дорог при использовании безопасных сообщений. Вторая выборка показала увеличение коэффициента функциональной безопасности на 37 %, что свидетельствует об эффективности предложенных мер.



■ **Рис. 4.** Зависимость времени передвижения АТС от плотности транспортного потока

■ **Fig. 4.** Graph of time dependence on traffic flow density

■ **Таблица 1.** Зависимость времени в пути от протяженности дорог

■ **Table 1.** Dependence of travel time on the length of roads

Протяженность дороги, м	Время в пути, с	
	с использованием безопасных сообщений	без использования безопасных сообщений
100	5	5
272	13	16
346	20	25
500	25	29
777	30	35
809	38	47
1022	52	60
3540	175	190
Среднеквадратичное отклонение	54,6	58,7

■ **Таблица 2.** Зависимость времени в пути от плотности транспортного потока

■ **Table 2.** Dependence of travel time on the length of roads

Плотность потока, авт/км	Время в пути, с	
	с использованием безопасных сообщений	без использования безопасных сообщений
4	20	30
8	25	37
12	30	35
24	47	67
30	63	85
Среднеквадратичное отклонение	17,73	24

Заключение

В исследовании был разработан и реализован программный комплекс для обеспечения безопасности и оптимизации маршрута передвижения АТС. В ходе работы рассмотрены различные аспекты безопасности, включая криптографическую защиту, анализ трафика и алгоритмы электронной цифровой подписи. Для оценки эффективности предложен коэффициент безопасности, учитывающий расстояние, пройденное АТС, и время, затраченное на преодоление этого расстояния. Сравнение этого коэффициента с использованием защищенных сообщений и без их

использования позволило оценить достижение поставленной цели — повышение безопасности при обмене сообщениями об оптимизации маршрута. К дальнейшему направлению исследования целесообразно отнести усовершенствование криптографических методов, анализа трафика и

системы обнаружения атак для более надежной защиты от различных видов угроз, а также проведение более широкого анализа и тестирования в различных условиях и сценариях функционирования.

Литература

1. Кольшкина Д. В., Дрогачева Я. А., Шевцова А. Г. Обзор программ имитационного моделирования движения транспортных потоков. *Воронежский научно-технический вестник*, 2019, т. 3, № 3(29), с. 111–117. EDN: SBZGHF
2. Zeina A., Qutaiba A. I. Examining the effects of exteroceptive sensors of autonomous vehicles (AV) on CAN bus. *International Journal of Sensors, Wireless Communications and Control*, 2023, vol. 13, no. 4, pp. 270–283. <https://dx.doi.org/10.2174/2210327913666230824145823>
3. Campos-Ferreira A. E., Lozoya-Santos J. d. J., Tudon-Martinez J. C., Mendoza R. A. R., Vargas-Martinez A., Morales-Menendez R., Lozano D. Vehicle and driver monitoring system using on-board and remote sensors. *Sensors*, 2023, no. 2: 814. <https://doi.org/10.3390/s23020814>
4. Song H. M., Kim H. K. Discovering CAN specification using on-board diagnostics. *IEEE Design & Test*, 2021, vol. 38, no. 3, pp. 93–103. doi:10.1109/MDAT.2020.3011036
5. Abhinand K. K., Bavos A., Achankunju T. A., Joseph J., John S., Kumar S. N. *IoT-based driving pattern analysis and engine sensor damage prediction using onboard diagnostics*. Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems. Springer, 2023, vol. 588, pp. 425–432. https://doi.org/10.1007/978-981-19-7982-8_35
6. Kumar R., Jain A. Classification by vehicle OBD data using machine learning. *J Supercomputer*, 2023, vol. 79, pp. 18800–18819. <https://doi.org/10.1007/s11227-023-05364-3>
7. Rimpas D., Papadakis A. Driving events identification and operational parameters correlation based on the analysis of OBD-II timeseries. *Proc. of the 8th Intern. Conf. on Vehicle Technology and Intelligent Transport Systems*, 2022, pp. 257–264. <https://doi.org/10.5220/0011036400003191>
8. Meenakshi, Nandal R., Awasthi N. OBD-II and big data: A powerful combination to solve the issues of automobile care. *Computational Methods and Data Engineering. Advances in Intelligent Systems and Computing*, 2021, vol. 1257, pp. 172–189. https://doi.org/10.1007/978-981-15-7907-3_14
9. Yang T., Murguia C., Lv C. Risk assessment for connected vehicles under stealthy attacks on vehicle-to-vehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, 2023, pp. 1–12. doi:10.1109/TITS.2023.3292188
10. Redmill K. A., Yurtsever E., Mishalani R. G., Coifman B., McCord M. R. Automated traffic surveillance using existing cameras on transit buses. *Sensors*, 2023, no. 11: 5086. <https://doi.org/10.3390/s23115086>
11. Choudhary A., Mian T., Fatima S., Panigrahi B. K. Deep transfer learning based fault diagnosis of electric vehicle motor. *IEEE Intern. Conf. on Power Electronics, Drives and Energy Systems (PEDES)*, 2022, pp. 1–6. doi:10.1109/PEDES56012.2022.10080274
12. Zhao M., Zhao N. Method for the construction of urban road digital elevation models integrated with semantic information. *Applied Sciences*, 2023, vol. 13, no. 7: 4210. <https://doi.org/10.3390/app13074210>
13. Svaty Z., Vrtal P., Kouhout T., Nouzovsky L. Automated detection and vectorization of road elements in high resolution orthographic images. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 2023, vol. XLVI-II-5/W2-2023, pp. 111–116. <https://doi.org/10.5194/isprs-archives-XLVI-II-5-W2-2023-111-2023>
14. Sharma H., Shrivastava V., Bharti K. K., Wang L. Smart city: Road traffic monitoring system based on the integration of IoT and ML. *Communication and Intelligent Systems*, 2022, vol. 686, pp. 177–189. https://doi.org/10.1007/978-981-99-2100-3_12
15. Zhong W., Du L. Predicting traffic casualties using support vector machines with heuristic algorithms: A study based on collision data of urban roads. *Sustainability*, 2023, vol. 15, no. 4: 2944. <https://doi.org/10.3390/su15042944>
16. Annu P., Rajalakshmi P., Praveen Tammana. Optimizing latency for real-time traffic and road safety applications through MEC-based V2X system. *Intern. Conf. on Smart Applications, Communications and Networking (SmartNets)*, Istanbul, Turkiye, 2023, pp. 1–8. doi:10.1109/SmartNets58706.2023.10215515
17. Nafi N. S., Khan R. H., Khan J. Y., Gregory M. A predictive road traffic management system based on vehicular ad-hoc network. *Australasian Telecommunication Networks and Applications Conference (ATNAC)*, Southbank, VIC, Australia, 2014, pp. 135–140. doi:10.1109/ATNAC.2014.7020887
18. Fatkueva R. R. Application of attack graphs to simulate the violation of the movement of vehicles in the convoy. *XXVI Intern. Conf. on Soft Computing and Measurements (SCM)*, Saint-Petersburg, Russian Federation, 2023, pp. 248–251. doi:10.1109/SCM58628.2023.10159111
19. Kong H. K., Hong M. K., Kim T. S. Security risk assessment framework for smart car using the attack

tree analysis. *Journal of Ambient Intelligence and Humanized Computing*, 2018, vol. 9, pp. 531–551. <https://doi.org/10.1007/s12652-016-0442-8>

20. Wang Y., Huang A., Yang F., Bian N., Zhang J., Guo L. Systematic assessment of cyber-physical security of lane keeping control system for autonomous vehicles. *Security and Safety*, 2023, vol. 2, 2023027, pp. 6. <https://doi.org/10.1051/sands/2023027>

21. Fatkueva R. R., Korytov P. V. Assessment of applicability of discrete situational networks for information transmission in intelligent transport networks. *Automatic Documentation and Mathematical Linguistics*, 2022, vol. 56, pp. 70–75. <https://doi.org/10.3103/S0005105522020029>

UDC 656.021, 004.75

doi:10.31799/1684-8853-2023-6-46-56

EDN: QFOYCC

Secure data transmission method for the movement of autonomous vehicles

R. R. Fatkueva^a, PhD, Tech., Associate Professor, orcid.org/0000-0003-4065-9611, rikki2@yandex.ru

^aSaint-Petersburg Electrotechnical University «LETI», 5, Prof. Popov St., 197376, Saint-Petersburg, Russian Federation

Introduction: Current vehicle monitoring and management systems, as well as methods for route optimization do not permit modeling cyberattacks on the transportation infrastructure nor assessing the disruption of traffic flow. **Purpose:** To develop a method for transmitting information messages using a discrete situational network device to improve the safety of autonomous vehicles. **Results:** We develop models of route construction and autonomous vehicle movement. Compared with traditional algorithms for finding the shortest paths, the route optimization for autonomous vehicles is carried out dynamically by evaluating the characteristics of the segment of the path encountered on the route and the time it takes to reach the destination. This is ensured by the proposed method of transmitting information messages in a discrete situational network, where the correction of route information is carried out on the basis of active and passive solvers accompanied by the formation of information messages about the disruptions of the current traffic situation as well as control messages for changing the route of movement. To improve the security of the transmission of information messages, we develop algorithms that ensure the confidentiality and reliability of the transmitted messages. **Practical relevance:** The results of the study can be used in the design and construction of control systems for autonomous vehicles, as well as for modeling their movement under the conditions of cyberattacks. Owing to the possibility of software implementation of the algorithm to ensure the reliability of transmitted messages, a practical result of protection against denial-of-service attacks is achieved.

Keywords – discrete situational network, decentralized network, cyberattack, functional security, route optimization, Dijkstra algorithm.

For citation: Fatkueva R. R. Secure data transmission method for the movement of autonomous vehicles. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 6, pp. 46–56 (In Russian). doi:10.31799/1684-8853-2023-6-46-56, EDN: QFOYCC

References

- Kolyshkina D. V., Drogacheva Y. A., Shevtsova A. G. Overview of traffic flow simulation programs. *Voronezh Scientific and Technical Journal*, 2019, vol. 3, no. 3(29), pp. 111–117 (In Russian). EDN: SBZGHH
- Zeina A., Qutaiba A. I. Examining the effects of exteroceptive sensors of autonomous vehicles (AV) on CAN bus. *International Journal of Sensors, Wireless Communications and Control*, 2023, vol. 13, no. 4, pp. 270–283. <https://dx.doi.org/10.2174/2210327913666230824145823>
- Campos-Ferreira A. E., Lozoya-Santos J. d. J., Tudon-Martinez J. C., Mendoza R. A. R., Vargas-Martinez A., Morales-Menendez R., Lozano D. Vehicle and driver monitoring system using on-board and remote sensors. *Sensors*, 2023, no. 2: 814. <https://doi.org/10.3390/s23020814>
- Song H. M., Kim H. K. Discovering CAN specification using on-board diagnostics. *IEEE Design & Test*, 2021, vol. 38, no. 3, pp. 93–103. doi:10.1109/MDAT.2020.3011036
- Abhinand K. K., Bavos A., Achankunju T. A., Joseph J., John S., Kumar S. N. *IoT-based driving pattern analysis and engine sensor damage prediction using onboard diagnostics*. In: *Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems*. Springer, 2023, vol. 588, pp. 425–432. https://doi.org/10.1007/978-981-19-7982-8_35
- Kumar R., Jain A. Classification by vehicle OBD data using machine learning. *J Supercomputer*, 2023, vol. 79, pp. 18800–18819. <https://doi.org/10.1007/s11227-023-05364-3>
- Rimpas D., Papadakis A. Driving events identification and operational parameters correlation based on the analysis of OBD-II timeseries. *Proc. of the 8th Intern. Conf. on Vehicle Technology and Intelligent Transport Systems*, 2022, pp. 257–264. <https://doi.org/10.5220/0011036400003191>
- Meenakshi, Nandal R., Awasthi N. OBD-II and big data: A powerful combination to solve the issues of automobile care. *Computational Methods and Data Engineering. Advances in Intelligent Systems and Computing*, 2021, vol. 1257, pp. 172–189. https://doi.org/10.1007/978-981-15-7907-3_14
- Yang T., Murguia C., Lv C. Risk assessment for connected vehicles under stealthy attacks on vehicle-to-vehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, 2023, pp. 1–12. doi:10.1109/TITS.2023.3292188
- Redmill K. A., Yurtsever E., Mishalani R. G., Coifman B., McCord M. R. Automated traffic surveillance using existing cameras on transit buses. *Sensors*, 2023, no. 11: 5086. <https://doi.org/10.3390/s23115086>
- Choudhary A., Mian T., Fatima S., Panigrahi B. K. Deep transfer learning based fault diagnosis of electric vehicle motor. *IEEE Intern. Conf. on Power Electronics, Drives and Energy Systems (PEDES)*, 2022, pp. 1–6. doi:10.1109/PEDES56012.2022.10080274
- Zhao M., Zhao N. Method for the construction of urban road digital elevation models integrated with semantic information. *Applied Sciences*, 2023, vol. 13, no. 7: 4210. <https://doi.org/10.3390/app13074210>
- Svaty Z., Vrtal P., Kouhout T., Nouzovsky L. Automated detection and vectorization of road elements in high resolution orthographic images. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 2023, vol. XLVIII-5/W2-2023, pp. 111–116. <https://doi.org/10.5194/isprs-archives-XLVIII-5-W2-2023-111-2023>
- Sharma H., Shrivastava V., Bharti K. K., Wang L. Smart city: Road traffic monitoring system based on the integration of IoT and ML. *Communication and Intelligent Systems*, 2022, vol. 686, pp. 177–189. https://doi.org/10.1007/978-981-99-2100-3_12
- Zhong W., Du L. Predicting traffic casualties using support vector machines with heuristic algorithms: A study based on

- collision data of urban roads. *Sustainability*, 2023, vol. 15, no. 4: 2944. <https://doi.org/10.3390/su15042944>
16. Annu P., Rajalakshmi P., Praveen Tammana. Optimizing latency for real-time traffic and road safety applications through MEC-based V2X system. *Intern. Conf. on Smart Applications, Communications and Networking (SmartNets)*, Istanbul, Turkiye, 2023, pp. 1–8. doi:10.1109/SmartNets58706.2023.10215515
 17. Nafi N. S., Khan R. H., Khan J. Y., Gregory M. A predictive road traffic management system based on vehicular ad-hoc network. *Australasian Telecommunication Networks and Applications Conference (ATNAC)*, Southbank, VIC, Australia, 2014, pp. 135–140. doi:10.1109/ATNAC.2014.7020887
 18. Fatkiewa R. R. Application of attack graphs to simulate the violation of the movement of vehicles in the convoy. *XXVI Intern. Conf. on Soft Computing and Measurements (SCM)*, Saint-Petersburg, Russian Federation, 2023, pp. 248–251. doi:10.1109/SCM58628.2023.10159111
 19. Kong H. K., Hong M. K., Kim T. S. Security risk assessment framework for smart car using the attack tree analysis. *Journal of Ambient Intelligence and Humanized Computing*, 2018, vol. 9, pp. 531–551. <https://doi.org/10.1007/s12652-016-0442-8>
 20. Wang Y., Huang A., Yang F., Bian N., Zhang J., Guo L. Systematic assessment of cyber-physical security of lane keeping control system for autonomous vehicles. *Security and Safety*, 2023, vol. 2, 2023027, pp. 6. <https://doi.org/10.1051/sands/2023027>
 21. Fatkiewa R. R., Korytov P. V. Assessment of applicability of discrete situational networks for information transmission in intelligent transport networks. *Automatic Documentation and Mathematical Linguistics*, 2022, vol. 56, pp. 70–75. <https://doi.org/10.3103/S0005105522020029>
-

УВАЖАЕМЫЕ АВТОРЫ!

Научная электронная библиотека (НЭБ) продолжает работу по реализации проекта SCIENCE INDEX. После того как Вы регистрируетесь на сайте НЭБ (<http://elibrary.ru/defaultx.asp>), будет создана Ваша личная страничка, содержание которой составят не только Ваши персональные данные, но и перечень всех Ваших печатных трудов, имеющих в базе данных НЭБ, включая диссертации, патенты и тезисы к конференциям, а также сравнительные индексы цитирования: РИНЦ (Российский индекс научного цитирования), h (индекс Хирша) от Web of Science и h от Scopus. После создания базового варианта Вашей персональной страницы Вы получите код доступа, который позволит Вам редактировать информацию, помогая создавать максимально объективную картину Вашей научной активности и цитирования Ваших трудов.
