УДК 004.031, 004.056

А.П. Нырков, С.С. Соколов, А.С. Белоусов, Н.М. Ковальногова, В.А. Мальцев

Обеспечение безопасного функционирования мультисервисной сети транспортной отрасли

Рассмотрены предпосылки создания интегрированного информационно-коммуни-кационного пространства транспортной отрасли, постановка задачи передачи данных в мультисервисной сети транспортной отрасли и методы обеспечения помехозащищенности каналов передачи данных, предложена модель идентификации пользователя в мультисервисной сети.

Ключевые слова: мультисервисная сеть, модель индентификации пользователя, методы кодирования, помехозащищенность каналов, помехоустойчивость, передача данных, интегрированное информационно-коммуникационное пространство транспортной отрасли.

Транспортная стратегия Российской Федерации на период до 2030 г. предусматривает инновационный сценарий повышения конкурентоспособности транспортной системы за счет реализации транзитного потенциала страны. В соответствии с Рамочными стандартами безопасности и облегчения мировой торговли (ВТамО, 2005) требования по обеспечению безопасности теперь должны выполняться через безбумажный документооборот и предварительное информирование о перемещении товаров. Такой подход зафиксирован в Таможенном кодексе РФ и в «Концепции развития российской таможенной службы на период до 2020 года». Он распространяется на систему управления рисками, практику внедрения современных информационных технологий, предварительного информирования таможенных органов о перемещенных товарах и т.п.

Информатизация транспортной отрасли ввиду технического и технологического разнообразия имеет отличительной особенностью многообразие каналов передачи данных, прикладных программных решений и аппаратного обеспечения. Проблемы их безопасного функционирования подробно рассмотрены в работах [1–4].

В связи с повышенным вниманием Правительства и Президента Российской Федерации к развитию транспорта, необходимости качественной интеграции в международное транспортное пространство в рамках вступления России во Всемирную транспортную организацию, на первый план выходит решение вопросов, связанных со стандартизацией типовых операций, унификацией инструментария деятельности и оптимизацией ресурсов. Эти вопросы призваны решить продукты автоматизации основных видов деятельности, которые должны функционировать единым концептуальным информационным целым, образуя собой интегрированное информационно-коммуникационное пространство транспортной отрасли (ИИКП ТО).

Основные предпосылки создания интегрированного информационно-коммуникационного пространства транспортной отрасли. Основной целью создания ИИКП ТО является эффективный синтез имеющегося программно-аппаратного обеспечения процессов транспортной отрасли (ТО).

Основные задачи создания ИИКП ТО [5]:

1. Создание и поддержание бесперебойно функционирующих зарегистрированных и сопровождаемых информационных ресурсов, лицензионного программного обеспечения, а также территориально распределенной развитой вычислительной и коммуникационной инфраструктуры ТО.
2. Создание и внедрение новых форм и методов в управлении ТО в формате электронных регламентов (сервисов) на основе современных информационно-коммуникационных технологий.
3. Обеспечение функционирования ИИКП ТО на основе российских и международных стандартов менеджмента качества (ISO 9001, ISO 20000, ISO/IEC 38500 и др.).
4. Стандартизация и минимизация однотипных рутинных операций и повышение эффективности работы сотрудников ТО путем внедрения и интеграции специализированных приложений и средств коллективной деятельности.
5. Создание качественной инфраструктуры управления отраслевыми знаниями и иными нематериальными активами ТО.
6. Создание оптимальной транспортной среды маршрутизации потоков данных в рамках мультисервисной сети ИИКП ТО.

7. Формирование системы сервисов, поддерживаемых необходимой и достаточной вычислительно-коммуникационной инфраструктурой, для пользователей ИИКП ТО в соответствии с правами, установленными в матрицах доступа соответствующих информационных ресурсов.

8. Соблюдение требований по бесперебойности функционирования ИИКП ТО.

9. Снижение уровня потерь, связанных с принятием неэффективных управленческих решений, вызванных неточностями в служебной информации, несвоевременностью предоставления данных, нарушениями в регламентах использования информации и т.д.

10. Снижение уровня издержек на реализацию стандартных, рутинных, относительно редко изменяющихся служебных процедур и регламентов.

11. Организация системы контроля качества информационных продуктов, создаваемых в рамках работы пользователей и систем в ИИКП ТО.

12. Внедрение программно-целевого подхода при планировании, организации и аудите результатов мероприятий и программ в рамках функционирования ИИКП ТО.

13. Внедрение сервисов ИИКП ТО в рамках развития всех основных процессов, обеспечивающих стабильную работу ТО.

Мультисервисная сеть транспортной отрасли как основа существования интегрированного информационно-коммуникационного пространства транспортной отрасли. Ввиду наличия большого количества сервисов и разнородного программно-аппаратного обеспечения объектов транспортной инфраструктуры основой создания ИИКП ТО является мультисервисная сеть транспортной отрасли (МС ТО), которая по сути своей является сетью связи следующего поколения NGN (Next Generation Networks).

NGN применительно к транспортной сфере концептуально должна обеспечивать предоставление неограниченного объема услуг с гибкой системой управления трафиком, персонализацией (пользовательской или сервисной) и создание новых информационных услуг за счет унификации и эффективного синтеза сетевых решений. Данная сеть должна быть универсальной транспортной сетью с распределенной коммутацией, вынесением функций предоставления услуг в оконечные сетевые узлы, а также иметь возможность интеграции с использующимися традиционными сетями.

МС ТО – сеть связи, построенная в соответствии с концепцией NGN и обеспечивающая неограниченный набор услуг. Основные требования, предъявляемые к МС ТО:

- независимость технологий предоставления услуг от транспортных технологий;
- гибкое изменение скорости передачи в достаточно широком диапазоне для сервисов;
- передача многокомпонентной информации с синхронизацией всех компонент в реальном времени;
- участие нескольких операторов (сервисов) в формировании информационного контента;
- организация доступа к сервису единой транспортной сети вне зависимости от используемых технологий взаимодействия и расположения сервиса согласно матрице разграничения прав доступа ИИКП ТО [6].

Постановка задачи передачи данных в мультисервисной сети транспортной отрасли. Для постановки задачи представим сеть MPLS как неориентированный граф $G(V,E)$, где множество вершин V соответствует маршрутизаторам, а множество ребер E – сегментам сети. Определим множество $V_1 \subseteq V$, которое содержит вершины, соответствующие пограничным маршрутизаторам.

На рис. 1 представлен неориентированный граф сети МС ТО.

Для дальнейшей постановки задачи введем множество $R \subseteq V_1 \times V_1$, которое содержит пары вершин, соответствующие пограничным маршрутизаторам, между которыми передаются данные. Таким образом, если трафик передается от *LER 2* к *LER 1* и между *LER 2* и *LER 3* в обоих направлениях, то множество *R* будет иметь вид $R = \{(v_1, v_4), (v_1, v_9), (v_9, v_1)\}$.

Введем дополнительные обозначения: $w(x,y)$ – пропускная способность ребра (x,y) графа *G*; $l(s,t) = ((s,x_1),(x_1,x_2),...,(x_{\gamma(s,t)},t))$ – маршрут из вершины *s* в вершину *t* графа *G*, где $\gamma(s,t)$ – длина маршрута $l(s,t)$; $\tilde{A}(s,t)$ – максимально допустимая длина маршрута $l(s,t)$; $L(s,t) = \left\{ l(s,t) \in L \middle| \gamma(s,t) \le \tilde{A}(s,t) \right\}$ – множество маршрутов из *s* в *t*, длина которых не превышает $\tilde{A}(s,t)$; $l_i(s, t)$ – *i*-й маршрут из *s* в *t*, $l_i(s,t) \in L(s,t)$; $f(s, t)$ – поток из *s* в *t*; $f_i(s, t)$ – часть потока $f(s, t)$ по маршруту $l_i(s, t)$; $b(s, t)$ – требование к пропускной способности сети для пары (s, t); $\phi(x,y)$ – суммарный поток по ребру (x,y), где $0 \le \phi(x,y) \le w(x,y)$.

Для формулировки задачи передачи данных в сети МС ТО необходимы следующие исходные данные: неориентированный граф сети $G(V,E)$, множество вершин V_1, множество взаимодействующих вершин R, пропускные способности ребер w графа $G(V,E)$, требования к пропускной способности b и множество маршрутов L между взаимодействующими вершинами. Обозначим через $|L(s,t)|$ мощность множества $L(s,t)$. Следующие отношения должны выполняться согласно постановке задачи:

$$f(s,t)=\sum_{i=1}^{|L(s,t)|} f_i(s,t); \quad \varphi(x,y)=\sum_{(s,t)\in R}\ \sum_{\substack{i=1; \\ (x,y)\in l_i(s,t)}}^{|L(s,t)|} f_i(s,t).$$

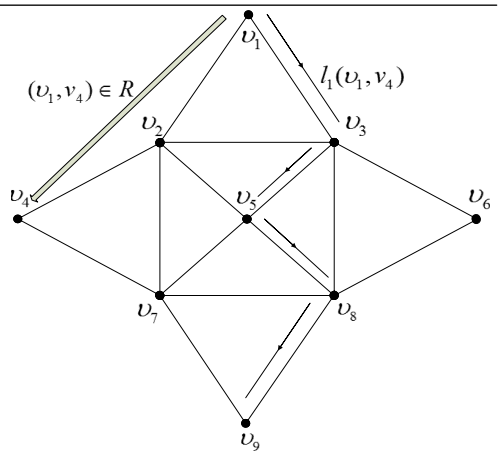

Рис. 1. Неориентированный граф сети МС ТО

Данная модель позволяет определить однокритериальные задачи согласно сформулированным выше принципам построения сетей МС ТО. При введении дополнительных параметров можно расширить модель и покрыть большее число критериев. Так, например, при известной стоимости передачи единицы потока по ребру $c(x,y)$ можно определить стоимость передачи потока по i-му маршруту в виде

$$c(l_i(s,t))=\sum_{(x,y)\in l_i(s,t)} \varphi(x,y)c(x,y),\ (s,t)\in R,\ i=\overline{1,|L(s,t)|}.$$

Задача минимизации стоимости передачи потоков будет заключаться в определении потоков $f_i(s,t)$, которые минимизируют функцию общей стоимости:

$$\sum_{(s,t)\in R}\ \sum_{i=1}^{|L(s,t)|} f_i(s,t)c(l_i(s,t))\to\min,$$

при выполнении ограничений

$$f_i(s,t)\ge 0,\ (s,t)\in R,\ i=\overline{1,|L(s,t)|};\quad \varphi(x,y)\le w(x,y),\ (x,y)\in R;\quad \sum_{i=1}^{|L(s,t)|} f_i(s,t)=b(s,t),\ (s,t)\in R.$$

Дальнейшее развитие модели позволит сформулировать большое число однокритериальных задач, таких как балансировка нагрузки в сети, минимизация числа маршрутов, задержек и пр. Также возможна постановка многокритериальной задачи, например задачи маршрутизации трафика [7].

Помехоустойчивость каналов передачи данных в мультисервисной сети транспортной отрасли. Под помехозащищенностью будем понимать возможность обеспечения надежной безошибочной работы сети передачи данных под действием внешних помех различного типа.

Современные методы обеспечения помехозащищенности условно можно разделить на четыре категории:

1. Изменение физических характеристик канала передачи данных.
2. Использование специальных средств подавления помех.
3. Изменение методов организации приема и/или передачи сигнала.
4. Кодирование передаваемой информации.

К первой категории можно отнести различные методы повышения качественных характеристик каналов передачи данных. Например, замену кабелей вида витая пара на кабели более высоких категорий, в которых используется дополнительное экранирование. Также в некоторых случаях проводные каналы передачи данных прокладывают в дополнительно защищенных кабельных трассах. В беспроводных каналах связи используются более сложные приемопередающие устройства, которые повышают помехозащищенность, например, за счет повышения отношения сигнал/шум.

К специальным средствам подавления помех можно отнести линейные и нелинейные генераторы шума и другие, отдельно используемые устройства.

Среди методов, которые позволяют увеличить помехозащищенность изменением организации приема/передачи сигнала, можно выделить такие, как метод разнесенного приема сигнала, исполь-

зование модуляции на меньшее количество состояний, использование различных методов принятия решения о передаваемом сигнале, использование сигналов с расширением спектра и другие методы.

Все вышеперечисленные методы имеют много субъективных факторов применения, накладывающих определённые ограничения на их использование. Каждый из этих методов применим только в конкретном классе задач, однако четвертая категория обладает отличительной особенностью – общностью применения, так как использование методов кодирования не зависит ни от канала передачи данных, ни от структуры сигнала.

Методы кодирования. История помехоустойчивых кодов или кодов, обнаруживающих и исправляющих ошибки, начинается в 1948 г. вместе со статьей Клода Элвуда Шеннона «Математическая теория связи». Шеннон в своей статье выразил главную мысль о том, что построение слишком хороших каналов является неоправданным, экономически выгоднее использовать кодирование. Именно с этого момента начинается активное изучение и разработка помехоустойчивых кодов.

На сегодняшний день насчитывается большое количество различных алгоритмов кодирования и декодирования информации для передачи по каналам связи. Однако основной идеей остается внесение избыточности. На этапе кодирования в информацию вносятся заранее определенным, специальным образом дополнительные символы или блоки символов, которые в дальнейшем могут быть использованы на этапе декодирования информации для обнаружения или исправления произошедших ошибок под действием внешних факторов и помех.

Алгоритмы можно группировать по различным признакам и категориям. По способу обработки информации коды можно разделить на 2 класса: блоковые и сверточные. Первый класс делит информацию на блоки определенной длины и обрабатывает каждый блок в отдельности, второй класс кодов обрабатывает и передает информацию в виде бесконечного потока.

Следует отметить методы комбинирования кодирования. Такие коды известны под названием каскадные коды. В таком коде информация кодируется сначала одним алгоритмом, а потом применяется другой алгоритм кодирования на уже кодированной информации. Таким образом, получается код-произведение. Для улучшения помехозащищенности каскадных кодов, часто после первого этапа кодирования, применяется операция перемежения, в результате которой символы, находящиеся на соседних позициях, располагаются на различном расстоянии друг от друга. При декодировании производят операцию, обратную перемежению, и символы расставляются по прежним местам в информационном потоке.

Популярной схемой каскадных кодов является алгоритм, который кодирует информацию блоковыми кодами Рида–Соломона, затем информация проходит операцию перемежения и кодируется сверточным кодом. На приемной стороне после декодирования сверточного кода происходит операция, обратная перемежению, при этом большие блоки ошибок рассортировываются и попадают в различные кодовые слова кода Рида–Соломона, тем самым еще более уменьшают вероятность ошибки при декодировании.

Отдельно следует обратить внимание на коды, использующие не только временной ресурс. При внесении избыточности количество полезной передаваемой информации снижается, а следовательно, снижается и скорость передачи данных. На сегодняшний день активно используются коды, использующие также и пространственный ресурс. Такие коды называются пространственно-временными. Суть их состоит в том, что информация передается не от одного источника, а одновременно от нескольких. Тем самым образуется пространственная избыточность. Принятый сигнал обрабатывается определенными алгоритмами и позволяет наиболее точно определить форму переданного сигнала, а следовательно, и произвести наиболее точное декодирование [8].

Идентификация пользователя в мультисервисной сети транспортной отрасли. Для успешной идентификации пользователя в мультисервисной сети транспортной отрасли необходимо выполнить следующую последовательность действий:

1. Произвести условное разбиение всей МС ТО на классы сервисов.
2. Для каждого класса МС ТО определить набор сервисов, входящих в него.

Будем различать два вида идентификации: полную и частичную.

Под полной идентификацией пользователя во всей МС ТО будем понимать совокупность успешных идентификаций пользователя во всех сервисах всех классов, в нее входящих. Под частичной идентификацией – совокупность успешных идентификаций пользователя во всех тех сервисах, в которых необходимо организовать доступ в рамках текущей сессии.

Также будем считать, что уровень корректности, полноты и качества идентификации с точки зрения уровня информационной защищенности активов МС ТО тем выше, чем больше атрибутов пользователя участвует в идентификации и чем сложнее степень их определения.

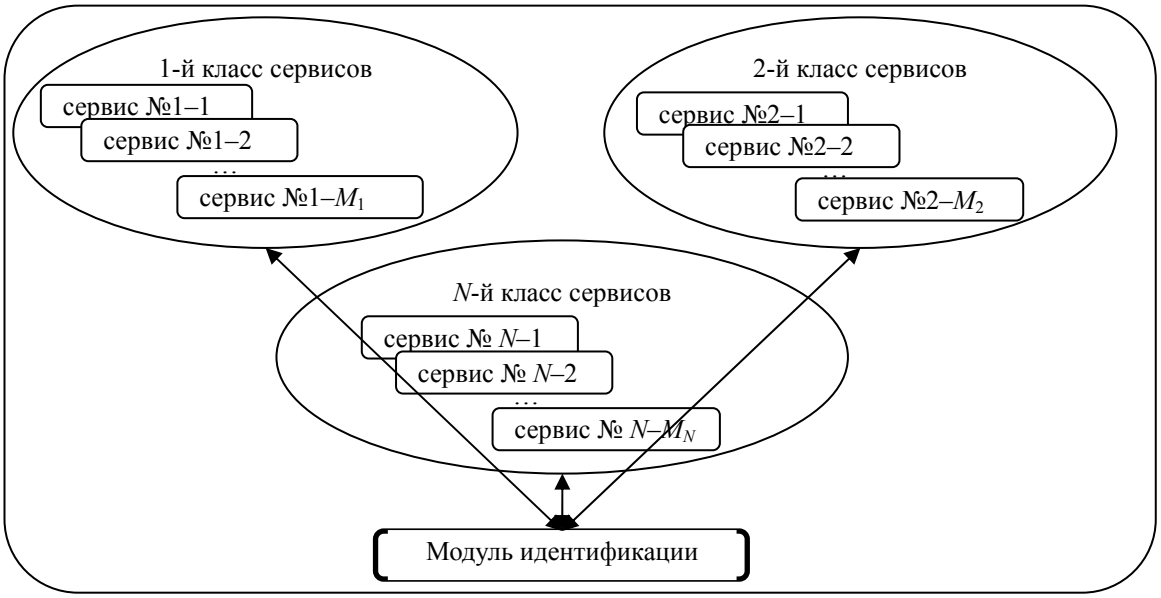

Рис. 2. Типовая схема взаимодействия модуля идентификации
как составного элемента МС ТО с классами сервисов

3. Провести процесс идентификации пользователя в МС ТО как поклассовую последовательность шагов по идентификации пользователя в каждом сервисе конкретного класса (для полной идентификации – все сервисы, для частичной – те, которые участвуют в идентификации).

За все процессы идентификации пользователя в МС ТО отвечает отдельный программно-аппаратный модуль, который обеспечивает эффективный синтез программных и аппаратных способов идентификации (рис. 2).

Для построения модели идентификации пользователя в МС ТО введем следующие обозначения: K_i – i-й класс сервисов; S_{ij} – j-й сервис в i-м классе; $a_{k_{ij}}$ – k-й идентификационный атрибут пользователя, определяемый в j-м сервисе i-го класса; $A_{ij} = \left\{a_{1_{ij}}, a_{2_{ij}}, ..., a_{k_{ij}}\right\}$ – множество идентификационных атрибутов пользователя, определяемое в j-м сервисе i-го класса.

Для каждого атрибута $a \in A$ определен домен V_a (для доменов допускается дискретность значений).

Множество 2^{V_a} – супердомен атрибута a $V = \bigcup\limits_{a \in A} V_a$. Таким образом, модель идентификации пользователя можно представить парой (A,V).

Для $\forall S \subseteq A$ определим следующие величины:

$$V_S = \bigcup_{s \in S} V_s, \quad \bar{2}^{V_S} = \bigcup_{s \in S} 2^{V_a}.$$

Под кортежем типа T будем понимать функцию следующего вида:

$$r : T \to \bar{2}^{V_T}$$

и $r(a) \subseteq V_a$ для всех $a \in T$, далее вместо $r(a)$ используем запись r_a, а для кортежа типа T – запись r_T, множество всех кортежей типа T обозначим как $U(T)$.

Под элементарным кортежем типа T будем понимать функцию

$$r : T \to V_T,$$

такую, что $r(a) \in V_a$ для любых $a \in T$, в случае если $V_a = \varnothing$, тогда $r(a) = null$ (это возможно в случает отсутствия оперативной необходимости идентификации пользователя в конкретном классе сервисов), множество кортежей типа T определим как $eU(T)$.

Для построения системы идентификации пользователей в МС ТО необходимо произвести классификацию сервисов (как было сказано ранее), категорирование пользователей и построение матри-

цы прав доступа, в которой по вертикали будут указаны категории пользователей, по горизонтали классы сервисов, а на пересечении – уровень доступа, определяемый для данной категории в рамках данного класса.

Пусть P – множество категорий пользователей. $D \subseteq A$ – набор атрибутов для категорирования. K_D – категорирование множества пользователей на основе атрибутов D. Категорию определим как элементарный кортеж:

$$r : D \to \bigcup_{a \in D} V_a ,$$

где $r(a) \in V_a$ для каждого $a \in D$. Множество всех элементарных кортежей типа D обозначим как $U(D)$. Таким образом, число категорий будет равно числу всех кортежей типа D; $K_D(r)$ – категория, определенная кортежем r.

Пользователь $p \in P$ принадлежит категории $K_D(r)$, если для каждого атрибута $a \in D$ значение идентификатора равно $r(a)$. Отсюда получаем следующее:

$$\bigcup_{r \in eU(D)} K_D(r) = L , \quad K_D \cap K_D(r') = \varnothing, \forall r, r' \in eU(D), r \neq r'.$$

Таким образом,

$$K_D = \{K_D(r) \mid r \in eU(D)\}$$

можно рассматривать как разбиение множества D. В результате некоторые категории могут оказаться пустыми (неактуальными в данный момент идентификации, например, при частичной идентификации) и их необходимо удалить из K_D.

Отметим также, что значения атрибутов модели идентификации пользователя могут изменяться в процессе функционирования МС ТО. Это определяется возможной миграцией и изменением состава сервисов, а также типом идентификации. При возникновении таких ситуаций необходимо произвести переклассификацию.

Также могут быть случаи идентификации по ряду альтернативных признаков.

Альтернативным признаком, например, может быть идентификация по отпечатку пальца или по сетчатке глаза и т.п.

Пусть a_i и a_{i^a} – попарно альтернативные признаки, а $\widetilde{a_j}$ – признаки, не имеющие альтернативных аналогов, тогда верная идентификация $True(I)$ возможна в случае истинности выражения:

$$True(I) \equiv \left(\widetilde{a_1} \,\&\, \widetilde{a_2} \,\&\, ... \,\&\, \widetilde{a_n}\right) \& \left(\left(a_1 \vee a_{1^a}\right) \& \left(\left(a_2 \vee a_{2^a}\right)\right) \& ... \& \left(a_m \vee a_{m^a}\right)\right),$$

где n – количество признаков, не имеющих альтернативных аналогов; m – количество признаков, имеющих альтернативные аналоги.

Заключение. Пространство информационного обмена, основой которого стала МС ТО, требует серьезно продуманной системы мер и правил по обеспечению должного уровня безопасности функционирования. В рамках одной статьи всего перечня мер не охватить. Предпосылками на будущее являются также существующие нормы законодательства РФ, которые дают четкие рекомендации по уровням защищенности и принципам категорирования информации. Именно хорошо продуманная система обеспечения информационной безопасности позволит, в том числе, стандартизировать многие процессы, что станет основой успешного развития всей отрасли как единого организма внутренних и международных отношений.

Литература

1. Нырков А.П. О проблемах защищенности беспроводных сетей передачи данных на внутренних водных путях / А.П. Нырков, А.В. Башмаков // Методы и технические средства обеспечения безопасности информации: матер. XIX науч.-техн. конф. – СПб.: Изд-во политехн. ун-та, 2010. – С. 43–44.

2. Каторин Ю.Ф. Защищенность информации в каналах передачи данных в береговых сетях автоматизированной идентификационной системы / Ю.Ф. Каторин, В.В. Коротков, А.П. Нырков // Журнал университета водных коммуникаций. – 2012. – № 1. – С. 98–102.

3. Нырков А.П. Методика проектирования безопасных информационных систем на транспорте / А.П. Нырков, С.С. Соколов, А.В. Башмаков // Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 3. – С. 58–61.

4. Нырков А.П. Безопасность информационных потоков в АСУДС / А.П. Нырков, П.В. Викулин // Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 4. – С. 78–82.

5. Соколов С.С. О создании единого интегрированного информационно-коммуникационного пространства транспортной отрасли // Региональная информатика РИ–2012: матер. Юбилейной XIII Санкт-Петербургской междунар. конф. 24–26 октября 2012 г. – СПб.: 2012. – С. 247–250.

6. Нырков А.П. Методы обеспечения доступа в ведомственных сетях на базе мультисервисных платформ / А.П. Нырков, А.А. Некрасов // Высокие технологии, фундаментальные исследования, образование: сб. тр. Восьмой Междунар. науч.-практ. конф. «Исследование, разработка и применение высоких технологий в промышленности». – СПб, 2009. – С. 68–71.

7. Нырков А.П. Мультисервисная сеть транспортной отрасли / А.П. Нырков, С.С. Соколов, А.С. Белоусов // Вестник компьютерных и информационных технологий. – 2014. – № 4. – С. 33–39.

8. Нырков А.П. Помехозащищенность как фактор обеспечения стабильной работы сети передачи данных на транспорте / А.П. Нырков, С.С. Соколов, А.С. Белоусов // Сборник научных трудов SWorld. – 2013. – Т. 8, № 1. – С. 5–9.

Нырков Анатолий Павлович
Д-р техн. наук, профессор, зав. каф. комплексного обеспечения информационной безопасности Государственного университета морского и речного флота (ГУМРФ) им. адм. С.О. Макарова
Тел.: 8 (812) 748-96-41
Эл. почта: NyrkowAP@gumrf.ru

Соколов Сергей Сергеевич
Канд. техн. наук, доцент, начальник управления информатизации ГУМРФ
Тел.: 8 (812) 748-97-20
Эл. почта: SokolovSS@gumrf.ru

Белоусов Андрей Сергеевич
Аспирант факультета информационных технологий ГУМРФ
Тел.: 8 (812) 748-97-20
Эл. почта: BelousovAS@gumrf.ru

Ковальногова Надежда Михайловна
Аспирант факультета информационных технологий ГУМРФ
Тел.: 8 (812) 748-97-50
Эл. почта: KovalnogovaNM@gumrf.ru

Мальцев Валерий Александрович
Аспирант факультета информационных технологий ГУМРФ
Тел.: 8 (812) 748-97-50
Эл. почта: MalcevVA@gumrf.ru

Nyrkov A.P., Sokolov S.S., Belousov A.S. , Kovalnogova N.M., Maltsev V.A.

Ensuring safe operation of multiservice network in transport industry

The article describes the prerequisites for the development of integrated information and communication space transportation industry, formulation of the problem of data transmission in multi-service transport industry and methods to ensure immunity of data transmission channels, a model of user identification in a multiservice network.

Key words: multiservice network, model proxy authentication user, coding techniques, channels immunity, immunity data, integrated information and communication space of transportation industry.