УДК 004.056.53

Н. В. Евглевская, Г. А. Бекбаев, А. А. Привалов, Д. Н. Шахматов

МОДУЛЬ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ЕДИНОГО ДОРОЖНОГО ДИСПЕТЧЕРСКОГО ЦЕНТРА УПРАВЛЕНИЯ ПЕРЕВОЗКАМИ ОАО «РЖД» НА ОСНОВЕ РАЦИОНАЛЬНОГО ВЫБОРА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕРОПРИЯТИЙ

Дата поступления: 25.04.2016
Решение о публикации: 25.04.2016

Цель: Создать модуль поддержки принятия решений по управлению информационной безопасностью (ИБ) телекоммуникационной сети (ТКС) единого дорожного диспетчерского центра управления перевозками (ЕДЦУ) ОАО «РЖД», позволяющего проводить комплексный анализ ИБ объектовой ТКС и выявлять критические уязвимости в системе защиты, а также поддерживать выработку мер по их устранению. **Методы:** Для совместной согласованной оценки возможностей нарушителя и системы управления информационной безопасностью (СУИБ) разработана комплексная модель функционирования ТКС ЕДЦУ ОАО «РЖД» в условиях реализации нарушителем информационных воздействий. При моделировании применялись метод топологического преобразования стохастических сетей, метод марковских цепей с дискретными состояниями и с непрерывным временем. Для оценки ИБ ТКС ЕДЦУ разработана методика оценки ИБ ТКС ЕДЦУ ОАО «РЖД», функционирующей в условиях реализации нарушителем информационных воздействий. На основе градиентного метода Гаусса – Зейделя создана методика выбора рациональных мероприятий по защите ТКС ЕДЦУ ОАО «РЖД». **Результаты:** Разработан модуль специального математического и программного обеспечения подсистемы поддержки принятия решений СУИБ ТКС ЕДЦУ ОАО «РЖД» на основе комплексной модели функционирования ТКС ЕДЦУ ОАО «РЖД» в условиях реализации нарушителем информационных воздействий, методики оценки ИБ ТКС, методики выбора рациональных мероприятий по защите ТКС ЕДЦУ ОАО «РЖД». Получены результаты оценки ИБ ТКС ЕДЦУ ОАО «РЖД». **Практическая значимость:** Использование модуля специального математического и программного обеспечения подсистемы поддержки принятия решений СУИБ ТКС ЕДЦУ позволяет оперативно принимать решение по нейтрализации (предотвращению) информационных воздействий.

Нарушитель, информационное воздействие, телекоммуникационная сеть, угроза, информационная безопасность.

***Natalya V. Evglevskaya**, electrician, n.evglevskaya@gmail.com (Central Regional Communication Centre), **Gamzatdin A. Bekbaev**, post graduate student, gamzat-86@mail.ru, **Andrey A. Privalov**, D. Military Sci., professor, aprivalov@inbox.ru (Petersburg State Transport University), **Dmitriy N. Shakhmatov**, senior researcher, d.shakhmatov@mail.ru (S. M. Budyonny Military Telecommunications Academy) DECISION-MAKING SUPPORT MODULE FOR TELECOMMUNICATION NETWORK INFORMATION SECURITY MANAGEMENT OF THE JOINT ROAD DISPATCHING TRANSPORTATIONS MANAGEMENT CENTRE OF RUSSIAN RAILWAYS JSC BASED ON RATIONAL CHOICE OF ORGANISATIONAL AND TECHNICAL ACTIONS

Objective: To create decision-making support module for telecommunication network (TCN) information security (IS) management of joint road dispatching transportations management centre (JRDTMC) of

Russian Railways JSC that allows to carry out object-specific TCN IS complex analysis, to identify critical vulnerabilities of security system, and to support measures for eliminating them. **Methods:** For a concerted joint evaluation of attacker and information security management system (ISMS) possibilities, a complex model of Russian Railways JSC JRDTMC TCN functioning in conditions when attacker realizes information impacts (II) was created. For the simulation, a method of topological transformation of stochastic networks (TTSN) and the method of Markov chains with discrete states and continuous time were used. For JRDTMC TCN IS evaluation, a method of evaluation of Russian Railways JSC JRDTMC TCN IS functioning under conditions when an attacker realizes II was developed. Using Gauss-Seidel gradient, a method of rational actions choice for protection of Russian Railways JSC JRDTMC TCN is created. **Results:** Special mathematical and software module (SMS) of decision-making support subsystem (DMSS) of Russian Railways JSC JRDTMC TCN ISMS was created using the complex model of Russian Railways JSC JRDTMC TCN functioning in conditions when attacker realizes II, TCN IS valuation methods, rational actions choice methods for protection of Russian Railways JSC JRDTMC TCN. The Russian Railways JSC JRDTMC TCN IS valuation results were obtained. **Practical importance:** Using JRDTMC TCN ISMS DMSS SMS module allows to make decision on efficiency of II neutralization or prevention.

Attacker, information impact, telecommunication network, threat, information security.

По данным Департамента безопасности ОАО «РЖД», около 50% усилий направлено на внедрение средств обеспечения безопасности в имеющихся телекоммуникационных сетях (ТКС), 10% – на продление лицензий на антивирусное программное обеспечение, около 35% – на разработку и внедрение средств обеспечения безопасности для автоматизированных систем управления (АСУ), вновь создаваемых в ОАО «РЖД» [2].

Внедрение в АСУ продуктов современных инфокоммуникационных технологий влечет появление новых видов угроз безопасности информации, реализуя которые, нарушитель деструктивно воздействует на произвольные элементы ТКС. В таких условиях традиционные принципы построения системы обеспечения информационной безопасности (ИБ) ТКС недостаточно эффективны [14, 15]. Это обусловлено тем, что в большинстве случаев анализу подлежат частные угрозы ИБ и реализуются типовые методы их предотвращения без учета структуры, роли, места, особенностей функционирования ТКС, участвующей в технологическом процессе [14, 15].

Особенностью предлагаемого подхода к созданию модуля специального математического и программного обеспечения (СМПО) подсистемы поддержки принятия решений (ППРР) системы управления информационной безопасностью (СУИБ) ТКС единого дорожного диспетчерского центра управления перевозками (ЕДЦУ) ОАО «РЖД» является его системность, позволившая представить ТКС ЕДЦУ в виде совокупности взаимосвязанных функциональных узлов и возможных каналов, используя которые, нарушитель может деструктивно воздействовать на сеть. В структуру модуля СМПО включена ППРР, предоставляющая администратору по ИБ ЕДЦУ перечень рациональных мероприятий, реализация которых обеспечит нейтрализацию актуальных угроз ИБ [14, 15].

Общая структура модуля СМПО ППРР СУИБ ТКС ЕДЦУ ОАО «РЖД»

Структура модуля СМПО представлена на рис. 1. Основным элементом модуля является субмодуль математического моделирования компьютерных атак и процесса добывания нарушителем данных по техническим каналам утечки информации (ТКУИ) в ЕДЦУ ОАО «РЖД» (субмодуль 4). В основе данного субмодуля лежит модель конфликта СУИБ и си-

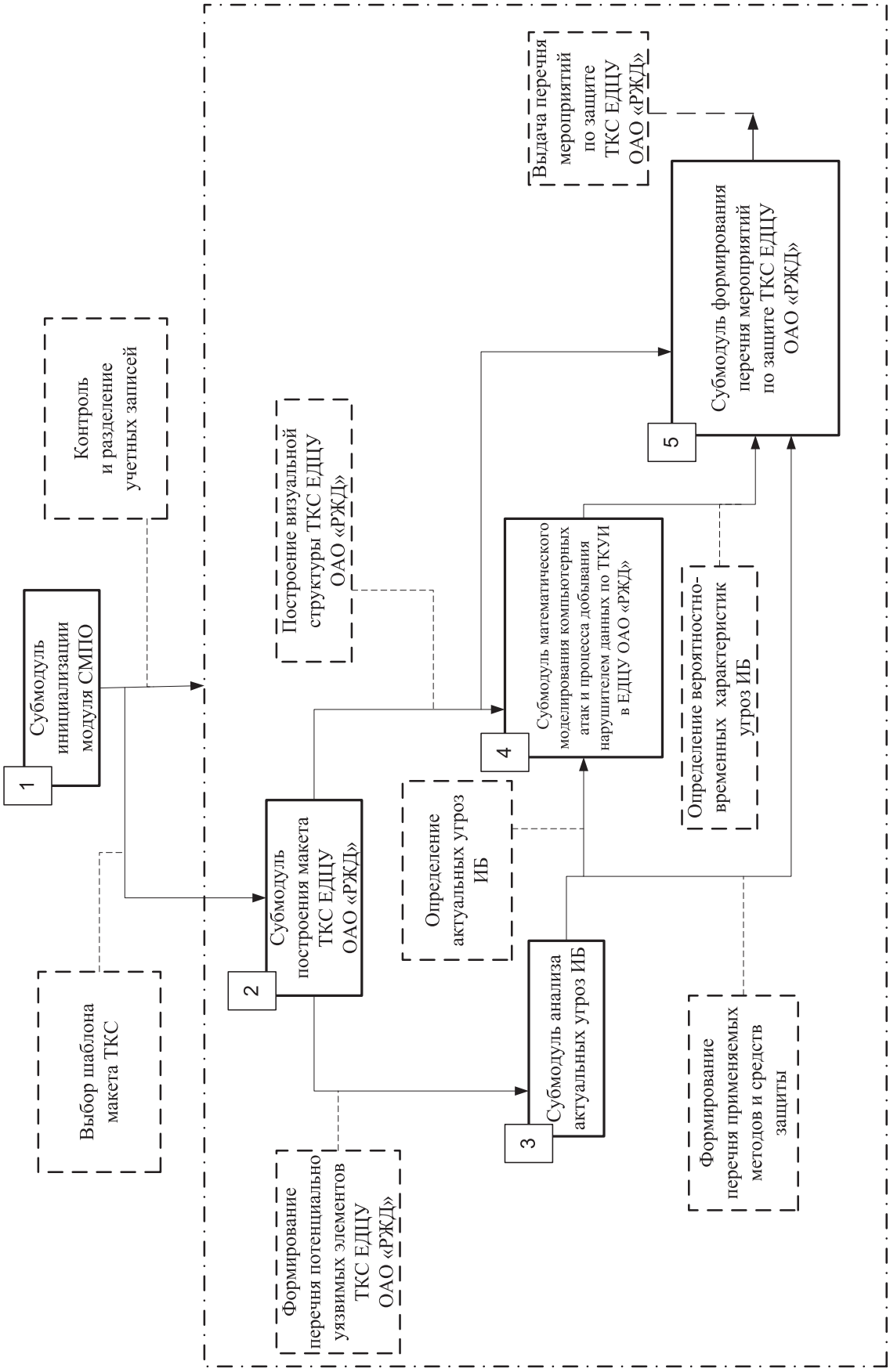

Рис. 1. Структура модуля СМПО ППРР СУИБ ТКС ЕДЦУ ОАО «РЖД»

стемы нарушителя (СН). Исходными данными для указанной модели являются результаты моделирования процессов реализации информационных воздействий (ИВ) нарушителя на ТКС ЕДЦУ и функционирования ТКС ЕДЦУ в условиях реализации ИВ. В свою очередь, исходными данными для моделирования процесса реализации ИВ нарушителя на ТКС ЕДЦУ являются результаты моделирования процессов вскрытия нарушителем ТКУИ в ЕДЦУ; установки закладочных устройств (ЗУ) в ТКУИ; внедрения вредоносных программ в элементы ТКС ЕДЦУ; вскрытия ТКС ЕДЦУ техническими средствами компьютерной разведки нарушителя. Модель процесса вскрытия ТКУИ в ЕДЦУ разработана с использованием результатов моделирования ТКУИ, выявленных в ЕДЦУ. Исходными данными для моделирования процесса вскрытия ТКС ЕДЦУ техническими средствами компьютерной разведки нарушителя послужили результаты моделирования процессов идентификации узлов, сервисов, операционной системы ТКС ЕДЦУ, определения технической роли узлов сети. Для моделирования данных процессов, а также процесса функционирования ТКС в условиях реализации ИВ используются данные, характеризующие ТКС ЕДЦУ, а также нормативные модели и методики оценки ИБ.

Указанный субмодуль обеспечивает расчет вероятностно-временных характеристик процессов реализации нарушителем актуальных угроз и формирует перечень наиболее вероятных. Кроме того, субмодуль взаимодействует с единой системой мониторинга и администрирования ТКС, тем самым обеспечивая накопление статистических данных об инцидентах безопасности [8, 14, 15].

Актуальные угрозы определяются в субмодуле анализа актуальных угроз ИБ (субмодуль 3), который по результатам опроса пользователя (администратора ИБ ТКС ЕДЦУ) с учетом применяемых методов защиты информации определяет элементы ТКС, наиболее подверженные риску воздействия, и актуальные угрозы со стороны нарушителя. Чтобы облегчить процесс определения основных функциональных элементов и сделать структуру ТКС ЕДЦУ более наглядной, разработан субмодуль построения макета ТКС ЕДЦУ ОАО «РЖД» (субмодуль 2). На заключительном этапе в субмодуле формирования перечня мероприятий по защите ТКС ЕДЦУ ОАО «РЖД» (субмодуль 5) формируются рекомендации администратору ИБ по устранению уязвимостей системы защиты и предотвращению угроз ИБ ТКС ЕДЦУ ОАО «РЖД». Субмодуль инициализации модуля СМПО (субмодуль 1) разделяет учетные записи на две категории: администратор и пользователь. Учетная запись «Администратор» обеспечивает управление учетными записями и устанавливается для администратора ИБ. Учетная запись «Пользователь» устанавливается для операторов рабочих станций и блокирует возможность присвоения прав администратора недобросовестным пользователям [1, 6–8, 15].

Модели, входящие в состав субмодуля 4, позволяют получить вероятностно-временные характеристики процессов реализации нарушителем ИВ в отношении элементов сети ЕДЦУ ОАО «РЖД» [4, 5, 12, 13].

Методика выбора рациональных мероприятий по защите ТКС ЕДЦУ ОАО «РЖД»

Чтобы обоснованно выбрать рациональные мероприятия по защите ТКС ЕДЦУ, разработана методика, позволяющая определять степени зависимости показателей оценки ИБ ТКС ЕДЦУ ОАО «РЖД», соответствующие требованиям нормативных документов, т. е. $\overline{T}_{\text{безоп}} \geq T_{\text{треб}} = 24$ ч, $P_{\text{безоп}}(t) \geq P_{\text{треб}} = 0{,}95$ [3], от значений и диапазонов возможного изменения частных параметров, используемых в качестве исходных данных. Изменению каждого частного параметра соответствует определенная совокупность организационно-технических мероприятий (ОТМ). Таким образом, определяя диапазон изменения частных параметров, можно выбрать такую совокупность ОТМ, реализация которой позволит

ТКС ЕДЦУ соответствовать уровню защищенности от ИВ согласно [3].

В качестве показателя степени зависимости обобщенного показателя защищенности ТКС ЕДЦУ от ИВ, реализуемых нарушителем, выбрано приращение $\Delta P_{\text{безоп}}(T_{\text{треб}})$ значений вероятности пребывания ТКС ЕДЦУ в состоянии безопасности за время $T_{\text{треб}}$. При этом критерием выбора приращений является

$$\max_i \{\Delta P_{\text{безоп}}(T_{\text{треб}}, x_i), i = \overline{1, N}\},$$

где x_i – частные показатели, используемые при моделировании в качестве исходных данных [3, 4, 8, 11, 12].

Помимо используемых при моделировании частных показателей x_i исходными данными являются диапазоны их возможного изменения Δx_i, определяемые как разность их конечного $x_{i\text{к}}$ и начального $x_{i\text{н}}$ значений, т. е. $\Delta x_i = x_{i\text{к}} - x_{i\text{н}}$.

Постановка задачи

Дана монотонная функция $P_{\text{безоп.}}(t)$, характеризующая распределение времени пребывания ТКС ЕДЦУ в состоянии безопасности. В общем случае на указанное время и, следовательно, на характер изменения $\Delta P_{\text{безоп.}}(t)$ влияет множество параметров $x_i, i = \overline{1, N}$, каждый из которых может изменяться в пределах между конечным $x_{i\text{к}}$ и начальным $x_{i\text{н}}$ значениями $\Delta x_i = x_{i\text{к}} - x_{i\text{н}}$.

Требуется определить максимальные степени зависимости значений вероятности пребывания ТКС ЕДЦУ в состоянии безопасности от значений и диапазонов изменения частных параметров с учетом вложенности моделей [4, 5, 12, 13].

$$N_i = \max f(\Delta P_{\text{безоп}}(t)_{xi}).$$

Решение

Поскольку для определения максимальных степеней N_i не требуется высокой точности расчета значений приращений целевой функции в зависимости от изменения ее аргументов, а необходим лишь знак этого приращения и номер соответствующего ему аргумента, для уменьшения объема и времени вычислений для решения задачи целесообразно воспользоваться градиентным методом Гаусса – Зейделя с учетом свойства вложенности моделей [10, 11].

Чтобы определить значения $\Delta P_{\text{безоп}}(t)_{xi}$, вычисляют частные производные функции $P_{\text{безоп}}(t, x_i)$ по каждому параметру x_i, изменяющемуся в некоторых пределах Δx_i. Это возможно, так как по условию $P_{\text{безоп}}(t, x_i)$ является аналитической функцией в области определения каждой переменной x_i, $i = \overline{1, N}$. Применяя теорему Лагранжа [10, 11], получим

$$\Delta P_{i\text{безоп}}(t, x_i, i = \overline{1, N}) = \frac{dP_{\text{безоп}}(t, x_i, i = \overline{1, N})}{dx_i} \Delta x_i. \quad (1)$$

Алгоритм выбора рациональных мероприятий по защите ТКС ЕДЦУ ОАО «РЖД» представлен на рис. 2.

На первом этапе вводят исходные данные [4, 5, 12].

На втором этапе рассчитывают функции распределения $C(t)$ времени реализации ИВ на ТКС ЕДЦУ, $G(t)$ времени вскрытия ТКС ЕДЦУ техническими средствами компьютерной разведки, $F(t)$ времени вскрытия ТКУИ и внедрения ЗУ, вероятности $P_{\text{безоп}}(t)$ пребывания ТКС ЕДЦУ в состоянии безопасности.

На третьем этапе сравнивают вычисленную на втором этапе $P_{\text{безоп}}(t)$ с требуемым значением [3]. Если критериальное условие выполняется, то подтверждается рациональность реализации запланированных мероприятий по защите ТКС ЕДЦУ.

В противном случае рассчитывают приращения $\Delta P_{\text{безоп}}(T_{\text{треб}})$ вероятности пребывания ТКС ЕДЦУ в состоянии безопасности за время $T_{\text{треб}}$.

Далее по формуле (1) рассчитывают $\{\Delta P_{\text{безоп}}\}_y$. При этом j-му элементу вектора $\{\Delta P_{\text{безоп}}\}_y$ соответствует i-й параметр моде-

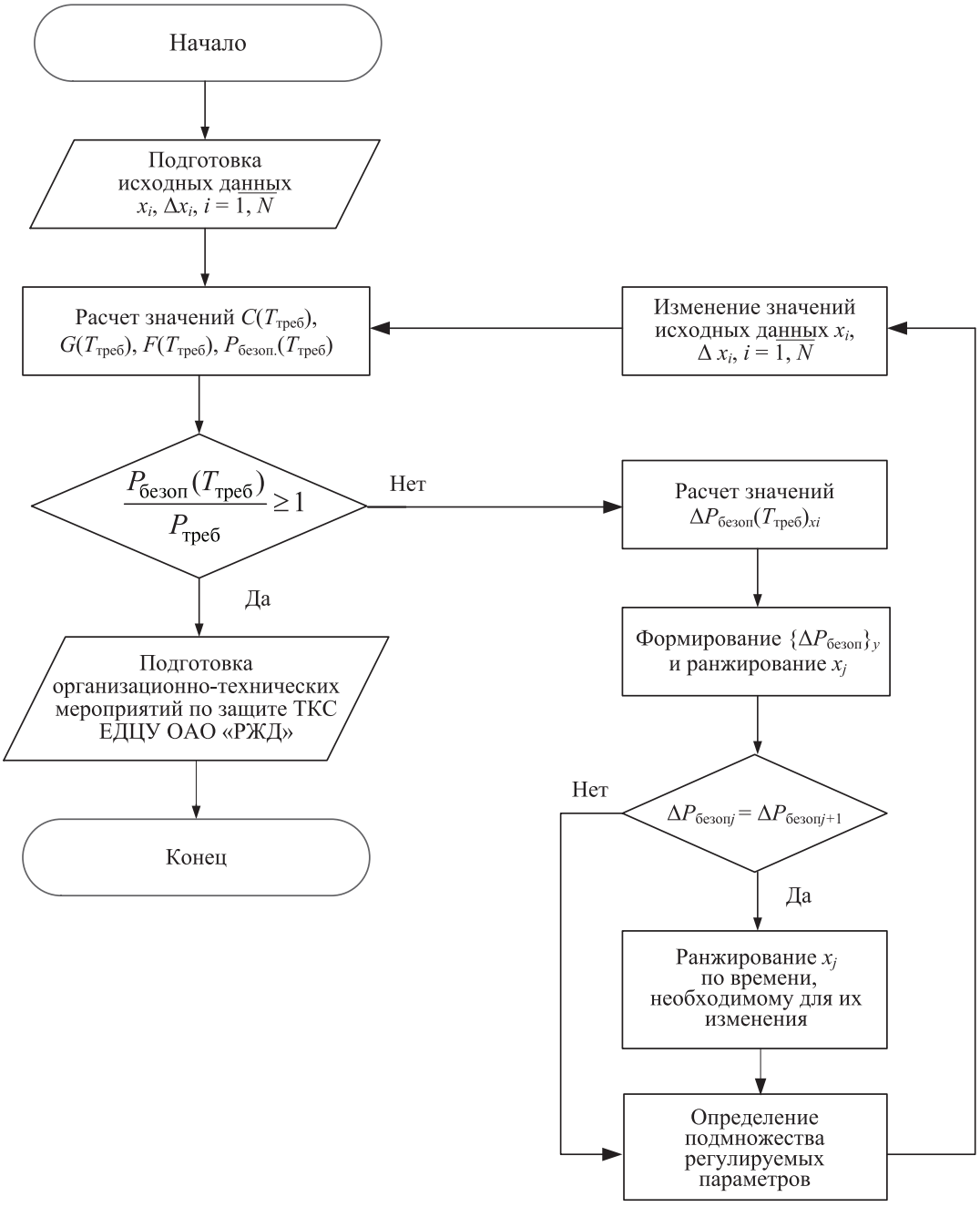

Рис. 2. Алгоритм выбора рациональных мероприятий по защите ТКС ЕДЦУ ОАО «РЖД»

ли процесса функционирования ТКС ЕДЦУ ОАО «РЖД» в условиях реализации нарушителем ИВ [5].

Если значение $P_{безопj}$ соответствует требуемому, производится ранжирование x_j; если значение $P_{безопj}$ ниже требуемого, необходимо определить регулируемые параметры и после изменения значений исходных данных повторно рассчитать $C(T_{треб})$, $G(T_{треб})$, $F(T_{треб})$, $P_{безоп}(T_{треб})$.

Пример расчета по методике

Исходные данные, используемые для расчета, характеризуют структуру и конфигура-

цию ТКС ЕДЦУ ОАО «РЖД», состояние среды общего доступа, принципы, возможности, алгоритмы нарушителя [3–5, 12].

Так как математические модели, входящие в субмодуль 4, обладают свойством вложенности, поиск приращений $\Delta P_{\text{безоп}}(T_{\text{треб}})$ производится послойно.

Формула (1) используется на каждом слое модели конфликта СУИБ и СН с тем различием, что на уровне выхода модели используется максимальное значение обобщенного показателя вероятности пребывания ТКС ЕДЦУ ОАО «РЖД» в состоянии безопасности, а на уровне частных показателей – минимальные значения, так как они характеризуют возможности нарушителя, реализующего ИВ на ТКС ЕДЦУ.

Результатом расчетов по формуле (1) является семейство функций приращений обобщенного и частных показателей вероятности пребывания ТКС ЕДЦУ ОАО «РЖД» в состоянии безопасности $\Delta P_{i\text{безоп}}(t, x_i, i = \overline{1, N})$ (рис. 3–6).

Чтобы обеспечить требуемый уровень защищенности сети, необходимо не только сократить время восстановления ТКС, но и выполнить ОТМ, затрудняющие нарушителю реализацию ИВ на ТКС ЕДЦУ.

Наиболее значимыми параметрами процесса реализации ИВ на ТКС ЕДЦУ являются время вскрытия ТКУИ в ЕДЦУ $t_{\text{вскрТКУИ}}$ и время вскрытия ТКС ЕДЦУ техническими средствами компьютерной разведки $t_{\text{вскрТКС}}$ (рис. 3), длительность которых можно увеличить путем выполнения таких ОТМ, как:

• экранирование кабелей и проводов;

• исключение из состава ТКС ЕДЦУ незадействованной аппаратуры и неиспользуемых проводов;

• расположение элементов ТКС ЕДЦУ на максимально возможном удалении от границы контролируемой зоны (КЗ);

• ограничение доступа персонала только к той аппаратуре и документам, которые ему необходимы для выполнения должностных обязанностей;

• применение систем маскировки ТКС ЕДЦУ и ее параметров.

Наиболее значимыми параметрами процесса вскрытия ТКС ЕДЦУ техническими средствами компьютерной разведки нарушителя являются время идентификации сетевых узлов t_d и время сканирования портов и идентификации сетевых сервисов t_n (рис. 4), длительность которых можно увеличить путем выполнения таких ОТМ, как:

• использование утилиты IPtables;

• применение механизма «port knocking»;

• эмуляция виртуальных сетевых узлов, портов, сервисов.

В свою очередь, наиболее значимыми параметрами процесса вскрытия нарушителем ТКУИ в ЕДЦУ являются время вскрытия нарушителем акустического ТКУИ $t_{\text{ак}}$, время внедрения ЗУ в ТКУИ $t_{\text{зу}}$ (рис. 5). Затруднить нарушителю выполнение данных действий помогут такие ОТМ, как:

• применение средств звукоглушения и звукоизоляции;

• применение метода противофазного подавления акустического сигнала;

• выявление технических средств, применение которых служебной необходимостью не обосновано;

• выявление незадействованных наземных, подземных воздушных, заложенных в скрытую канализацию кабелей, выходящих за пределы КЗ.

Анализ полученных результатов

Из графиков, представленных на рис. 6, можно сделать вывод, что основным направлением достижения пребывания ТКС ЕДЦУ в состоянии безопасности согласно требованиям нормативных документов, является сокращение времени восстановления состояния безопасности ТКС ЕДЦУ после успешной реализации нарушителем ИВ.

На рис. 7 представлены вероятностно-временные характеристики пребывания ТКС ЕДЦУ в состоянии безопасности при существующем порядке функционирования ТКС ЕДЦУ и в случае применения модуля СМПО

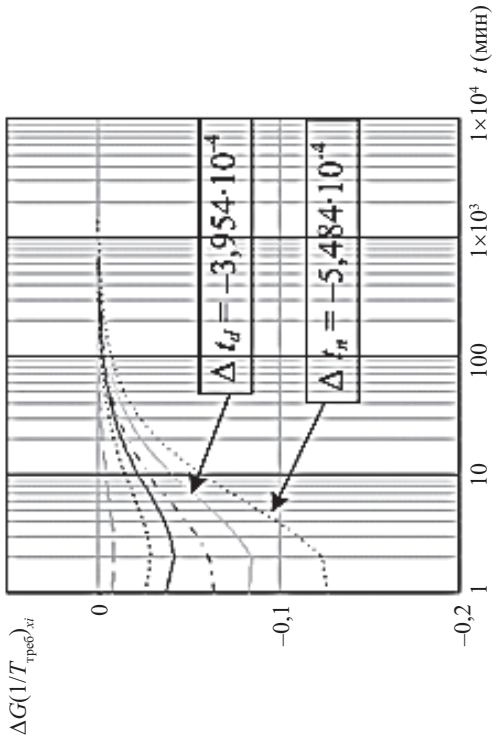

Рис. 4. Графики зависимостей $\Delta G(1/T_{треб})_{xi}$

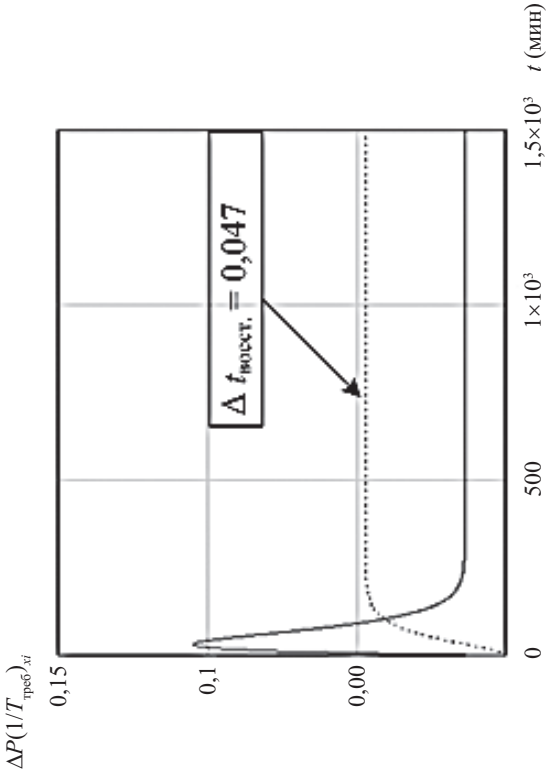

Рис. 6. Графики зависимостей $\Delta P(1/T_{треб})_{xi}$

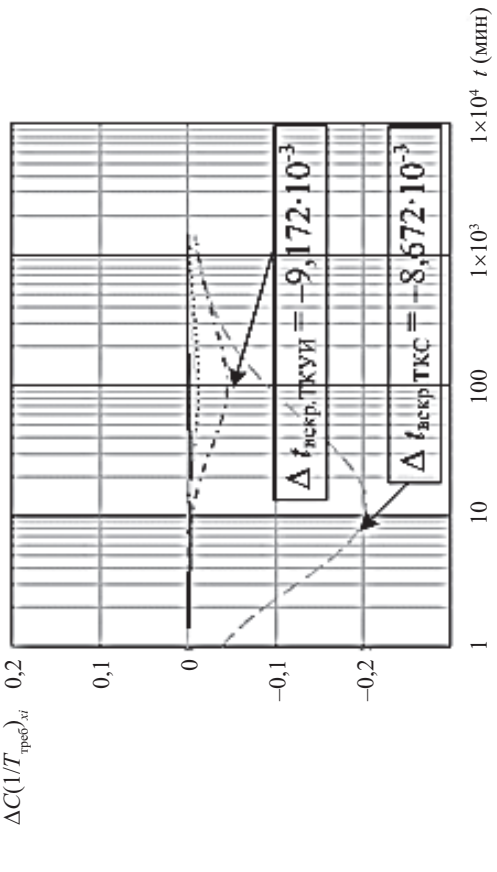

Рис. 3. Графики зависимостей $\Delta C(1/T_{треб})_{xi}$

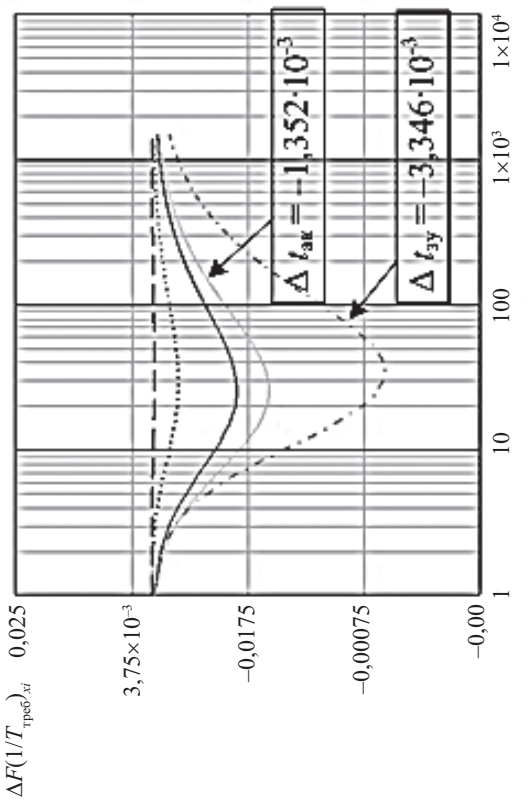

Рис. 5. Графики зависимостей $\Delta F(1/T_{треб})_{xi}$

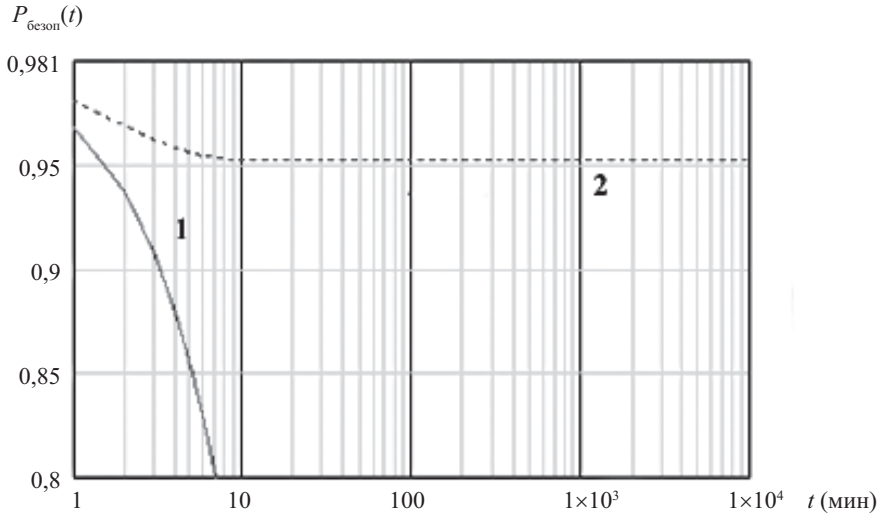

Рис. 7. Вероятностно-временные характеристики пребывания ТКС ЕДЦУ ОАО «РЖД» в состоянии безопасности

ППРР СУИБ ТКС ЕДЦУ ОАО «РЖД», обеспечивающего сокращение времени восстановления состояния безопасности сети. Представленные на графиках зависимости $P_{безоп}(t)$ позволяют оценить влияние времени восстановления состояния безопасности сети $t_{восст}$ и времени реализации ИВ $t_{ИВ}$ нарушителем на продолжительность пребывания ТКС в состоянии безопасности. До применения модуля СМПО и выполнения ОТМ, затрудняющих нарушителю реализацию ИВ, время восстановления состояния безопасности сети составляло $t_{восст} = 600$ мин, длительность реализации нарушителем ИВ – $t_{ИВ} = 31$ мин, при этом продолжительность пребывания сети в состоянии безопасности при $P_{треб} = 0{,}95$ составило 1,6 мин (кривая 1). После применения модуля СМПО и выполнения ОТМ время восстановления состояния безопасности сети составило $t_{восст} = 2$ мин, $t_{ИВ} = 40$ мин, при этом вероятность пребывания ТКС в состоянии безопасности – не ниже 0,96, что соответствует требованиям нормативных документов.

Заключение

Разработанный модуль СМПО ППРР СУИБ ТКС ЕДЦУ ОАО «РЖД», позволяет администратору ИБ оперативно принимать решение по управлению сетью, функционирующей в условиях реализации нарушителем ИВ.

Библиографический список

1. Болтенкова Е. О. Модуль построения макета телекоммуникационного объекта ОАО «РЖД» / Е. О. Болтенкова, В. О. Кириленко, А. А. Привалов // Труды 70-й науч.-технич. конф., посвященной Дню радио. – СПб., 2015. – С. 312–314.

2. Гапанович В. А. Системы автоматизации и информационные технологии управления перевозками на железных дорогах / В. А. Гапанович, А. А. Грачев. – М. : Маршрут, 2006. – 541 с.

3. ГОСТ РВ 51987-2002. Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения. – М. : Госстандарт России, 2002. – 54 с.

4. Евглевская Н. В. Марковская модель конфликта автоматизированных систем обработки информации и управления с системой деструктивных воздействий нарушителя / Н. В. Евглевская, А. А. Привалов, Е. В. Скуднева // Известия ПГУПС. – 2015. – Вып. 1 (42). – С. 78–84.

5. Евглевская Н. В. Модель процесса подготовки злоумышленника к информационному воздей-

ствию на автоматизированные системы управления железнодорожным транспортом / Н. В. Евглевская, А. А. Привалов, Ал. А. Привалов // Бюллетень результатов научных исследований. – 2012. – № 5 (4). – С. 17–25.

6. Карабанов Ю. С. Модуль анализа потенциальных моделей угроз телекоммуникационных объектов ОАО «РЖД» / Ю. С. Карабанов, А. А. Привалов, П. Э. Чимирзаев // Труды 70-й науч.-технич. конф., посвященной Дню радио. – СПб., 2015. – С. 310–311.

7. Карабанов Ю. С. Модуль инициализации программного комплекса анализа угроз безопасности телекоммуникационного объекта ОАО «РЖД» / Ю. С. Карабанов, В. О. Кириленко, А. А. Привалов // Труды 70-й науч.-технич. конф., посвященной Дню радио. – СПб., 2015. – С. 311–312.

8. Королев А. И. Модуль математического моделирования компьютерных атак и добывания нарушителем данных по техническим каналам утечки информации / А. И. Королев, А. А. Привалов, П. Э. Чимирзаев // Труды 70-й науч.-технич. конф., посвященной Дню радио. – СПб., 2015. – С. 314–315.

9. Коцыняк М. А. Устойчивость информационно-телекоммуникационных сетей / М. А. Коцыняк, И. А. Кулешов, О. С. Лаута. – СПб. : Санкт-Петербург. гос. политехнич. ун-т, 2013. – 91 с.

10. Куделя В. Н. Методы математического моделирования систем и процессов связи / В. Н. Куделя, А. А. Привалов, О. В. Петриева, В. П. Чемиренко. – СПб. : Изд-во Политехнич. ун-та, 2009. – 368 с.

11. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ / А. А. Привалов. – СПб. : ВМА, 2000. – 166 с.

12. Привалов А. А. Модель процесса вскрытия каналов утечки информации на объектах телекоммуникаций / А. А. Привалов, Н. В. Евглевская, Ал. А. Привалов // Вопр. радиоэлектроники. – 2014. – №. 1. – С. 156–161.

13. Привалов А. А. Модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя / А. А. Привалов, Н. В. Евглевская, К. Н. Зубков // Изв. ПГУПС. – 2014. – Вып. 2 (39). – С. 106–111.

14. Привалов А. А. Разработка программного комплекса для оценки информационной безопасности торгового объекта / А. А. Привалов, Н. В. Евглевская, В. О. Кириленко, Е. О. Болтенкова // Проблемы экономики и управления в торговле и промышленности. – 2015. – № 3 (011). – С. 63–72.

15. Привалов А. А. Структура программного комплекса моделирования информационного конфликта системы безопасности телекоммуникационного объекта РЖД с подсистемой нарушителя / А. А. Привалов, Ю. С. Карабанов, А. И. Королев, С. И. Сидоров // Интеллектуальные технологии на транспорте. – 2015. – № 1. – С. 22–31.

References

1. Boltenkova Ye.O., Kirilenko V. O. & Privalov A. A. Modul postroyeniya maketa telekommunikatsionnogo obyekta OAO RZhD [Modular Layout for Designing Telecommunications Object of the Russian Railways JSC]. *Trudy 70-y nauchno-tekhnicheskoy konferentsii, posvyashchennoy Dnyu Radio* (*Proc. of 70th Sci. and Practical Conf. Dedicated to Radio Day*). St. Petersburg, 2015. Pp. 312-314.

2. Gapanovich V. A. & Grachev A. A. Sistemy avtomatizatsii i informatsionnyye tekhnologii upravleniya perevozkami na zheleznykh dorogakh [Automation Systems and Information Technologies for Railway Traffic Control]. Moscow, Marshrut, 2006. 541 p.

3. GOST RV 51987-2002. Informatsionnaya tekhnologiya. Kompleks standartov na avtomatizirovannye sistemy. Tipovye trebovaniya i pokazateli kachestva funkcionirovaniya informacionnyh sistem. Obshchie polozheniya [Information Technology. Set of Standards for Automated Systems. Typical Requirements and Indicators of the Quality of Information Systems. General Provisions]. Moscow, Gosstandart Rossii, 2002. 54 p.

4. Evglevskaya N. V., Privalov A. A. & Skudneva Ye. V. *Izvestiya PGUPS – Proc. Petersburg Transp. Univ.*, 2015, Is. 1 (42), pp. 78-84.

5. Evglevskaya N. V., Privalov A. A. & Privalov Al. A. *Byulleten rezultatov nauchnykh issledovaniy – Bull. Res. Results*, 2012, no. 5 (4), pp. 17-25.

6. Karabanov Yu.S., Privalov A. A. & Chimirzayev P. E. Modul analiza potentsialnykh modeley ugroz telekommunikatsionnykh obyektov OAO RZhD

[Potential Threat Analysis Module for Russian Railways JSC Telecommunications Objects]. *Trudy 70-y nauchno-tekhnicheskoy konferentsii, posvyashchennoy Dnyu Radio* (*Proc. of 70th Sci. and Practical Conf. Dedicated to Radio Day*). St. Petersburg, 2015. Pp. 310-311.

7. Karabanov Yu.S., Kirilenko V.O. & Privalov A.A. Modul initsializatsii programmnogo kompleksa analiza ugroz bezopasnosti telekommunikatsionnogo obyekta OAO RZhD [Module for Initiation of Program Complex for Analysis of Security Threats for Russian Railways JSC Telecommunications Object]. *Trudy 70-y nauchno-tekhnicheskoy konferentsii, posvyashchennoy Dnyu Radio* (*Proc. of 70th Sci. and Practical Conf. Dedicated to Radio Day*). St. Petersburg, 2015. Pp. 311-312.

8. Korolev A.I., Privalov A.A. & Chimirzayev P.E. Modul matematicheskogo modelirovaniya kompyuternykh atak i dobyvaniya narushitelem dannykh po tekhnicheskim kanalam utechki informatsii [Module for Mathematical Simulation of Computer Attacks and Attacker Obtaining Data through Technical Channels of Information Leak]. *Trudy 70-y nauchno-tekhnicheskoy konferentsii, posvyashchennoy Dnyu Radio* (*Proc. of 70th Sci. and Practical Conf. Dedicated to Radio Day*). St. Petersburg, 2015. Pp. 314-315.

9. Kotsynyak M.A., Kuleshov I.A. & Lauta O.S. Ustoychivost informatsionno-telekommunikatsionnykh setey [Stability of Information and Telecommunications Networks]. St. Petersburg, Sankt-Peterburgskiy gosudarstvennyy politekhnicheskiy universitet, 2013. 91 p.

10. Kudelya V.N., Privalov A.A., Petriyeva O.V. & Chemirenko V.P. Metody matematicheskogo modelirovaniya sistem i protsessov svyazi [Methods of Mathematical Simulation of Communication Systems and Processes]. St. Petersburg, Izdatelstvo Politekhnicheskogo universiteta, 2009. 368 p.

11. Privalov A.A. Metod topologicheskogo preobrazovaniya stokhasticheskikh setey i yego ispolzovaniye dlya analiza sistem svyazi VMF [A Method of Topological Transformation of Stochastic Networks and Its Application for Analysis of Navy Communication Systems]. St. Petersburg, VMA, 2000. 166 p.

12. Privalov A.A., Evglevskaya N.V. & Privalov Al.A. *Voprosy radioelektroniki – Radioelectronics Issues*, 2014, no. 1, pp. 156-161.

13. Privalov A.A., Evglevskaya N.V. & Zubkov K.N. *Izvestiya PGUPS – Proc. Petersburg Transp. Univ.*, 2014, Is. 2 (39), pp. 106-111.

14. Privalov A.A., Evglevskaya N.V., Kirilenko V.O. & Boltenkova Ye.O. *Problemy ekonomiki i upravleniya v torgovle i promyshlennosti – Prob. of Econ. and Management in Trade and Industry*, 2015, no. 3 (011), pp. 63-72.

15. Privalov A.A., Karabanov Yu.S., Korolev A.I. & Sidorov S.I. *Intellectualnyye tekhnologii na transporte – Intelligent Technologies in Transport*, 2015, no. 1, pp. 22-31.

*ЕВГЛЕВСКАЯ Наталья Валерьевна – электромеханик, n.evglevskaya@gmail.com (Центральный региональный центр связи); БЕКБАЕВ Гамзатдин Алеуатдинович – аспирант, gamzat-86@mail.ru; ПРИВАЛОВ Андрей Андреевич – доктор воен. наук, профессор, aprivalov@inbox.ru (Петербургский государственный университет путей сообщения Императора Александра I); ШАХМАТОВ Дмитрий Николаевич – соискатель, d.shakhmatov@mail.ru (Военная академия связи имени Маршала Советского Союза С.М. Будённого).