УДК 62-519 DOI:10.31854/1813-324X-2020-6-1-32-42

Комплекс моделей функционирования и управления пакетной радиосетью КВ-диапазона

Д.О. Беляев[1], А.К. Канаев[2], С.П. Присяжнюк[1, 3], М.А. Сахарова[2*], Р.П. Сорокин[2]

[1]ЗАО «Институт телекоммуникаций»,
Санкт-Петербург, 194100, Российская Федерация
[2]Санкт-Петербургский государственный университет путей сообщения Императора Александра I,
Санкт-Петербург, 190031, Российская Федерация
[3]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербург, 197101, Российская Федерация
[*]Адрес для переписки: zuvakamariya@mail.ru

Информация о статье
Поступила в редакцию 02.12.2019
Принята к публикации 19.02.2020

Ссылка для цитирования: Беляев Д.О., Канаев А.К., Присяжнюк С.П., Сахарова М.А., Сорокин Р.П. Комплекс моделей функционирования и управления пакетной радиосетью КВ-диапазона // Труды учебных заведений связи. 2020. Т. 6. № 1. С. 32–44. DOI:10.31854/1813-324X-2020-6-1-32-42

Аннотация: *Разработана концептуальная модель системы управления для обеспечения устойчивого функционирования проектируемой перспективной пакетной радиосетью КВ-диапазона. Функции управления на уровне Element management system предложено реализовать на базе автоматизированных радиоцентров, а функции управления уровня Network Management System – реализовать на базе выделенного сервера. Такой подход к управлению позволяет построить иерархическую централизованную архитектуру системы управления радиосетью. Выполнено имитационное моделирование для разработанных алгоритмов выделенных функций управления радиосетью. В работе представлены результаты моделирования, а именно – вероятностно-временные характеристики процессов управления состоянием узлов, маршрутизации и функционирования в условиях атак.*

Ключевые слова: *система управления, пакетная радиосеть КВ-диапазона, UML, надежность, маршрутизация, безопасность, моделирование.*

Введение

Перспективная пакетная радиосеть КВ-диапазона предназначена для обеспечения связью подвижных и стационарных групп и отдельных абонентов, удаленных на большие расстояния (до 5000 км), когда оказываются недоступными традиционные средства связи [1]. В этом смысле пакетная радиосеть является межвидовой резервной сетью связи, обеспечивающей гарантированную передачу данных от командных центров до удаленных объектов управления. Функции сетевого уровня пакетной радиосетью КВ-диапазона выполняют управляемые модульные маршрутизаторы (УММ). В состав УММ входят интерфейсные модули радиоканала (ИМ-Р), интерфейсные модули абонентов (ИМ-А), процессорный модуль коммутации и маршрутизации (ПМ-КМ) и процессорный модуль контроля и управления (ПМ-КУ). Развитие систем связи, в частности радиосетей, на основе пакетных технологий требует соответствующей модернизации или разработки новой модели системы управления. Объектом управления является перспективная пакетная радиосеть КВ-диапазона.

Концептуальная модель системы управления пакетной радиосетью

Разработана концептуальная модель системы управления (СУ) пакетной радиосетью (рисунок 1), отличающаяся от известных распределением функций согласно архитектуре TMN [2] по уровням управления. На каждом из уровней выделены базы данных, предоставляющие операторам необходимые и достаточные сведения для выполнения своих обязанностей. А также представленная модель системы управления позволяет выполнять задачи контроля, учета, планирования и эксплуатации проектируемой пакетной радиосети [3].

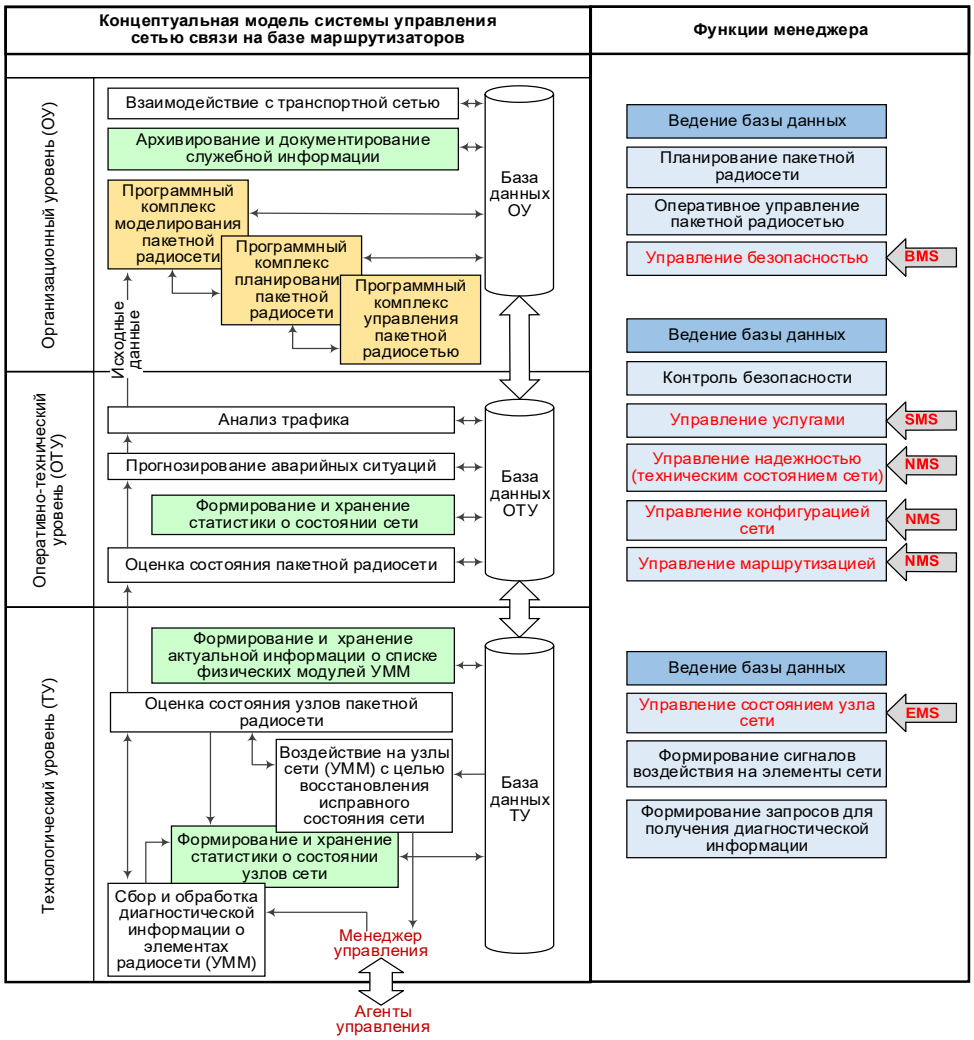


Рис. 1. Концептуальная модель системы управления пакетной радиосетью

Fig. 1. Conceptual Model of Packet Radio Network Management System

Модель процесса управления состояниями узлов пакетной радиосети

Мониторинг как подпроцесс управления состоянием узлов пакетной радиосети представляет собой единый комплекс систематических целенаправленных мероприятий (организационных, технологических и технических), основанный на непрерывном, либо периодическом наблюдении за состоянием узлов сети (сбор, хранение, обработка и анализ информации о состоянии), качественном и количественном оценивании состояния и прогнозировании изменений состояния объекта исследования под влиянием деструктивных факторов.

В зависимости от необходимости или решения определенных задач, процесс мониторинга может быть выполнен как автоматизировано, так и автоматически, что представлено на UML-диаграмме модели (рисунок 2). Реализации описанных выше процессов мониторинга представлены на рисунке 3.

Модули маршрутизатора с заданной периодичностью T_{din} (мин.) формируют потоки диагностических данных, что реализовано в модели блоками {M_1..M_7}. Модуль контроля обрабатывает поток диагностических данных за время T_{kontr} и передает через программу ПМ-КМ по каналу связи администратору сети, который выполняет процесс технической диагностики за время T_{diagn}. По ее результатам формируется диагностическое решение, соответствующее одному из обнаруженных состояний маршрутизатора $S = \{S_{испр}, S_{неиспр}\}$.

При выявлении неисправного состояния маршрутизатора $S_{неиспр}$ выполняется процесс восстановления за время T_{vosst} и контрольная проверка выполненных мероприятий. Процесс выполнения контрольной проверки состояния маршрутизатора выполняется по алгоритму реализации процесса мониторинга в статическом режиме.

При наличии встроенных средств диагностики выполняется процесс контроля каждого модуля маршрутизатора за время T_{kontr}, а при их отсутствии – дополнительно выполняется процесс измерения ДД внешними средствами диагностики за время T_{izm}.

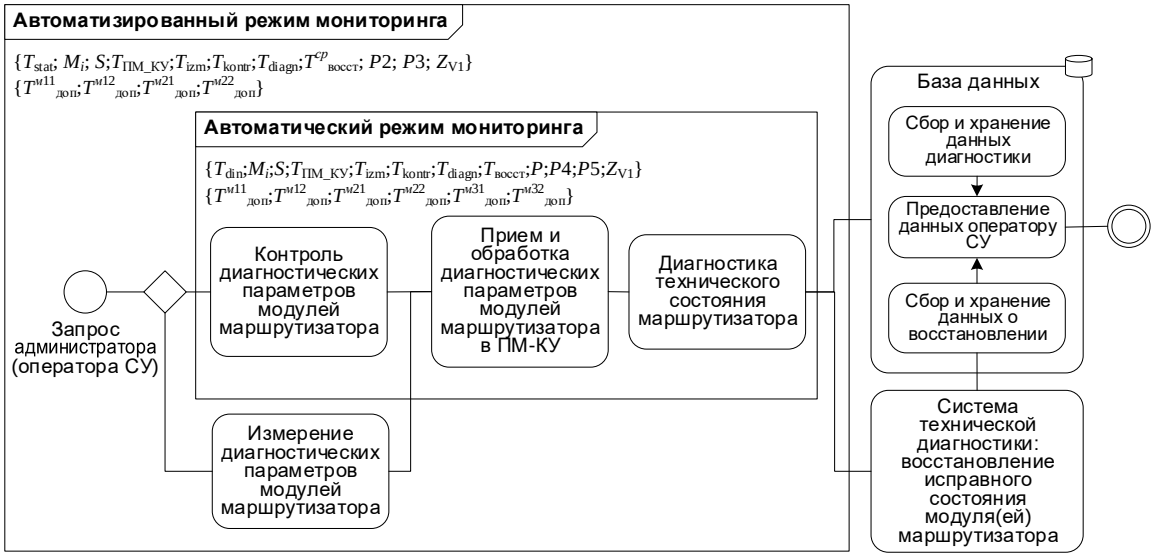


Рис. 2. UML-диаграмма процесса управления состоянием узлов радиосети

Fig. 2. UML-Diagram of the Process of Managing the State of Radio Network Nodes

Требуется определить время работы системы мониторинга при заданных исходных данных (см. таблицу 1).

ТАБЛИЦА 1. Исходные данные

TABLE 1. Source Data

№ п/п	Характеристики элементов сети	Значение
1.	Период предоставления данных модулями УММ системе управления	{0,25..5} мин.
2.	Генератор запросов от администратора сети	{1..60} мин.
3.	Количество состояний модулей УММ	$\{S_{испр}, S_{неиспр}\}$
4.	Величина задержки в ПМ-КМ	3÷7 мс
5.	Закон распределения времени задержки в канале связи	Нормальный (*normal*)
6.	Длительность процесса измерения	Не более 5 мин.
7.	Длительность процесса контроля	Не более 5 мин.
8.	Длительность процесса диагностики	Не более 5 мин.
9.	Среднее время восстановления исправного состояния	Не более 30 мин.
10.	Закон распределения длительностей процессов измерения, контроля и диагностики, восстановления	Нормальный (*normal*)
11.	Закон распределения вероятности обнаружения исправного состояния	Вейбулла (*weibull*)
12.	Заданная (начальная) вероятность обнаружения исправного состояния	0,85
13.	Заданная (начальная) вероятность обнаружения исправного состояния после восстановления	0,8
14.	Заданная (начальная) вероятность обнаружения исправного состояния после повторного восстановления	0,9
15.	Величина задержки в канале связи	0,5÷2с
16.	Закон распределения времени задержки в канале связи	Нормальный (*normal*)

При выполнении моделирования процессов управления заданной сетью приняты следующие допущения:

– вместимость всех входных буферов принята максимальной;

– функция распределения случайных величин относится к классу экспоненциальных;

– вероятности, соответствующие ветвям стохастической сети, определяются статистическими методами;

– модель предполагает отсутствие новых заявок до окончания обработки предыдущей;

– потоки заявок являются неконкурирующими.

С целью обеспечения непрерывной работы узла сети (маршрутизатора) к его системе мониторинга предъявляются жесткие требования по выполнению поставленных задач за отведенное время:

$$T_м = \{t_{изм}, t_{контр}, t_{диагн}, t_{восст}, t_{канал}, t_{пм\text{-}ку}\}.$$

Производится топологическое преобразование стохастической сети к эквивалентной. При этом эквивалентная функция определяется из топологического уравнения Мейсона согласно выражению, приведенному в [4].

На основе разработанной стохастической сети процесса автоматического мониторинга узла сети получены эквивалентная функция $F(s_{ЛПР})$ (1) и эквивалентная функция $F(s_{auto})$ (2). Методом двухмоментной аппроксимации для $F(s_{ЛПР})$ и $F(s_{auto})$ можно получить соответствующие функции распределения времени (рисунок 4) реализации цикла мониторинга узла сети (УММ), позволяющие сделать следующие выводы:

– при увеличении времени реализации цикла управления растет значение вероятности завершения цикла управления за отведенное время;

– цикл автоматизированного мониторинга с наибольшей вероятностью достигается за 120 мин.;

– цикл автоматического мониторинга с наибольшей вероятностью достигается за 90 мин.

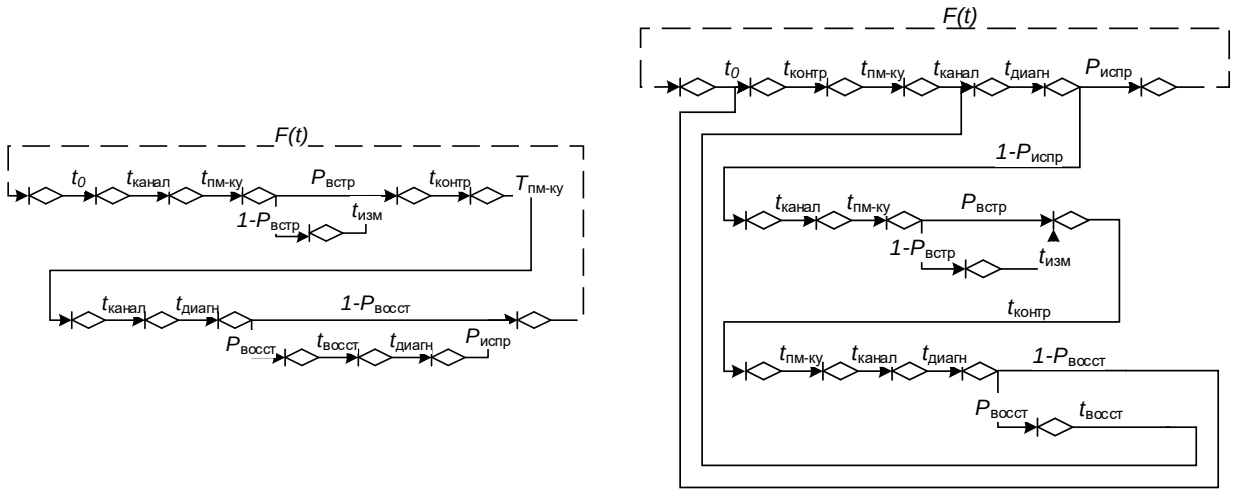


Рис. 3. Стохастическая сеть процесса автоматизированного (a) и автоматического (b) и мониторинга узла сети

Fig. 3. Stochastic Network for Automated (a) and Automatic (b) Packet Radio Network Management Based on UMM

$$F(s_{\text{ЛПР}}) = \frac{\left(\frac{t_{\text{канал}}}{t_{\text{канал}}+s}\right)^2 \left(\frac{t_{\text{пмку}}}{t_{\text{пмку}}+s}\right)^2 \frac{t_{\text{контр}}}{t_{\text{конт}}+s} \frac{t_{\text{диагн}}}{t_{\text{диагн}}+s} \left(P_{\text{встр}} + \left(1-P_{\text{встр}}\right)\frac{t_{\text{изм}}}{t_{\text{изм}}+s}\right)\left(\left(1-P_{\text{восст}}\right) + P_{\text{восст}} \frac{t_{\text{восст}}}{t_{\text{восст}}+s} \frac{t_{\text{диагн}}}{t_{\text{диагн}}+s} P_{\text{испр}}\right)}{1 - \left(\frac{t_{\text{канал}}}{t_{\text{канал}}+s}\right)^2 \left(\frac{t_{\text{пмку}}}{t_{\text{пмку}}+s}\right)^2 \frac{t_{\text{контр}}}{t_{\text{конт}}+s} \frac{t_{\text{диагн}}}{t_{\text{диагн}}+s} \left(P_{\text{встр}} + \left(1-P_{\text{встр}}\right)\frac{t_{\text{изм}}}{t_{\text{изм}}+s}\right)\left(P_{\text{восст}} \frac{t_{\text{восст}}}{t_{\text{восст}}+s} \frac{t_{\text{диагн}}}{t_{\text{диагн}}+s}\left(1-P_{\text{испр}}\right)\right)}, \quad (1)$$

$$F(s_{auto}) = \frac{\frac{t_{\text{контр}}}{t_{\text{конт}}+s} \frac{t_{\text{пмку}}}{t_{\text{пмку}}+s} \frac{t_{\text{канал}}}{t_{\text{канал}}+s} \frac{t_{\text{диагн}}}{t_{\text{диагн}}+s} P_{\text{испр}}}{1 - \left(\frac{t_{\text{контр}}}{t_{\text{конт}}+s}\right)^2 \left(\frac{t_{\text{канал}}}{t_{\text{канал}}+s}\right)^3 \left(\frac{t_{\text{пмку}}}{t_{\text{пмку}}+s}\right)^3 \left(\frac{t_{\text{диагн}}}{t_{\text{диагн}}+s}\right)^2 \left(1-P_{\text{испр}}\right)\left(P_{\text{встр}} + \left(1-P_{\text{встр}}\right)\frac{t_{\text{изм}}}{t_{\text{изм}}+s}\right)\left(1-P_{\text{восст}}\right) - \frac{1}{-\left(\frac{t_{\text{контр}}}{t_{\text{конт}}+s}\right)\left(\frac{t_{\text{канал}}}{t_{\text{канал}}+s}\right)^2 \left(\frac{t_{\text{пмку}}}{t_{\text{пмку}}+s}\right)^2 \left(\frac{t_{\text{диагн}}}{t_{\text{диагн}}+s}\right)^2 \left(1-P_{\text{испр}}\right)\left(P_{\text{встр}} + \left(1-P_{\text{встр}}\right)\frac{t_{\text{изм}}}{t_{\text{изм}}+s}\right) P_{\text{восст}} \frac{t_{\text{восст}}}{t_{\text{восст}}+s}}}. \quad (2)$$

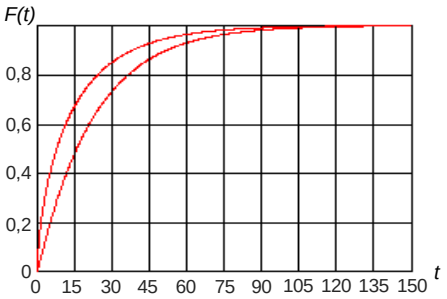


Рис. 4. Функция распределения времени реализации цикла мониторинга

Fig. 4. The Distribution Function of the Time of Realization of the Monitoring Cycle

Модель процесса маршрутизации пакетной радиосети

Маршрутизация является процессом определения маршрута следования информации в сетях связи. В модели OSI маршрутизация является функцией сетевого уровня, где выполняет:

– поддержание маршрутно-адресных таблиц (МАТ) и обмен информацией об изменениях в топологии сети с другими маршрутизаторами; эта функция реализуется с помощью одного или нескольких протоколов маршрутизации либо при помощи статически настроенных МАТ;

– перенаправление пакетов с входного интерфейса маршрутизатора на выходной интерфейс в зависимости от МАТ; при необходимости маршрутизатор может произвести переупаковку пакета из одного вида канального уровня в другой.

Процесс маршрутизации использует МАТ, протоколы и алгоритмы маршрутизации, чтобы определить наиболее эффективный путь для пересылки пакета. Формирование МАТ может быть выполнено как статическим методом, так и динамическим [5].

Анализ существующих протоколов маршрутизации представлен в [5]. С целью минимизации служебной нагрузки было предложено новое алгоритмическое решение. В [6] предложен способ оперативного управления потоками данных в сетях с коммутацией пакетов (способ зондирования) для контроля состояния сети и построения плана распределения потоков данных в условиях высокой неоднородности каналов и динамических структурных изменений КВ-радиосети. UML-диаграмма разработанного способа представлена на рисунке 5.

На базе представленного решения может быть разработано множество вариантов решений процесса зондирования, например, безадресное, адресное или взвешенное зондирование [6, 7]. В таблице 2

приведена краткая характеристика вариантов реализации зондирования. На основании представленных сведений приведем сравнительные результаты (рисунок 6) вариантов реализации зондирования.

Выявлено (см. рисунок 6а), что время сходимости при использовании взвешенного алгоритма зондирования на 30 секунд больше при скорости 1200 бит/с, чем при адресном зондировании. Также выявлено, что время сходимости не превышает 10 секунд при скорости более 9600 бит/с.

Показано (см. рисунок 6), что служебная загрузка при использовании алгоритма взвешенного зондирования не превышает 10 % от общей, что обеспечивает выполнение требований по оптимальному использованию накладных расходов.

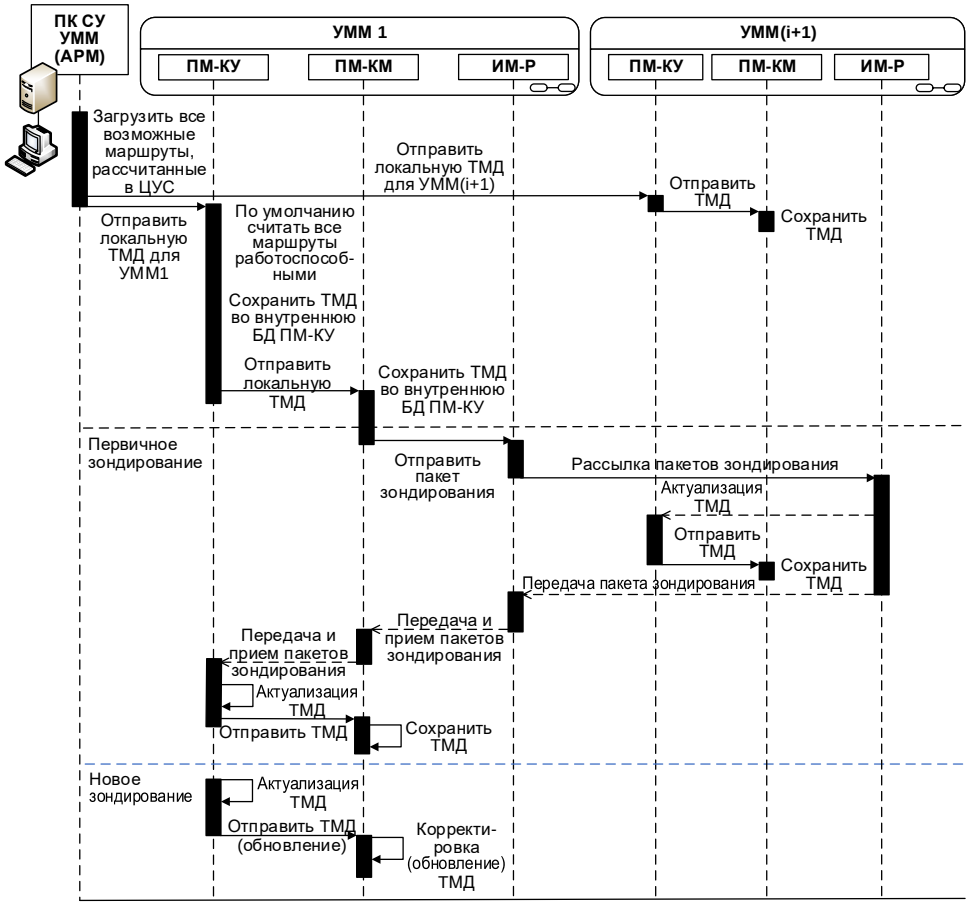


Рис. 5. UML-диаграмма реализации алгоритма зондирования сети

Fig. 5. UML Diagram of the Implementation of the Network Sensing Algorithm

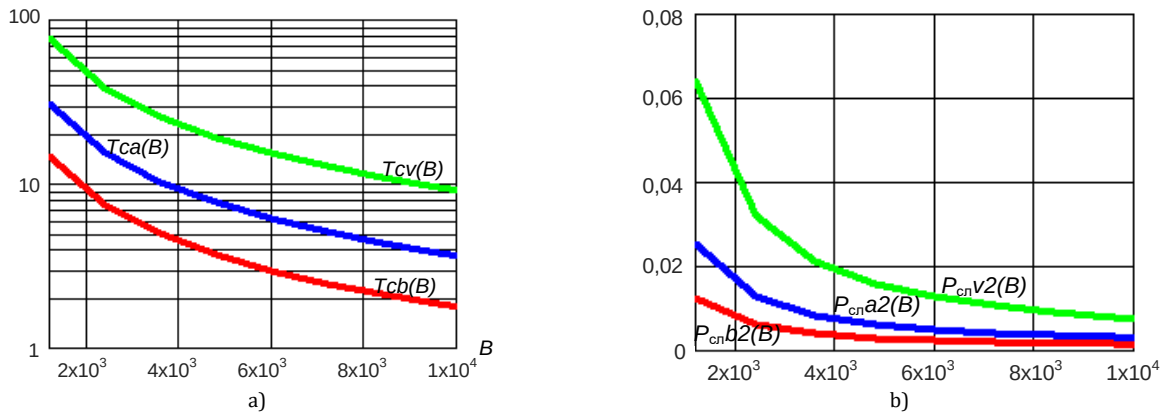


Рис. 6. Графики зависимости: a) времени сходимости протокола маршрутизации на основе алгоритма зондирования от скорости в канале (B); b) служебной загрузки Pсл от скорости в канале (B) при цикле зондирования 1200 с

Fig. 6. Dependency graph: a) time convergence of the routing protocol based on the sensing algorithm from the speed in the channel (B); b) Pсл service load from the speed in the channel (B) with a sensing cycle of 1200 s

ТАБЛИЦА 2. Варианты реализации зондирования

TABLE 2. Variants of Sensing Implementation

Параметр	Варианты реализации зондирования		
	Безадресное	Адресное	Взвешенное
Построение МАТ	Да	Да	Да
Построение матриц смежности	Нет	Да	Нет
Построение матриц весов	Нет	Нет	Да
Содержание служебного сообщения (зонда)	Порядковый номер узла ($P_{ном}$ = 1 бит)	Адреса смежных узлов в маршруте ($P_{адр}$ = 6 бит)	Адреса смежных узлов в маршруте ($P_{адр\_кс}$ = 8 бит)
Размер зонда, бит, где $P_{заг}$ = 64 бит	$P_b = P_{заг} + P_{ном}*N$	$P_a = P_{заг} + P_{адр}*N$	$P_v = P_{заг} + P_{адр\_кс}*N$
Результат	Сокращение служебного трафика. Обеспечение быстродействия.	Решение задачи распределения потоков. Контроль топологии сети.	Решение задачи распределения потоков. Полный контроль состояния сети.

Выполнение задачи маршрутизации с применением метода зондирования предполагается в два этапа.

Этап 1. Формирование МАТ

Формирование МАТ предложено реализовать одним из вариантов зондирования: безадресным, адресным, взвешенным.

Объем служебных (Рсл) сообщений зависит от выбранного алгоритма зондирования. Например, для сети из 32 узлов и минимальной связностью 3 для безадресного алгоритма зондирования Рсл соответствует 96 бит, для адресного алгоритма зондирования Рсл = 256 бит, для взвешенного алгоритма зондирования Рсл = 320 бит.

На основании полученных результатов предлагается использовать для формирования маршрутно-адресных таблиц алгоритм взвешенного зондирования в радиосети ДКМВ-диапазона.

Этап 2. Выбор маршрута для передачи данных

Формирование маршрута для передачи данных обеспечивается алгоритмом адаптивной одношаговой маршрутизации по запросу (рисунок 7).

Модель процесса функционирования пакетной радиосети в условиях реализации атак

Гарантированная передача данных по каналам пакетной радиосети, являющейся межвидовой резервной сетью связи, может быть нарушена под влиянием внешних дестабилизирующих факторов. В то же время эти факторы способствуют несоблюдению принципов конфиденциальности, целостности и доступности информации, тем самым нарушая безопасность ее передачи. Одним из таких воздействий является атака «Взлом паролей», в ходе которой нарушитель стремится получить доступ к системе от имени доверенного пользователя. Однако данные атаки будут иметь абсолютно другие последствия, если нарушитель получает доступ в систему от имени доверенного пользователя. В этом случае, наличие системы безопасности и ее исправная работа не гарантирует обеспечения конфиденциальности, целостности и доступности информации.

Рис. 7. Алгоритм адаптивной одношаговой маршрутизации по запросу

Fig. 7. Adaptive One-Step Routing Algorithm on Request

Рассмотрим разработанную модель реализации атаки «Взлом паролей». Пусть задана пакетная радиосеть [1, 10], которая функционирует в условиях воздействия угрозы несанкционированного доступа к передаваемой информации. Предполагается, что нарушитель имеет непосредственный доступ к устройству, в котором необходимо взломать пароли. При реализации атаки «Взлом паролей» нарушитель активирует атакуемое устройство и инициализирует BIOS за среднее время $\bar{t}_{уст}$ с функцией распределения *B3(t)*. После инициализации BIOS с вероятностью $P_{ат}$ изменяются настройки первичной загрузки за среднее время $\bar{t}_{настр}$ с функцией распределения *C3(t)*. Далее за среднее время $\bar{t}_{нос}$ с функцией распределения *D3(t)* устанавливается сменный носитель, на него пере-

дается управление за среднее время $\bar{t}_{упр}$ с функцией распределения *F3(t)* и с вероятностью $P_{ос}$ происходит загрузка альтернативной операционной системы устройства за среднее время $\bar{t}_{ос}$ с функцией распределения *G3(t)*. После этого нарушитель копирует файлы SAM и SYSTEM на электронный носитель за среднее время $\bar{t}_{ss}$ с функцией распределения *H3(t)* и носитель извлекается из атакуемого устройства за среднее время $\bar{t}_{нос}$ с функцией распределения *D3(t)*.

На втором уровне атаки нарушитель действует удаленно без непосредственного доступа к атакуемому устройству. Устанавливается программа подбора паролей за среднее время $\bar{t}_{уст}$ с функцией распределения *J3(t)*, далее за среднее время $\bar{t}_{нос}$ с функцией распределения *D3(t)* устанавливается сменный носитель. После этого за среднее время $\bar{t}_{зап}$ с функцией распределения *K3(t)* установленная программа запускается и подбирает нужный пароль, сравнивая информацию, хранящуюся в скопированных файлах *SAM* и *SYSTEM* за среднее время $\bar{t}_{подб}$ с функцией распределения *L3(t)*. С вероятностью $P_{пар}$ проводимые мероприятия будут выполнены успешно. В случае, если пароль подобрать не удалось, программа подбора запускается вновь.

Третий уровень алгоритма может выполняться как удаленно, так и при непосредственном доступе к устройству. Удаленное выполнение возможно за счет загрузки альтернативной операционной системы, выполненной на первом уровне. Нарушитель включает устройство и инициализирует *BIOS* за среднее время $\bar{t}_{уст}$ с функцией распределения *B3(t),* после чего производит ввод подобранного пароля за среднее время $\bar{t}_{ввод}$ с функцией распределения *M3(t).* С вероятностью $P_{взлом}$ пароль подобран верно. В случае неуспешного подбора нарушитель вновь запускает программу подбора паролей [11, 12].

Моделирование выделенных этапов реализации атаки проводилось в компьютерной среде имитационного моделирования AnyLogic [13] согласно исходным данным (таблица 3), полученным в ходе экспертной оценки разработанного алгоритма модели. Области просмотра этапов реализации атаки представлены на рисунках 8–10.

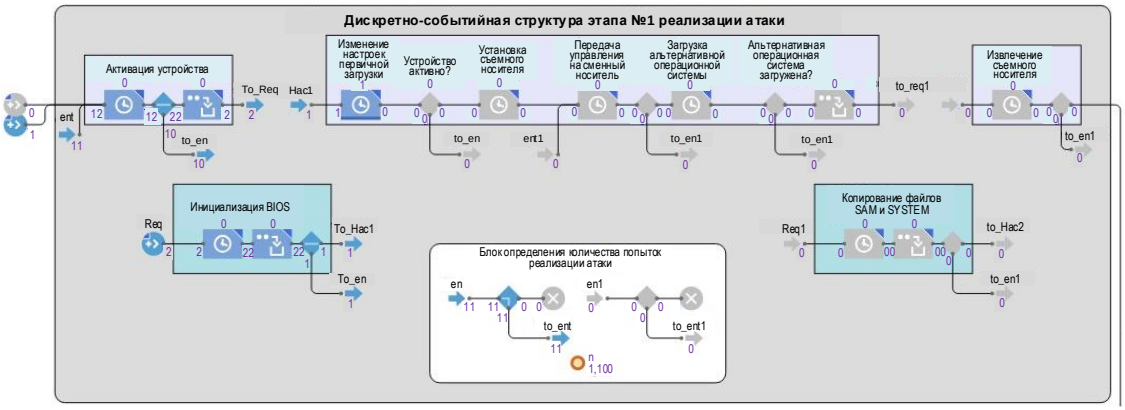


Рис. 8. Копирование необходимых файлов (уровень 1)

Fig. 8. Copying All the Required Files (Level 1)

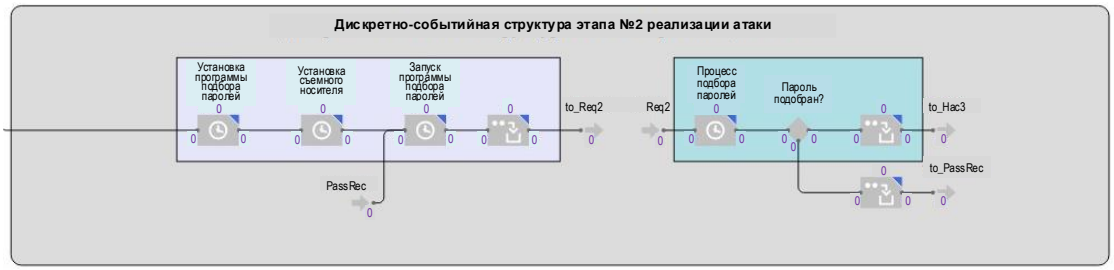


Рис. 9. Подбор пароля (уровень 2)

Fig. 9. Password Selection (Level 2)

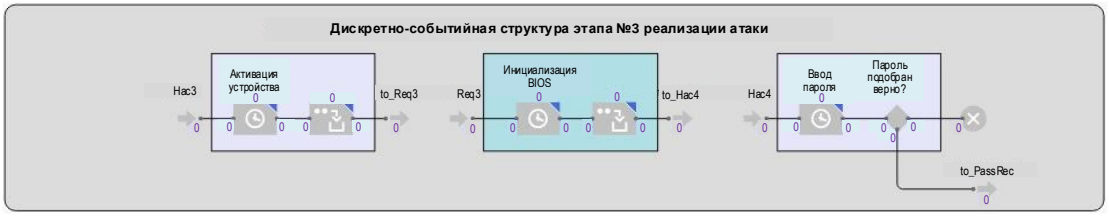
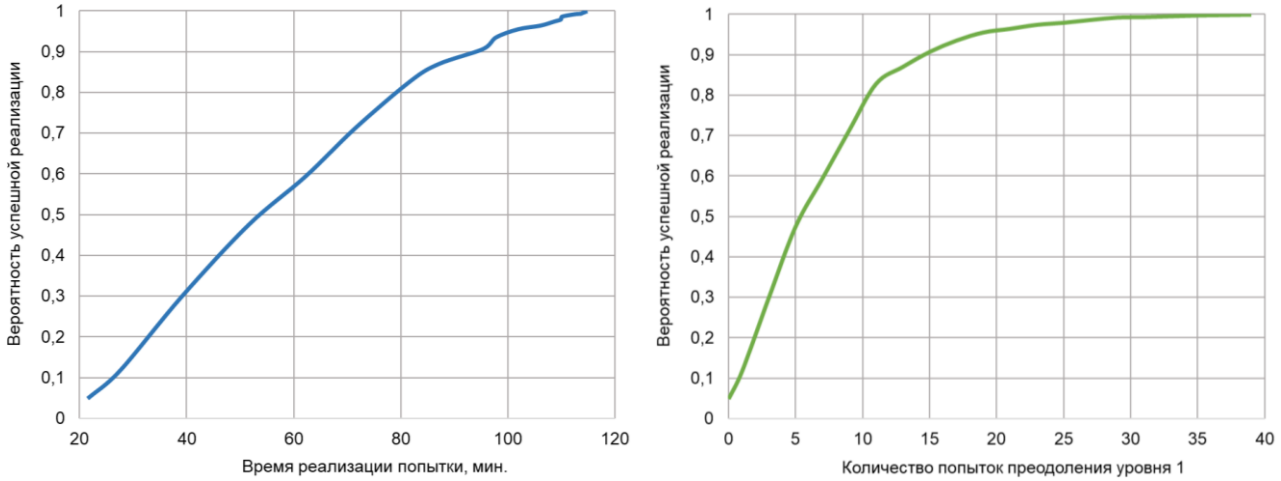


Рис. 10. Установление соединения (уровень 3)

Fig. 10. Establishing a Connection (Level 3)

В случае неуспешной реализации атаки нарушитель предпринимает повторную попытку совершения несанкционированного доступа. При этом число таких попыток (n) зависит от возможности нарушителя оставаться необнаруженным в ходе выполнения атаки, а также его оснащенности и подготовленности. С учетом этого получена вероятность успешного выполнения атаки «Взлом паролей» для 1000 попыток реализации. В случае неуспешного осуществления одного из этапов атаки нарушитель осуществляет повторную попытку в соответствии с заданным числом попыток реализации (n).

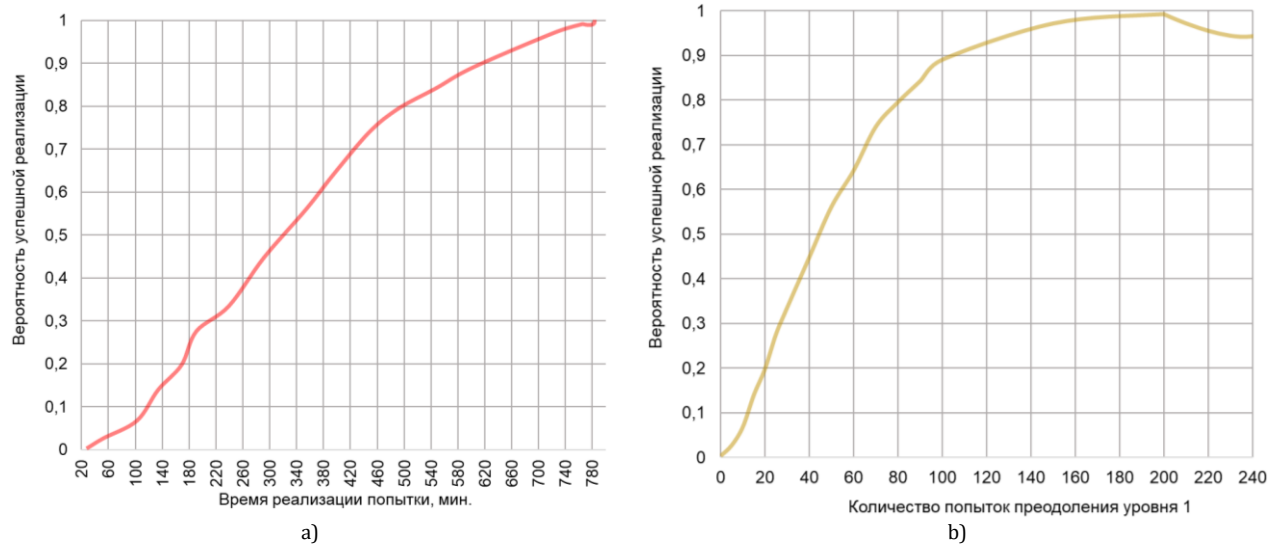
Полученные вероятностно-временные характеристики реализации атаки без учета дополнительных факторов обеспечения безопасности передачи информации представлены на рисунках 11a и 12a, а с учетом отсутствия предварительной информации об объекте атаки – на рисунках 11b и 12b.



a) b)

Рис. 11. Вероятностно-временные характеристики реализации атаки «взлом паролей»:
a) без учета дополнительных факторов обеспечения безопасности передачи информации;
b) с учетом отсутствия предварительной информации об объекте атаки

Fig. 11. Probabilistic-Characteristics of the Implementation of the "Password Hacking" Attack:
a) without Taking into Account Additional Factors for Ensuring the Security of Information Transfer;
b) Taking into Account the Lack of Preliminary Information About the Object of the Attack



a) b)

Рис. 12. Зависимость вероятности успешной реализации атаки от количества попыток реализации:
a) без учета дополнительных факторов обеспечения безопасности передачи информации;
b) с учетом отсутствия предварительной информации об объекте атаки

Fig. 12. Dependence of the Probability of Successful Implementation of the Attack on the Number of Implementation Attempts:
a) without Taking into Account Additional Factors for Ensuring the Security of Information Transfer;
b) Taking into Account the Lack of Preliminary Information About the Object of the Attack

Анализ полученных результатов (см. рисунки 11 и 12) позволяет сделать вывод, что среднее время реализации атаки «Взлом паролей» с вероятностью не менее 0,8 составляет 80 минут. При этом достаточно осуществить около 10 попыток реализации атаки, что позволяет говорить о необходимости разработки механизмов защиты.

ТАБЛИЦА 3. Вероятностно-временные характеристики реализации атаки

TABLE 3. Probabilistic-Time Characteristics of the Attack Implementation

№ п/п	Характеристика действий нарушителя	Аббр.	Значение
1.	Активация устройства и инициализация BIOS	$\bar{t}_{уст}$	7 секунд
2.	Функция распределения времени $\bar{t}_{ат}$	*B3(t)*	normal (5, 10)
3.	Изменение настроек первичной загрузки	$\bar{t}_{настр}$	20 секунд
4.	Функция распределения времени $\bar{t}_{алг}$	*C3(t)*	normal (15, 30)
5.	Вероятность активации устройства	$P_{ат}$	normal (0.3, 0.99)
6.	Установка съемного носителя	$\bar{t}_{нос}$	5 секунд
7.	Функция распределения времени $\bar{t}_{нос}$	*D3(t)*	normal (2, 10)
8.	Передача управления на носитель	$\bar{t}_{упр}$	7 секунд
9.	Функция распределения времени $\bar{t}_{упр}$	*F3(t)*	normal (5, 10)
10.	Загрузка альтернативной операционной системы	$\bar{t}_{ос}$	20 минут
11.	Функция распределения времени $\bar{t}_{ос}$	*G3(t)*	normal (10, 30)
12.	Вероятность успешной загрузки альтернативной операционной системы	$P_{ос}$	normal (0.3, 0.99)
13.	Копирование файлов SAM и SYSTEM	$\bar{t}_{ss}$	10 секунд
14.	Функция распределения времени $\bar{t}_{ss}$	*H3(t)*	normal (5,15)
15.	Установка программы подбора паролей	$\bar{t}_{уст}$	2 минуты
16.	Функция распределения времени $\bar{t}_{уст}$	*J3(t)*	normal (1, 3)
17.	Запуск программы подбора паролей	$\bar{t}_{зап}$	20 секунд
18.	Функция распределения времени $\bar{t}_{зап}$	*K3(t)*	normal (10, 30)
19.	Процесс подбора паролей	$\bar{t}_{подб}$	1 час
20.	Функция распределения времени $\bar{t}_{подб}$	*L3(t)*	normal (0.2, 2)
21.	Вероятность подбора пароля	$P_{пар}$	normal (0.2 ,0.99)
22.	Ввод подобранного пароля	$\bar{t}_{ввод}$	10 секунд
23.	Функция распределения времени $\bar{t}_{ввод}$	*M3(t)*	normal (5, 15)
24.	Вероятность успешного подбора пароля	$P_{взлом}$	normal (0.3, 0.99)

С учетом отсутствия предварительной информации об объекте атаки, среднее время реализации атаки «Взлом паролей» с вероятностью более 0,8 составляет 480 минут. При этом достаточно осуществить около 80 попыток преодоления 1 уровня реализации атаки, что значительно превышает существующие требования по разведзащищенности систем связи различного назначения.

Современные системы защиты информации должны работать не только на программном, но и на техническом уровне. Как показало исследование, проведение атаки «Взлом паролей» достаточно трудоемкий, но при этом выполнимый процесс, который под силу осуществить подготовленному и технически оснащенному нарушителю. Чтобы усложнить задачу подбора пароля, необходимо придерживаться ряда рекомендаций по безопасности и защите информации.

Заключение

В работе представлены частные решения модели функционирования и управления пакетной радиосетью КВ-диапазона, в частности модель функционирования системы управления пакетной радиосетью, модуль процесса маршрутизации пакетной радиосети, модель процесса функционирования пакетной радиосети в условиях реализации атак. Представленные частные модели позволили получить вероятностно-временные характеристики функционирования пакетной радиосети КВ-диапазона.

Выполнено имитационное и аналитическое моделирование процессов управления проектируемой перспективной пакетной радиосетью КВ-диапазона в рамках разработанной концептуальной модели системы управления, что позволило сделать вывод об эффективности предложенных решений по разноуровневому управлению сетью.

Стоит также отметить, что коллективом авторов реализовано специальное программное обеспечение системы управления перспективной пакетной радиосетью, что подтверждено свидетельствами о регистрации программ для ЭВМ [14, 15].

Список используемых источников

1. Присяжнюк С.П., Присяжнюк А.С. Модель управления когнитивной декаметровой радиосетью // Информация и космос. 2018. № 4. С. 44–48.

2. Гребешков А.Ю. Управление сетями электросвязи по стандарту TMN: учеб. пособие. М.: Радио и связь, 2004. 155 с.

3. Сахарова М.А., Канаев А.К. Управление состоянием сети передачи данных оперативно-технологического назначения // Международная конференция по мягким вычислениям и измерениям. 2018. Т. 1. С. 470–472.

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

5. Каплин А.Ю., Канаев А.К., Коротин А.А., Лямаев Д.Б., Сахарова М.А., Лукичев М.М. Исследование влияния протоколов маршрутизации на функционирование MANET сетей специального назначения и определение условий моделирования // Радиоэлектронные комплексы многоцелевого назначения: сборник научных трудов. СПб: Политехника, 2016. С. 111–123.

6. Присяжнюк С.П., Аванесов М.Ю. Способ оперативного управления потоками данных в сетях с коммутацией пакетов. Патент на изобретение RUS 2574814 от 12.08.2014. Опубл. 10.02.2016. Бюл. № 4.

7. Аванесов М.Ю. Оперативное управление потоками данных в мультисервисных сетях связи. СПб.: БГТУ, 2007. 87 с.

8. Канаев А.К., Опарин Е.В. Формирование процесса управления безопасностью организации, реализующей технологический процесс // 73-я Всероссийская научно-техническая конференция, посвященная Дню радио: сборник трудов. СПб: Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина), 2018. С. 302–303.

9. Р 50.1.053. Информационные технологии. Основные термины и определения в области технической защиты информации. Введ. с 01.01.2006. Москва: Стандартинформ, 2005. 12 с.

10. Присяжнюк С.П., Присяжнюк А.С., Сахарова М.А., Логин Э.В. Дискретно-событийная модель функционирования пакетной радиосети КВ-диапазона общего пользования // Информация и космос. 2019. № 2. С. 41–48.

11. Ануфренко А.В., Канаев А.К., Логин Э.В. Модель воздействия злоумышленника на фрагмент транспортной сети связи на основе технологии Carrier Ethernet // Труды учебных заведений связи. 2018. Т. 4. № 3. С. 17-25. DOI:10.31854/1813-324X-2018-4-3-17-25

12. Канаев А.К., Марченко Д.В., Субботин Д.В. Модели функционирования транспортной сети связи специального назначения, учитывающие высокую динамику изменения состояний сети вследствие внешнего воздействия // VII Международная научно-техническая и научно-методическая конференция. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018, Санкт-Петербург, Россия, 28 февраля–01 марта 2018 г.): сборник статей. Санкт-Петербург: СПбГУТ, 2018. С. 304–308.

13. Боев В.Д., Кирик Д.И., Сыпченко Р.П. Компьютерное моделирование: Пособие для курсового и дипломного проектирования // СПб.: ВАС, 2011. 348 с.

14. Присяжнюк А.С., Сахарова М.А., Беляев Д.О., Ильюшко Д.В., Бочаров П.М., Овчинников Г.Р. Программный комплекс контроля и мониторинга радиосети. Свидетельство о регистрации программы для ЭВМ. RUS 2019617338 от 27.05.2019. Опубл. 06.06.2019.

15. Присяжнюк А.С., Сахарова М.А., Логин Э.В. Программа имитационного моделирования процессов функционирования и управления радиосетью связи. Свидетельство о регистрации программы для ЭВМ. RUS 2019613923 от 12.03.2019. Опубл. 26.03.2019.

* * *

Conceptual Model of HF-Band Packet Radio Network Control System

D. Belyaev[1], **A. Kanaev**[2], **S. Prisyazhniuk**[1, 3], **M. Saharova**[2], **R. Sorokin**[2]

[1]JSC "Institute of telecommunications»,
St. Petersburg, 194100, Russian Federation
[2]Emperor Alexander Ist. Petersburg State Transport University,
St. Petersburg, 190031, Russian Federation
[3]Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
St. Petersburg, 197101, Russian Federation

Article info
DOI:10.31854/1813-324X-2020-6-1-32-42
Received 2nd December 2019
Accepted 19th February 2020

For citation: Belyaev D., Kanaev A., Prisyazhniuk S., Saharova M., Sorokin R. Conceptual Model of HF-Band Packet Radio Network Control System. *Proc. of Telecom. Universities.* 2020;6(1):32–42. (in Russ.) DOI:10.31854/1813-324X-2020-6-1-32-42

Abstract: *The author develop the conceptual control system model to ensure the sustainable projected promising packet radio network HF-band operating. It is proposed to implement the control functions at the Element Management System level on the basis of automated radio centers, and to implement the Network Management System level management functions on the basis of a dedicated server. Such a management approach allows you to build a hierarchical centralized radio network management system architecture. We can observe a simulation modeling for the developed algorithms of the selected radio network control functions. The paper presents the simulation results, namely probabilistic-temporal characteristics of the processes reliability, routing and functioning under attacks.*

Keywords: *control system, HF-band packet radio network, UML, reliability, routing, safety, simulation.*

References

1. Prisyazhniuk A., Prisyazhniuk S. Control model of cognitive decameter radio network. *Information and Space*. 2018;4(8):44–48. (in Russ.)
2. Grebeshkov A.Yu. *Management of Telecommunication Networks According to the TMN Standard*. Moscow: Radio i sviaz; 2004. 155 p. (in Russ.)
3. Sakharova M.A., Kanaev A.K. Management of the State of a Data Transmission Network for Operational and Technological Purposes. *International Conference on Soft Computing and Measurements*. 2018. vol.1. p.470–472. (in Russ.)
4. Privalov A.A. *The Method of Topological Transformation of Stochastic Networks and its Use for the Analysis of Communication Systems of the Navy*. St. Petersburg: S.M. Kirov Military Medical Academy Publ.; 2000. 166 p. (in Russ.)
5. Kaplin A.Yu., Kanaev A.K., Korotin A.A., Lamaev D.B., Saharova M.A., Lukichev M.M. *Influence of Routing Information Protocols on Functionality of Special Purpose MANET Nets with Determination of Modeling Conditions. Multipurpose Electronic Systems*. St. Petersburg: Politehknika Publ.; 2016. p.111–123. (in Russ.)
6. Prisyazhniuk S.P., Avanesov M.Yu. *A Method for Operational Control of Data Flows in Packet-Switched Networks*. Patent RF, no. 2574814, 08.12.2014. (in Russ.)
7. Avanesov M.Yu. *Operational management of data flows in multiservice communication networks*. St. Petersburg: Baltic State Technical University "VOENMEH" named after D.F. Ustinov Publ.; 2007. 87 p. (in Russ.)
8. Kanaev A.K., Oparin E.V. Formation of the Security Management Process of an Organization Implementing a Technological Process. *Proceedings of the 73rd All-Russian Scientific and Technical Conference dedicated to Radio Day*. St. Petersburg: Saint Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin); 2018. PP. 302–303. (in Russ.)
9. *P 50.1.053. Information technologies. Basic terms and definitions in scope of technical protection of information*. 01.01.2006. Moscow: Standardinform Publ.; 2005. 12 p. (in Russ.)
10. Prisyazhniuk S.P., Prisyazhniuk A.S., Sakharova M.A., Login E.V. Discrete-Event Model of Functioning of a Packet Radio Network of the KV Band of General Use. *Information and Space*. 2019;2:41-48 (in Russ.)
11. Anufrenko A., Kanaev A., Login E. Model of the Attacker's Influence on a Fragment of a Transport Communication Network Based on the Carrier Ethernet Technology. *Proc. of Telecom. Universities.* 2018;4(3):17–25. DOI:10.31854/1813-324X-2018-4-3-17-25
12. Kanaev A., Marchenko D., Subbotin D. Model of Functioning of the Transport Networks for Special Purposes, Taking into Account the High Dynamics of the Network Conditions Due to External Influences. *Proceedings of the VIIth International Conference on Infotelecommunications in Science and Education, 28 February–1 March 2018, St. Petersburg, Russian Federation.* St. Petersburg: Saint-Petersburg State University of Telecommunications Publ.; 2018. p. 304–308. (in Russ.)
13. Boev V.D., Kirik D.I., Sypchenko R.P. *Computer Modeling: A Guide for Course and Graduate Design*. St. Petersburg.: Telecommunications Military Academy Publ.; 2011. 348 p. (in Russ.)
14. Prysyazhniuk A.S., Sakharova M.A., Belyaev D.O., Ilyushko D.V., Bocharov P.M., Ovchinnikov G.R. *The Software Package for Monitoring and Monitoring the Radio Network*. Computer Registration Certificate, no 2019617338, 27.05.2019. (in Russ.)
15. Prysyazhniuk A.S., Sakharova M.A., Login E.V. *The Program of Simulation of the Processes of Functioning and Control of the Radio Communication Network*. Computer Registration Certificate, no. 2019613923, 12.03.2019 (in Russ.)

Сведения об авторах:

БЕЛЯЕВ Денис Олегович — ведущий программист ЗАО «Институт телекоммуникаций», dobelyaev@gmail.com

КАНАЕВ Андрей Константинович — доктор технических наук, профессор, заведующий кафедрой «Электрическая связь» Санкт-Петербургского государственного университета путей сообщения Императора Александра I, kanaev@pgups.ru
https://orcid.org/0000-0002-1578-2629

ПРИСЯЖНЮК Сергей Прокофьевич — доктор технических наук, профессор, генеральный директор ЗАО «Институт телекоммуникаций», руководитель образовательных программ «Геоинформационные системы» и «Программно-защищенные инфокоммуникации» Национального исследовательского университета ИТМО, office@itain.ru

САХАРОВА Мария Александровна — кандидат технических наук, доцент кафедры «Электрическая связь» Санкт-Петербургского государственного университета путей сообщения Императора Александра I, zuvakamariya@mail.ru

СОРОКИН Роман Павлович — аспирант кафедры «Электрическая связь» Санкт-Петербургского государственного университета путей сообщения Императора Александра I, 123roman456@mail.ru