DOI: 10.55648/1998-6920-2024-18-4-62-76 УДК 519.23:005.334:004.896

Интегрированная с API байесовская модель управления рисками на базовых станциях сети сотовой связи

К. Э. Григорьев[1], В. С. Канев[2], А. Н. Полетайкин[1,2]

[1] Кубанский государственный университет (КубГУ)
[2] Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ)

Аннотация: В статье рассмотрен новый подход к управлению рисками возникновения нештатных ситуаций на базовых станциях сети сотовой связи. Многообразие нештатных ситуаций, возникающих на гетерогенном оборудовании под влиянием множества разнообразных внешних факторов делают задачу управления рисками критически важной. Новизна заключается в создании математической модели, учитывающей указанное многообразие. Это обеспечивает более точное и комплексное предсказание нештатных ситуаций. Модель построена на базе байесовской сети и генерирует оперативное решение в виде вероятностей возникновения нештатных ситуаций, показывает критические точки и потенциальные угрозы для работоспособности базовой станции в целом. Это помогает формировать рекомендации по снижению рисков нештатных ситуаций, определять приоритетные направления для внедрения улучшений и модернизации оборудования.

Для обеспечения эффективного взаимодействия с моделью осуществляется разработка и исследование API с использованием FastAPI и языка Python. API взаимодействует с байесовской моделью, созданной в BayesFusion GeNIe. Модель реализует новый способ интеграции созданной байесовской сети с существующими приложениями на принципах REST API. Тем самым реализуется новый подход к управлению рисками. Описаны процессы создания API, тестирования его производительности и развертывание. В результате применения API достигается возможность оперативного управления рисками, что помогает операторам предотвращать аварийные ситуации.

Интегрированная модель построена в исследовательских целях для мониторинга рискового фона базовых станциях сети сотовой связи. Применение этой модели позволяет значительно повысить уровень автоматизации процесса управления рисками в ходе эксплуатации базовых станций сети сотовой связи.

Работа выполнена в рамках государственного задания 071-03-2024-001 от 19.01.2024.

Ключевые слова: байесовская сеть, API, оценка рисков, нештатные ситуации, сотовая связь, базовые станции, BayesFusion GeNIe, управление рисками, прогнозирование аварий, FastAPI, тестирование API, автоматизация.

Для цитирования: Григорьев К. Э., Канев В С., Полетайкин А. Н. Интегрированная с API байесовская модель управления рисками на базовых станциях сотовой связи // Вестник СибГУТИ. 2024. Т. 18, № 4. С. 62–76. https://doi.org/10.55648/1998-6920-2024-18-4-62-76.

Статья поступила в редакцию 01.10.2024;
переработанный вариант – 05.11.2024;
принята к публикации 06.11.2024.

1. Введение

Управление нештатными ситуациями на базовых станциях сотовой связи играет важную роль в обеспечении стабильности телекоммуникационных сетей. Базовые станции – ключевые элементы инфраструктуры, и любые сбои в их работе могут приводить к значительным последствиям. В современных условиях, когда частота сбоев возрастает, критически важно иметь инструменты для оперативного и точного прогнозирования рисков и их предотвращения.

Одним из эффективных подходов к оцениванию рисков в телекоммуникациях является использование байесовских сетей, которые позволяют моделировать вероятности нештатных ситуаций на основе множества факторов [1]. Байесовские модели обладают гибкостью, что делает их идеальными для таких задач, как управление аварийными ситуациями на базовых станциях. Существующие математические и программные решения, реализующие такие модели, требуют интеграции с существующими на объекте программными системами. Таким решением может быть разработка специализированного API [2].

API (Application Programming Interface) – это интерфейс, предоставляющий набор методов для взаимодействия между различными программными системами. Взаимодействие через API обеспечивает стандартизированный обмен данными и функциями, что играет важную роль в разработке современных приложений и сервисов, построенных на микросервисной архитектуре [3]. API поддерживает модульность и инкапсуляцию программного обеспечения, что улучшает гибкость систем. Развивается API-First подход, в котором главная роль при разработке приложения отводится API [4]. REST, SOAP являются основными архитектурными стилями для построения API. Кроме того, популярны API на основании GraphQL и gRPC. Чаще всего используется REST (Representational State Transfer) благодаря своей простоте и соответствию современным принципам веб-инфраструктуры [5, 6]. Этот подход основан на стандартных HTTP-методах (GET, POST, PUT, DELETE), что делает его понятным и доступным для разработчиков. REST API легко масштабировать и интегрировать с другими веб-сервисами, что особенно важно в условиях современного многоуровневого программного обеспечения.

Цель работы – разработка мероприятий по повышению рисковой устойчивости функционирования базовых станций сотовой связи за счет создания и применения нового научно обоснованного инструмента на основе современных математических и программных средств, предоставляющего операторам связи возможность не только предсказывать аварии, но и принимать превентивные меры для минимизации сбоев.

2. Методы оценивания рисков в телекоммуникациях

Управление рисками представляет собой комплексный процесс, направленный на выявление, оценку и минимизацию рисков, связанных с деятельностью организации. Современные подходы к управлению рисками включают разнообразные методы, основанные на научных исследованиях и практическом опыте. В основном методы управления рисками делятся на качественные и количественные. Однако с исследовательской точки зрения представляет интерес интегративный вариант. Это позволяет получить более комплексное понимание рисков и разработать эффективные стратегии их управления. Среди таких методов следует выделить FMEA (Failure Modes and Effects Analysis) – метод анализа видов и последствий отказов технических средств [7]. Расширение традиционного анализа FMEA – FMECA – добавляет оценку критичности отказов. Этот метод позволяет систематически идентифицировать возможные режимы отказа, оценивать их последствия и определять меры по снижению риска. Метод нашел широкое применение в телекоммуникационных системах и многократно исследован [7–10]. Будучи интегративным, он имеет реализации в комплексе с оптимизационным моделированием [8] и машинным обучением [9, 10].

Еще одним интегративным методом является нечеткий метод Дельфи (FDM) [11]. FDM сочетает в себе метод Дельфи с нечеткой логикой. Это позволяет учесть и эффективно обработать неопределенность и неточность, присущие экспертным мнениям. Этот метод особенно полезен для оценивания рисков, которые трудно измерить количественно, таких как стратегические и операционные риски [12]. Метод применяется в том числе и в телекоммуникациях [13], подобно FMECA, оценивая критичность нештатных ситуаций.

Востребованным и мощным инструментом для анализа рисков являются Байесовские сети. Они позволяют моделировать вероятностные зависимости между различными событиями [14]. Этот метод нашел применение также и в сочетании с анализом видов и последствий отказов (FMEA) для управления рисками неисправностей в телекоммуникационных системах [10]. Комплексное применение байесовских сетей в задаче анализа рисков ИТ-проектов выполнено в исследовании [15] в сочетании с методами проектного менеджмента и имитационным моделированием. Также применение байесовских сетей для анализа рисков показало высокую эффективность в многомерном факторном пространстве. Соответствующее исследование анализа рисков медицинской эвакуации опубликовано автором в [16].

Также среди интегративных методов выделяется Interpretive Structural Modeling (ISM). ISM помогает в понимании сложных взаимоотношений между различными элементами анализируемого процесса и структурировании этих отношений для принятия управленческих решений. В телекоммуникациях ISM используется для анализа иерархических зависимостей между факторами риска. Может быть использован как самостоятельно [17], так и в комплексе с другими методами, например, с методом FDM [18] для оценивания рисков в телекоммуникационных системах.

Рассмотренные интегративные методы имеют свои сильные стороны и специфические области применения в анализе и управлении рисками. FMECA является традиционным методом, который систематически идентифицирует возможные режимы отказа и оценивает их последствия, но часто не справляется с неопределенностью и сложности взаимодействий между рисками. FDM добавляет к этому процессу нечеткую логику, что позволяет эффективнее обрабатывать неопределенности экспертных суждений, но он по-прежнему требует значительных усилий по сбору и согласованию мнений экспертов. С другой стороны ISM, поддерживает структурирование сложных взаимоотношений иерархических зависимостей между факторами риска, но может быть ограничен в количественной оценке вероятностей и последствий [21].

Байесовские сети выделяются на фоне этих методов благодаря способности прогнозирования широкого спектра рисковых событий и моделирования вероятностных зависимостей между событиями. Они позволяют не только выявлять и оценивать риски, но и понимать их взаимосвязи, что особенно полезно в сложных системах, таких как телекоммуникационные. Это дает возможность более точно прогнозировать последствия различных сценариев и принимать обоснованные решения по снижению рисков. Также они дают понятное объяснение своих выводов, допускают логическую интерпретацию и модификацию структуры отношений между переменными задачи, а также позволяют в явной форме учесть априорный опыт экспертов [1]. Методологическая широта применения байесовских сетей, как то:

- прогнозирование, или прямой вывод (определение вероятности события при наблюдаемых причинах);
- диагностирование, или обратный вывод (определение вероятности причины при наблюдаемых следствиях);
- межпричинный (смешанный) вывод (определение вероятности одной из причин наступившего события при условии наступления одной или нескольких других причин этого события);
- позволяет получить ответы на самые разные типы вероятностных запросов [16].

3. Байесовская модель

Модель строится на основе аварийных сообщений, которые генерируются блоком вывода аварий базовой станции WCDMA Nokia. Всего было идентифицировано 120 различных неисправностей, фиксируемых станциями WCDMA Nokia MetroSite. В данном исследовании используется упрощённая модель, которая учитывает 26 наиболее частых аварийных сообщений, а также данные, получаемые системой мониторинга базовой станции. Среди них – температура окружающей среды, нагрузка на трафик и уровень заряда аккумуляторов. Эти показатели совместно предоставляют информацию о текущем состоянии и работоспособности станции. В табл. 1 представлены основные переменные из системы мониторинга, включая внутреннюю температуру станции, заряд батареи WIB (Wireless Interface Battery) и объём трафика.

Таблица 1. Переменные для данных, поступающих из системы мониторинга

Переменная	Идентификатор	Состояние	Показания СМ
Температура кабинета	ambient_temperature	lessm10	[-50, -10]
		fm10t0	[-10, 0]
		f0t10	[0, 10]
		f10t20	[10, 20]
		f20t30	[20, 30]
		f30t50	[30, 50]
		more50	[50, 100]
Заряд блока WIB	battery_charge	f0t25	[0, 25],
		f25t50	[25, 50]
		f50t75	[50, 75]
		f75t100	[75, 100]
Запас по трафику	traffic_capacity	less5	[0, 5]
		f5t10	[5, 10]
		more10	[10, 100]

В табл. 2 приведены переменные, отражающие данные, которые создаются в результате работы блока вывода аварий. Эти переменные бинарные и показывают, присутствует ли определенное аварийное сообщение в системе. Рассматриваемые сбои связаны с ключевыми компонентами базовой станции (BTS), включая следующие элементы: фильтр антенны (WAF), блок внешних аварийных сигналов (WEA), батарея интерфейса (WIB), блок системных часов (WSC), асинхронный блок передачи данных (ATM), блок перекрестного соединения ATM (AXU).

Байесовская сеть состоит из набора узлов (переменных) и взаимосвязей между ними, основанных на вероятностных зависимостях. В данной модели связи между узлами указывают на причинно-следственные отношения, а вероятности этих связей вычислялись на основе данных, полученных в ходе эксперимента с реальными базовыми станциями. Модель анализирует данные о текущем состоянии оборудования и рассчитывает вероятности различных неисправностей. Это позволяет операторам принять необходимые меры заранее, снижая риск простоев и повышая надежность работы сети. Передадим модели следующие параметры базовой станции: температура кабинета: 28,8 ˚C; заряд блока WIB: 72 %; запас по трафику сети: 3,6 %; аварийные сообщения, поступающие с базовой станции: BURGLAR_ON, SMOKE_ALARM, FIRE_ALARM, WIB_TEMP_HIGH. Для построения модели использовалось программное обеспечение BayesFusion GeNIe [19]. На рис. 1 представлена визуализация этой сети.

Таблица 2. Переменные для данных, генерируемых блоком вывода внешних аварий

№	Переменная	Идентификатор
1	Несанкционированный доступ	Burglar
2	Пожар на объекте	fire_on_site
3	Отключение электросети	ELECTRICAL_GRID_OFF
4	Отказ WEA	WEA_FAIL
5	Санкционированный доступ	worker
6	Сбой датчика взлома	burglar_sensor_malf
7	Срабатывание датчика взлома	BURGLAR_ON
8	Отказ кондиционирования	CONDITIONING_FAIL
9	Перегрузка трафика ATM	ATM_TRAFFIC_OVERLOAD
10	Высокая температура устройства	UNIT_TEMP_HIGH
11	Низкая температура устройства	UNIT_TEMP_LOW
12	Высокая температура WIB	WIB_TEMP_HIGH
13	Отказ WIB	WIB_BATTERY_FAIL
14	Неисправность WAF	WAF_FAULTY
15	Неисправность низкочастотного усилителя WAF	WAF_LOW_NOISE_AMPLIFIER_FAULTY
16	Отключение ячейки	CELL_OFF
17	Разница фаз WSC	WSC_PHASE_DIFFERENCE_JAMMED
18	Неисправность процессора ATM	ATM_PROCESSOR_FAULTY
19	Трафик в несуществующем подключении ATM	TRAFFIC_FLOW_IN_NON_EXISTENT_ATM_CONNECTION
20	Деградация работы BTS	BTS_OPERATION_DEGRADED
21	Отключение BTS	BTS_OFF
22	Сбой датчика пожара	fire_sensor_malf
23	Пожарная тревога	FIRE_ALARM
24	Отказ нагревателя	HEATER_FAIL
25	Сбой датчика дыма	smoke_sensor_malf
26	Дымовая тревога	SMOKE_ALARM

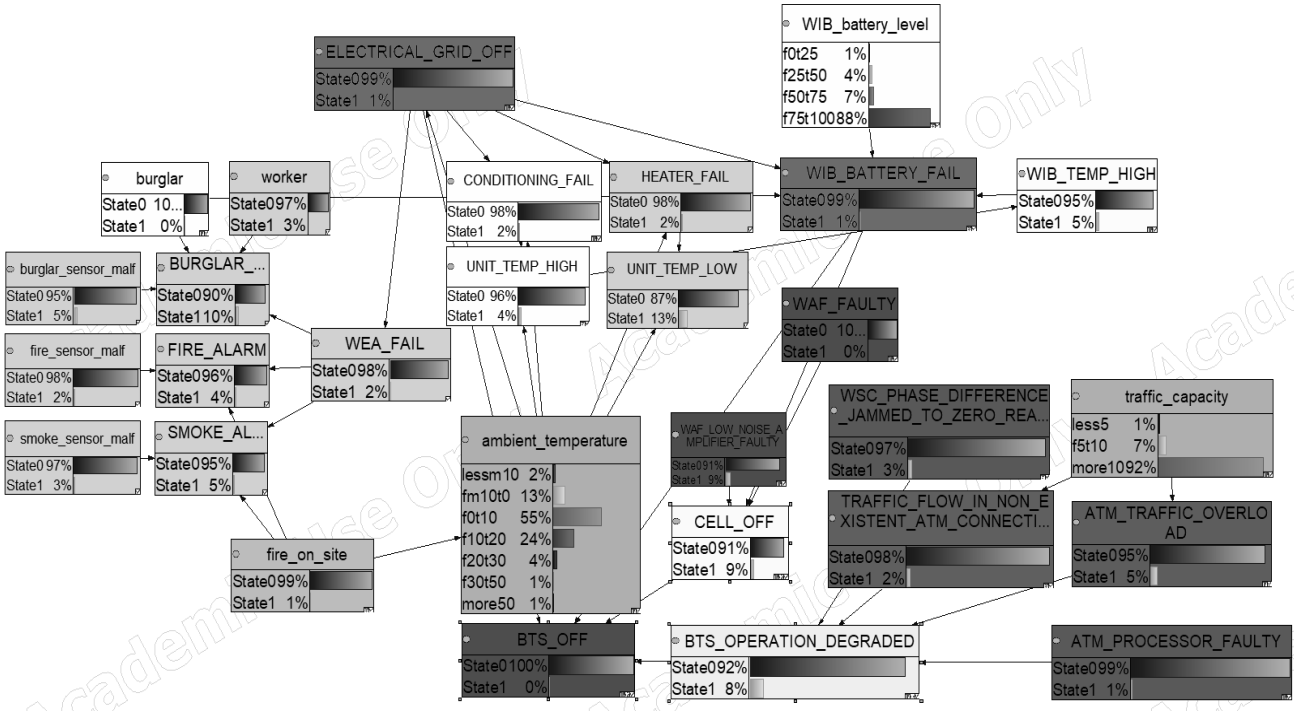

Рис. 1. Созданная байесовская сеть в интерфейсе GeNIe: узлы сети, связи между ними, априорные вероятности (критические узлы выделены тёмно-серым цветом)

В результате модель рассчитывает вероятности рисковых событий (в табл. 3 показаны рисковые события, вероятность которых выше 0,01). Стоит заметить, что в процессе поступления текущих данных о нештатных ситуациях априорные вероятности будут уточняться.

Таблица 3. Результаты имитационного моделирования в среде GeNIe (фрагмент)

Аварийный узел (идентификатор согласно табл. 2)	Вероятность
WAM_FAIL	0.985
UNIT_TEMP_HIGH	0.664
BTS_OPERATION_DEGRADED	0.433
ATM_TRAFFIC_OVERLOAD	0.340
TRAFFIC_FLOW_IN_NON_EXISTENT_ATM	0.133
CONDITIONING_FAIL	0.079
burglar_sensor_maf	0.077
worker	0.057
fire_sensor_malf	0.054
smoke_sensor_malf	0.054
HEATER_FAIL	0.049
ELECTRICAL_GRID_OFF	0.045
WIB_BATTERY_FAIL	0.037
CELL_OFF	0.030
BTS_OFF	0.028
fire_on_site	0.016
burglar	0.012

Созданная модель также позволяет провести анализ чувствительности байесовской сети, позволяя выявить критические точки в системе. Анализ чувствительности выполнен средствами BayesFusion GeNIe по методике Gaag и Kjaerulff [20]. Анализ проводится путем исследования влияния небольших изменений числовых параметров модели (априорных и условных вероятностей) на выходные параметры (апостериорные вероятности). Рассчитывают максимальную и среднюю чувствительность.

Максимальная чувствительность показывает, насколько сильно результат модели может измениться при изменении одного из её параметров на небольшую величину. Это значение используется для определения наиболее влиятельных параметров модели. Если изменение параметра приводит к значительному изменению вероятности или исхода, то параметр имеет высокую максимальную чувствительность.

Средняя чувствительность показывает среднее изменение результата модели по всем параметрам при их небольшом изменении. Это усреднённый показатель того, насколько сильно результаты модели зависят от её параметров. Средняя чувствительность используется для общей оценки устойчивости модели. Если средняя чувствительность низкая, это указывает на то, что модель в целом устойчива к изменениям её параметров.

Результаты анализа чувствительности показаны в табл. 4 и на рис. 1. Серым цветом выделены узлы с полным отсутствием влияния на целевой узел (BTS_OFF). Белый цвет характеризует узлы с низкой чувствительностью. Светло-серый цвет обозначает среднюю чувствительность. Критические узлы выделены тёмно-серым. К таким узлам в построенной модели относятся узлы электроснабжения: ELECTRICAL_GRID_FAIL, WIB_BATTERY_FAIL, а также узлы, отражающие аппаратные неисправности: ATM_PROCESSOR_FAULTY, WAF_FAULT, WSC_PHASE_DIFFERENCE_JAMMED_TO_ZERO_READING. Это позволяет определить приоритетные направления для улучшений и модернизации комплекса технических средств базовой станции.

Таблица 4. Результаты анализа чувствительности модели

Аварийный узел (идентификатор согласно табл. 2)	Чувствительность	
	Максимальная	Средняя
WAF_LOW_NOISE_AMPLIFIER_FAULTY	0.961	0.506
WAF_FAULTY	0.918	0.215
WSC_PHASE_DIFFERENCE_JAMMED_TO_ZERO_READING	0.687	0.334
ATM_PROCESSOR_FAULTY	0.674	0.338
ATM_TRAFFIC_OVERLOAD	0.652	0.118
TRAFFIC_FLOW_IN_NON_EXISTENT_ATM_CONNECTION	0.635	0.144
ELECTRICAL_GRID_OFF	0.521	0.279
WIB_BATTERY_FAIL	0.504	0.126

4. Рекомендации по снижению рисков

На основе результатов исследования предложены следующие меры по минимизации выявленных рисков:

1. Плановое техническое обслуживание оборудования. Регулярное техническое обслуживание снижает вероятность выхода из строя аппаратных компонентов, что подтверждается анализом критических узлов байесовской сети, таких как ATM_PROCESSOR_FAULTY, WAF_FAULTY, WSC_PHASE_DIFFERENCE_JAMMED_TO_ZERO_READING. Поддержание в исправном состоянии оборудования предотвращает непредвиденные сбои и продлевает срок службы компонентов, снижая риски потерь данных и ухудшения качества услуг.
2. Усиление системы электроснабжения. Анализ чувствительности выявил узлы ELECTRICAL_GRID_OFF, WIB_BATTERY_FAIL как критические. Усиление системы электроснабжения, включая добавление резервных источников питания и проведение плановых проверок текущих систем, обеспечивает устойчивость к перебоям в электроснабжении. Это снижает риск сбоев, вызванных недостаточной надежностью энергоснабжения, и поддерживает стабильность работы базовых станций.
3. Внедрение дополнительных систем мониторинга. Дополнительные системы мониторинга помогают своевременно выявлять и устранять потенциальные проблемы, что критично для узлов TRAFFIC_FLOW_IN_NON_EXISTENT_ATM_CONNECTION, WIB_BATTERY_FAIL и WIB_TEMP_HIGH. Эти системы обеспечивают оперативное реагирование на проблемы и предотвращают их эскалацию, что способствует поддержанию общего качества предоставляемых услуг и повышению надежности системы.

5. Разработка API

5.1. Архитектурное проектирование

API предназначен для получения прогнозов на основе существующей байесовской сети и данных из хранилища. Основная задача API – предоставлять пользователям доступ к предсказаниям вероятных аварий и извлечение необходимых данных мониторинга без изменения структуры или параметров сети. API принимает данные мониторинга (например, температура, заряд батареи, трафик) и возвращает прогноз вероятных аварий, полученный на основе байесовской сети (см. раздел 3). Байесовская сеть уже построена и настроена, поэтому пользователи могут только передавать входные данные для прогнозирования, но не могут изменять структуру сети.

Также посредством API пользователи смогут запрашивать ретроспективные данные мониторинга, аварийные сообщения, а также предсказания, сохранённые в базе данных. Это полезно для анализа трендов и проверки корректности сделанных ранее прогнозов.

Для данного проекта выбрана архитектура REST API благодаря ее простоте интеграции, широкому использованию и поддержке в различных системах. REST (Representational State Transfer) позволяет четко разделять ресурсы, используя стандартные HTTP-методы, что упрощает взаимодействие между клиентом и сервером. Эта архитектура легко масштабируется и поддерживает кэширование, что повышает производительность. Кроме того, RESTful сервисы легко документируются, что делает их понятными для разработчиков и упрощает интеграцию с различными клиентами и платформами.

Модель данных функционирования API показана на рис. 2 и включает 4 реляционных отношения: requests – запросы на получения предсказаний, responses-prediction_logs – предсказания, accident – справочник нештатных ситуаций.

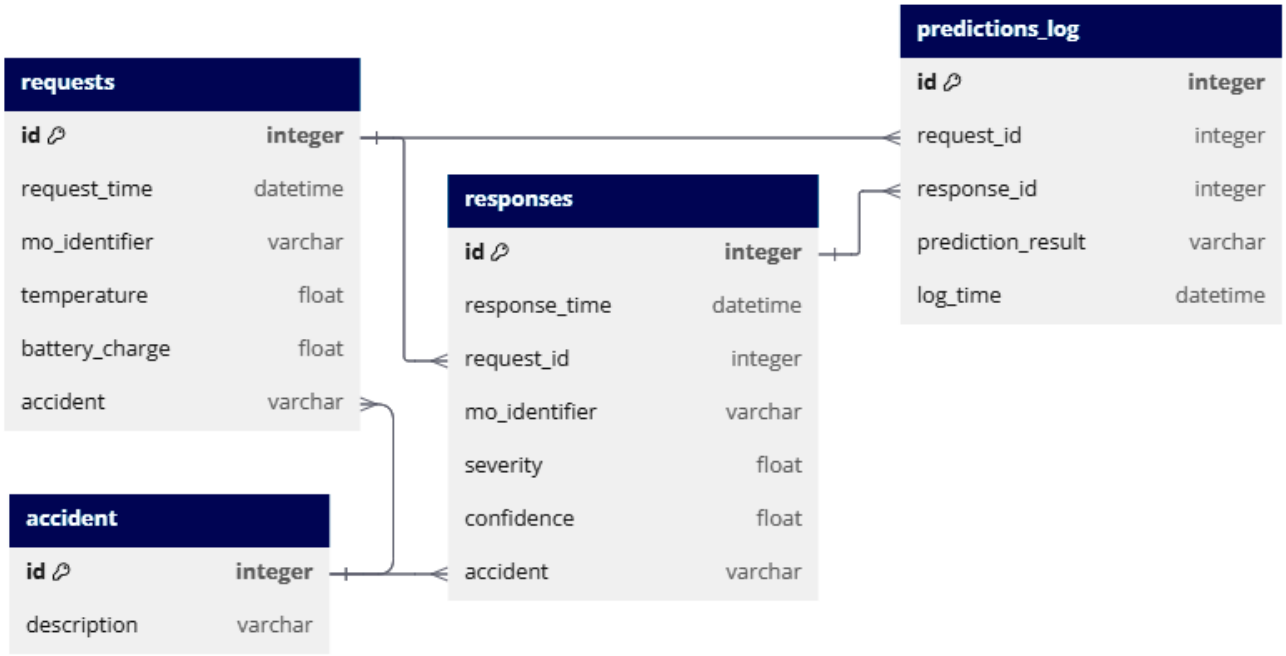

Рис. 2. Модель данных для работы API

Работа с API требует аутентификации текущего пользователя и принимает объект MultiplePredictionRequest (список запросов типа List[request], где request – структура входных данных запроса на предсказание, см. рис. 2) в POST-запросе. Каждый запрос обрабатывается следующим образом:

1.Для каждого запроса данные подготавливаются и вставляются в таблицу requests в базе данных, используя параметризованный SQL-запрос.

2.После успешной вставки данных выполняется прогнозирование с помощью функции `bayesian_predict` для каждого запроса. Полученные предсказания сохраняются в таблицу responses.

3.В ответе на запрос отправляется объект, содержащий результаты предсказаний для каждого запроса, включая параметры предсказания, такие как степень риска и уверенность (в таблице responses поля severity и confidence соответственно).

Во всех маршрутах приложения используется логирование ключевых моментов выполнения запроса, таких как получение параметров запроса, выполнение SQL-запроса и обработка результатов. В случае возникновения ошибки, возвращается HTTP-ответ с кодом ошибки 500, содержащий детали ошибки.

5.2. Развертывание

Развертывание приложения в качестве сервера с использованием Uvicorn обеспечивает высокую производительность и асинхронную обработку запросов. Uvicorn – это легковесный сервер ASGI, который идеально подходит для работы с фреймворком

FastAPI. Он позволяет обрабатывать множество соединений одновременно, что особенно важно для приложений с высокой нагрузкой.

Для запуска приложения достаточно выполнить команду `uvicorn main:app --host 0.0.0.0 --port 8000`. Здесь `main` – имя файла, содержащего приложение, а `app` – экземпляр FastAPI. Такой подход позволяет легко масштабировать приложение и поддерживать высокую нагрузку благодаря эффективному управлению асинхронными задачами.

Uvicorn также поддерживает горячую перезагрузку, что упрощает процесс разработки и тестирования. Это значит, что изменения в коде будут автоматически подхватываться без необходимости перезапускать сервер, что делает Uvicorn отличным выбором для разработки и развертывания высокопроизводительных API.

5.3. Тестирование

Основное внимание было уделено нагрузочному тестированию, которое помогает оценить производительность и устойчивость API под высокой нагрузкой. В качестве инструмента для тестирования использован фреймворк Locust, который позволяет моделировать поведение пользователей и автоматизировать процесс тестирования.

Тест, написанный с использованием Locust, моделирует поведение пользователя, который отправляет запросы на предсказание нештатных ситуаций на базовых станциях. Скрипт выполняет генерацию случайных данных для запросов, включающих идентификаторы базовых станций, температуру, уровень заряда батареи и список инцидентов и отправку POST-запросов к конечной точке /predict с использованием сгенерированных данных.

Производительность API была определена на основе пропускной способности, измеренной в количестве запросов, обработанных за определенный промежуток времени. Результаты тестирования показаны на рис. 3.

На рис. 3 представлены следующие графики, отражающие параметры проведенного нагрузочного тестирования:

1. Total Requests per Second – показывает стабильную пропускную способность на уровне около 500 запросов в секунду (RPS). Это свидетельствует о том, что API способен обрабатывать высокий объем запросов с постоянной скоростью на протяжении всего тестирования.

2. Response Times – демонстрирует время ответа API на запросы. Среднее время ответа (нижняя линия) стабильно держится около 200 мс на протяжении всего тестирования. В то же время, 95-й перцентиль (верхняя линия) показывает, что для 95% запросов время ответа не превышает примерно 250-300 мс. Наблюдается незначительное колебание времени ответа, что может указывать на временны́е всплески нагрузки или другие факторы, влияющие на производительность.

3. Number of Users – показывает, что количество пользователей оставалось постоянным на уровне около 100 на протяжении всего тестирования. Это позволяет оценить устойчивость системы при увеличении нагрузки. API показал высокую устойчивость, сохраняя стабильную производительность и время ответа при увеличенной нагрузке. Не наблюдается значительных изменений в пропускной способности или времени ответа, что свидетельствует о хорошей устойчивости системы.

Параметры Total Requests per Second и Response Times показывают, что количество ошибок (Failures/s) практически отсутствует или составляет незначительную величину (нижняя линия на графике Total Requests per Second). Это указывает на высокую надежность API при проведенном тестировании.

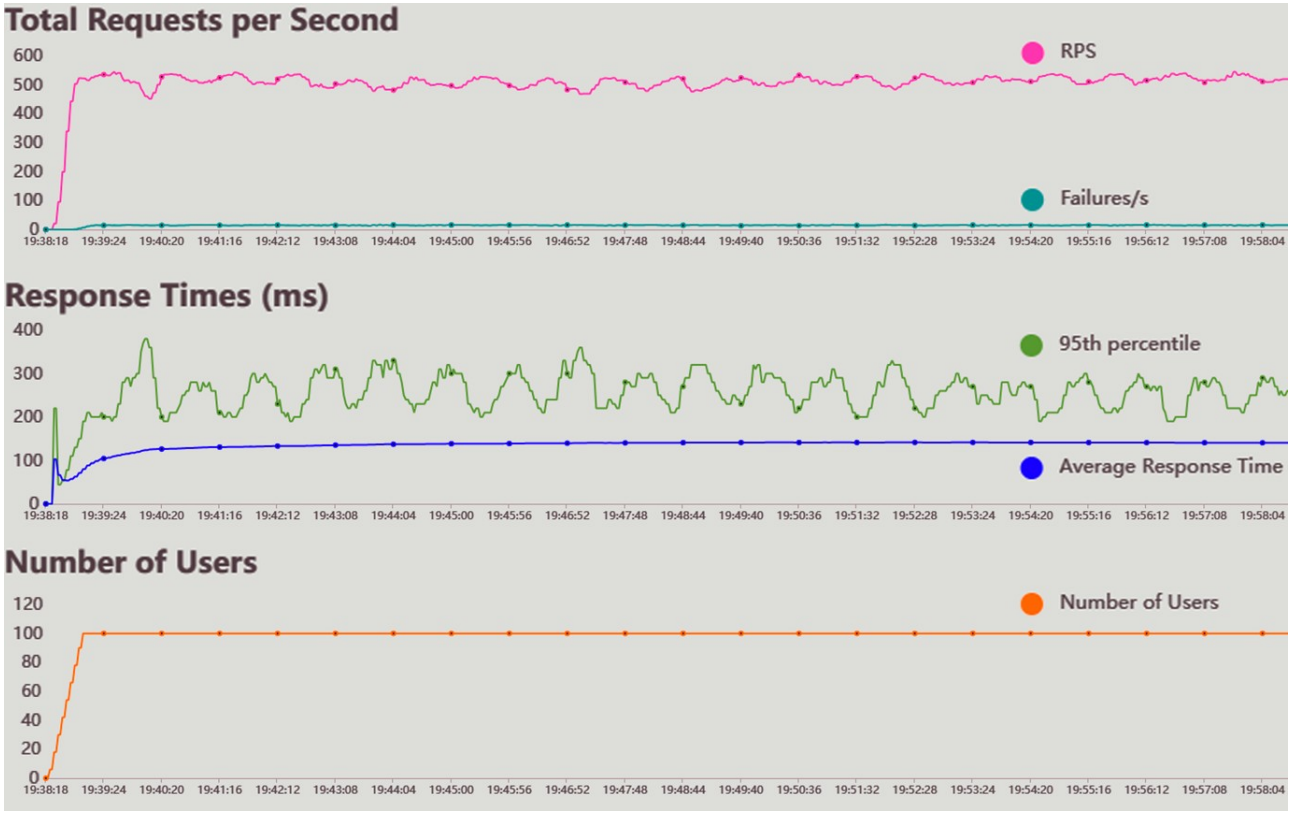

Рис. 3. Результаты нагрузочного тестирования API

6. Заключение

Принципиальное отличие байесовских сетей от других ориентированных структур при анализе рисков состоит в открывающейся возможности соизмерять априорные и апостериорные вероятности критических событий, событий ответственных за фатальное течение обстоятельств в данной рисковой ситуации. Содержательно это означает с точки зрения аналитики управления рисками:

а) накопление ретроспективной информации о рисковом объекте;

б) количественное отслеживание оперативной информации о рисковом объекте;

в) соизмерение ретроспективной и оперативной информации и выработка продуктивных управляющих воздействий.

Таким образом реализуется байесовский принцип управления в телекоммуникационной сети на уровне собственников бизнес-процессов. Анализ на ориентированной сети повышает общую адекватность модельного представления связных рисковых событий.

Применение инструмента байесовских сетей для решения задачи расчета рисков возникновения нештатных ситуаций на оборудовании базовых станций показало свою эффективность. Созданная модель позволяет не только рассчитывать вероятность нештатных ситуаций на оборудовании базовых станций, но и определять критические точки в описываемой системе. На основе результатов моделирования формируются рекомендации по минимизации рисков возникновения нештатных ситуаций. Эти рекомендации направлены на повышение стабильности и надежности базовых станций сотовой связи, а также на улучшение общего качества предоставляемых услуг.

Для эффективного взаимодействия с моделью разработан API, результаты тестирования которого показали его высокую пропускную способность на уровне около 500 запросов в секунду, среднее время ответа составляло около 200 мс, а система в целом показала высокую устойчивость при увеличенной нагрузке. Количество ошибок оказалось минимальным, что свидетельствует о высокой надежности API. Разработанный API способен

эффективно обрабатывать высокий объем запросов с минимальным временем ответа, что делает его пригодным для использования в реальных условиях эксплуатации.

Отлаженная модель может быть реализована как подсистема компьютеризированной системы риск-менеджмента на базовых станциях сети сотовой связи. Благодаря такой системе оператор сотовой связи может применить адекватные превентивные меры для предотвращения сбоев и аварий на объекте.

Дальнейшие исследования планируется продолжить в направлении усовершенствования модели за счет добавления новых узлов и взаимосвязей между ними для уточнения результатов моделирования, а также расширения возможностей байесовского вывода. Для усовершенствования модели также необходимо произвести сбор дополнительных данных, уточняющих априорные и условные вероятности узлов байесовской сети.

Литература

1. *Бунцев И. А., Канев В. С.* Системное управление рисками в телекоммуникациях (состояние проблемы, методы, модели, реализации). Вестник СибГУТИ. 2009. С. 26-52.
2. *Diedrich, A., Deutschmann, P. and Junker, C.* ServiceNavigator - a bayesian assistance system for diagnosing industrial production systems. In 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS) (pp. 1-6).
3. *Bogner, Justus & Fritzsch, Jonas & Wagner, Stefan & Zimmermann, Alfred.* (2019). Microservices in Industry: Insights into Technologies, Characteristics, and Software Quality. DOI: 10.1109/ICSA-C.2019.00041.
4. *Beaulieu, Nicole & Dascalu, Sergiu & Hand, Emily.* (2022). API-First Design: A Survey of the State of Academia and Industry. 10.1007/978-3-030-97652-1_10.
5. *Резединова Е. Ю., Кыркунов П. Н., Сергеев А. В.* Выбор сервис-ориентированной архитектуры для создания сервиса по благоустройству города // SAEC. 2023. №3.
6. *Галигузова Е. В., Илларионова Ю. Е.* Язык запросов GraphQL как замена REST API. сравнение GraphQL и REST API // Символ науки. 2023. № 1-2.
7. *Zhang, H., Wang, Z. R., Wang, X. W., Lin, F. C.* (2023). Practice and Research on FMEA of Telecommunication Satellite System. In: Sun, J., Wang, Y., Huo, M., Xu, L. (eds) Signal and Information Processing, Networking and Computers. Lecture Notes in Electrical Engineering, vol 917. Springer, Singapore. https://doi.org/10.1007/978-981-19-3387-5_110.
8. *Alijanzadeh, M. R., Shayannia, S. A. & Movahedi, M. M.* (2024). Optimization of maintenance in supply chain process and risk-based critical failure situations (case study: Iranian oil pipeline and telecommunication company, north district). Journal of applied research on industrial engineering , 11(1), pp. 125-142.
9. *Carretero-Ayuso, M. J.; Sánchez-Barroso, G.; González-Domínguez, J.; García-Sanz-Calcedo, J.* Failure Modes in Electricity and Telecommunication Facilities in Dwellings in Spain. Appl. Sci. 2021, 11, 5274. https://doi.org/10.3390/app11115274
10. *Tarcsay B. L., Bárkányi Á, Németh S, Chován T, Lovas L, Egedy A.* Risk-Based Fault Detection Using Bayesian Networks Based on Failure Mode and Effect Analysis. Sensors. 2024; 24(11):3511.
11. *Nalluri, V & Chen, L.* (2022). Risk assessment for sustainability on telecom supply chain: A hybrid fuzzy approach. Uncertain Supply Chain Management, 10(2), pp. 559-576.
12. *Цыганов В. В., Гурлев И. В.* Когнитивное прогнозирование информационно-телекоммуникационной инфраструктуры крупномасштабного региона // ИТНОУ: информационные технологии в науке, образовании и управлении. 2020. №1 (15). С. 3-7.
13. *Mishra, Arnuv & Kumar, Deepak & Shuaib, Mohd & Tyagi, Mohit & Singh, Ravi.* (2021). Measurement of Critical Factors: A Case of Telecommunication Industry. 10.1007/978-981-15-6017-0_16.

14. *Bayas B, Zambrano C.* (2021). Redes bayesianas aplicadas a la predicción de errores en las redes definidas por software. 13. pp. 419-429.
15. *Думбрайс К. О., Глущенко О. М.* Моделирование и анализ рисков ИТ-проектов // Наука и образование сегодня. 2021. №2 (61). pp. 26–33.
16. *Демчук Д. А., Демчук К. А., Шевцова Ю. В., Полетайкин А. Н.* Байесовский подход при численном расчете риска медицинской эвакуации автотранспортом. Вестник СибГУТИ. 2023;17(1):18-32. https://doi.org/10.55648/1998-6920-2023-17-1-18-32.
17. *Adib, D., Safarzadeh, H., Mohammadi, M.* (2023). 'Designing and explaining the IoT commercialization model in Iranian organizations (Telecommunication Company of Iran): An interpretive structural modeling (ISM) approach', International Journal f Nonlinear Analysis and Applications, 14(1), pp. 723-738. doi: 10.22075/ijnaa.2022.26942.3456.
18. *Chen, W.-K.; Nalluri, V.; Ma, S.; Lin, M.-M.; Lin, C.-T.* An Exploration of the Critical Risk Factors in Sustainable Telecom Services: An Analysis of Indian Telecom Industries. Sustainability 2021, 13, 445. https://doi.org/10.3390/su13020445.
19. GeNIe Modeler. User's Manual: [Электронный ресурс] // BayesFusion, LLC. 2024 – URL: https://support.bayesfusion.com/docs/GeNIe.pdf (Avaiable at: 12.08.2024).
20. *Gaag, Linda C. & Kjaerulff, Uffe.* Making Sensitivity Analysis Computationally Efficient // Proceedings of the 16th Conference on Uncertainty in Artificial Intelligence. 2000. pp. 317 – 325.

Григорьев Константин Эрнстович

магистрант по направлению подготовки «Прикладная математика и информатика», Кубанский государственный университет (350040, г. Краснодар, ул. Ставропольская, 149), e-mail: k.e.grigorev@gmail.com, ORCID ID: 0009-0004-5518-6989.

Канев Валерий Семенович

доктор технических наук, профессор, зав. кафедрой математического моделирования и цифрового развития бизнес-систем (ММиЦРБС) СибГУТИ (630102, г. Новосибирск, ул. Кирова, д. 86), тел. (383) 269-82-77, e-mail: kanev@sibguti.ru, ORCID ID: 0009-0008-2562-3016.

Полетайкин Алексей Николаевич

кандидат технических наук, доцент, доцент кафедры информационных технологий Кубанского государственного университета (350040, г. Краснодар, ул. Ставропольская, 149), доцент кафедры ММиЦРБС СибГУТИ (630102, Новосибирск, ул. Кирова, 86), e-mail: alex.poletaykin@gmail.com, ORCID ID: 0000-0002-5128-1952.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

API-Integrated Bayesian Risk Management Model for Cellular Network Base Stations

Konstantin E. Grigoriev[1], Valery S. Kanev[2], Aleksei N. Poletaikin [1,2]

[1] Kuban State University (KubSU)

[2] Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: The article presents a new approach to risk management of emergency situations at cellular network base stations. The diversity of emergencies arising on heterogeneous equipment under the influence of various external factors makes risk management a critically important task. The novelty lies in the creation of a mathematical model that accounts for this

diversity, providing more accurate and comprehensive prediction of emergency situations. The model is based on a Bayesian network and generates real-time solutions in the form of probabilities of emergency occurrences, identifying critical points and potential threats to the base station's overall functionality. This helps generate recommendations for reducing risks, identifying priority areas for implementing improvements, and modernizing equipment.
To ensure effective interaction with the model, an API is being developed and studied using FastAPI and Python. The API interacts with the Bayesian model created in BayesFusion GeNIe. The model implements a new method for integrating the developed Bayesian network with existing applications based on REST API principles, thus introducing a new approach to risk management. The article describes the processes of API creation, performance testing, and deployment. As a result of using the API, real-time risk management becomes possible, helping operators prevent emergency situations.
The integrated model was developed for research purposes to monitor the risk landscape of cellular network base stations. The application of this model significantly increases the level of automation in the risk management process during the operation of cellular network base stations.

Keywords: Bayesian network, API, risk assessment, emergency situations, cellular networks, base stations, BayesFusion GeNIe, risk management, accident prediction, FastAPI, API testing, automation.

For citation: Grigoriev K. E., Kanev V. S., Poletaikin A. N. API-Integrated Bayesian Risk Management Model for Cellular Network Base Stations. 2024. V. 18, № 4. P. 62–76. https://doi.org/10.55648/1998-6920-2024-18-4-62-76.

The article was submitted: 01.10.2024;
revised version: 05.11.2024;
accepted for publication 06.11.2024.

References

1. *Buntsev, I. A., Kanev, V. S.* Sistemnoe upravlenie riskami v telekomunikatsiyakh [Systematic risk management in telecommunications (state of the problem, methods, models, implementations). Vestnik SibGUTI. 2009, pp. 26-52.
2. *Diedrich, A., Deutschmann, P. and Junker, C.* ServiceNavigator - a bayesian assistance system for diagnosing industrial production systems. Proc. of 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS) (pp. 1-6).
3. *Bogner, J., Fritzsch, J., Wagner, S., Zimmermann, A.* Microservices in Industry: Insights into Technologies, Characteristics, and Software Quality. 2019. 10.1109/ICSA-C.2019.00041.
4. *Beaulieu, N., Dascalu, S. & Hand, E.* API-First Design: A Survey of the State of Academia and Industry. 2022. 10.1007/978-3-030-97652-1_10.
5. *Rezedinova, E. Yu., Kyrkunov, P. N., Sergeev, A. V.* Vybor servis-orientirovannoy arkhitektury dlya sozdaniya servisa po blago ustroystvu goroda [Choice of service-oriented architecture for creating a city improvement service]. SAEC, 2023, no. 3.
6. *Galiguzova, E. V., Illarionova, Yu. E.* Yazyk zaprosov GraphQL kak zamena REST API: sravnenie GraphQL i REST API [GraphQL query language as a replacement for REST API: comparison of GraphQL and REST API]. Simvol nauki, 2023, no. 1-2.
7. *Zhang, H., Wang, Z. R., Wang, X. W., Lin, F. C.* Practice and Research on FMEA of Telecommunication Satellite System. In: Sun, J., Wang, Y., Huo, M., Xu, L. (eds) Signal and Information Processing, Networking and Computers. Lecture Notes in Electrical Engineering, 2023, vol. 917. Springer, Singapore. https://doi.org/10.1007/978-981-19-3387-5_110.
8. *Alijanzadeh, M. R., Shayannia, S. A. & Movahedi, M. M.* Optimization of maintenance in supply chain process and risk-based critical failure situations (case study: Iranian oil pipeline and telecommunication company, north district). Journal of applied research on industrial engineering, 2024, vol. 11(1), pp. 125-142.

9. *Carretero-Ayuso, M.J.; Sánchez-Barroso, G.; González-Domínguez, J.; García-Sanz-Calcedo, J.* Failure Modes in Electricity and Telecommunication Facilities in Dwellings in Spain. Applied Sciences, 2021, vol. 11:5274. https://doi.org/10.3390/app11115274
10. *Tarcsay B. L., Bárkányi Á, Németh S, Chován T, Lovas L, Egedy A.* Risk-Based Fault Detection Using Bayesian Networks Based on Failure Mode and Effect Analysis. Sensors, 2024; vol. 24:3511.
11. Nalluri, V., Chen, L. Risk assessment for sustainability on telecom supply chain: A hybrid fuzzy approach. Uncertain Supply Chain Management, 2022, no. 10(2), pp. 559-576.
12. *Tsyganov, V. V., Gurlev, I. V.* Kognitivnoe prognozirovanie informatsionno-telekommunikatsionnoy infrastruktury krupnomasshtabnogo regiona [Cognitive forecasting of information and telecommunication infrastructure in a large-scale region]. ITNOU: Informatsionnye tekhnologii v nauke, obrazovanii i upravlenii, 2020, no. 1 (15). pp. 3-7.
13. *Mishra, A., Kumar, D., Shuaib, M., Tyagi, M., Singh, R.* Measurement of Critical Factors: A Case of Telecommunication Industry. 2021. 10.1007/978-981-15-6017-0.
14. *Bayas, B., Zambrano, C.* Redes bayesianas aplicadas a la predicción de errores en las redes definidas por software [Bayesian networks applied to error prediction in software-defined networks]. Revista Universidad y Sociedad, 2021, Vol. 13, pp. 419-429.
15. *Dumbrais, K. O., Glushchenko, O. M.* Modelirovanie i analiz riskov IT-proyektov [Modeling and analysis of risks in IT projects]. Nauka i obrazovanie segodnya, 2021, No. 2 (61), pp. 26–33.
16. *Demchuk, D. A., Demchuk, K. A., Shevtsova, Y. V., Poletaykin, A. N.* Bayesovskiy podkhod pri chislennom raschete riska meditsinskoy evakuatsii avtotransportom [Bayesian approach to numerical risk assessment in medical evacuation by road transport]. Vestnik SibGUTI, 2023, vol. 17(1), pp. 18-32. https://doi.org/10.55648/1998-6920-2023-17-1-18-32.
17. *Adib, D., Safarzadeh, H., Mohammadi, M.* Designing and explaining the IoT commercialization model in Iranian organizations (Telecommunication Company of Iran): An interpretive structural modeling (ISM) approach, International Journal f Nonlinear Analysis and Applications, 2023, vol. 14(1), pp. 723-738. doi: 10.22075/ijnaa. 2022.26942.3456.
18. *Chen, W.-K., Nalluri, V., Ma, S., Lin, M.-M., Lin, C.-T.* An Exploration of the Critical Risk Factors in Sustainable Telecom Services: An Analysis of Indian Telecom Industries. Sustainability, 2021, no. 13, pp. 445. https://doi.org/10.3390/su13020445.
19. GeNIe Modeler. User's Manual. BayesFusion, LLC, 2024. Available at: https://support.bayesfusion.com/docs/GeNIe.pdf (Accessed: 12 August 2024).
20. *Gaag, L. C., Kjaerulff, U.* Making Sensitivity Analysis Computationally Efficient, Proceedings of the 16th Conference on Uncertainty in Artificial Intelligence, 2000, pp. 317–325.
21. *Kudryavtsev A. A., Radionov A. V.* Introduction to quantitative risk management: textbook. – St. Petersburg: Publishing house of St. Petersburg University, 2016. – 192 p.

Konstantin E. Grigorev

Master's student of Applied Mathematics and Computer Science, Kuban State University (350040, Krasnodar, Stavropolskaya St., 149), e-mail: k.e.grigorev@gmail.com, ORCID ID: 0009-0004-5518-6989.

Valery S. Kanev

Doctor of Sci. (Engineering), Head at the Mathematical Modeling and Digital Development of Business Systems Department, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 269 82 77, e-mail: kanev@sibguti.ru, ORCID ID: 0009-0008-2562-3016, Scopus AuthorID: 56418038200, ResearcherID: ABG-3120-2020.

Aleksey N. Poletaikin

Cand. of Sci. (Engineering), Assistant Professor at the Information Technologies Department, Kuban State University (KubSU, Russia, 350040, Krasnodar,, Stavropolskaya st., 149), Assistant Professor at the Mathematical Modeling and Digital Development of Business Systems Department, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 861 2199 577, e-mail: alex.poletaykin@gmail.com, ORCID ID: 0000-0002-5128-1952, Scopus AuthorID: 57213829361, ResearcherID: ABF-6799-2020.