УДК 004.772

Методика комплексной оценки качества функционирования сети передачи данных киберфизических систем ОАО «РЖД»

А. А. Привалов[1], А. М. Болдинов[2]

[1]Военная ордена Жукова академия войск национальной гвардии Российской Федерации, Российская Федерация, 198206, Санкт-Петербург, ул. Л. Пилютова, 1
[2]Петербургский государственный университет путей сообщения Императора Александра I, Российская Федерация, 190031, Санкт-Петербург, Московский пр., 9

Для цитирования: *Привалов А. А., Болдинов А. М.* Методика комплексной оценки качества функционирования сети передачи данных киберфизических систем ОАО «РЖД» // Известия Петербургского университета путей сообщения. — СПб.: ПГУПС, 2025. — Т. 22. — Вып. 2. — С. 316–328. DOI: 10.20295/1815-588X-2025-2-316-328

Аннотация

Цель: Разработка методики оценки качества функционирования сети передачи данных (СПД) киберфизической системы (КФС) ОАО «РЖД» в условиях кибервоздействий злоумышленников и возможных технических отказов. **Методы:** Методика построена на базе частных и обобщенных математических моделей. Включает в себя: математическую модель радиоканала с учетом процессов установления и поддержания соединения, модель кибервоздействия типа «отказ в обслуживании», модель обнаружения кибервоздействия с последующим восстановлением процесса передачи данных, модель передачи данных по различным маршрутам, модель узла связи в условиях кибервоздействий и возможных технических отказов, модель передачи данных по проводным каналам связи с использованием протокола TCP, а также комплексную модель СПД КФС ОАО «РЖД» в условиях кибервоздействий злоумышленников и технических отказов. **Результаты:** Разработанная методика позволяет оценивать качество функционирования СПД КФС ОАО «РЖД» в условиях кибервоздействий и технических отказов. Выработаны направления по предотвращению срывов передачи данных объектам управления КФС. Методика представлена в виде блок-схемы алгоритма, в которой каждый блок иллюстрирует расчет функции распределения времени на основе частных математических моделей. **Практическая значимость:** Предложенная методика предназначена для комплексной оценки качества функционирования СПД КФС ОАО «РЖД» в условиях кибервоздействий и технических отказов. Она может быть полезна научно-исследовательским организациям и предприятиям, занимающимся разработкой и совершенствованием беспилотных и роботизированных систем, поскольку обеспечивает подходы для разработки надежных и устойчивых сетей передачи данных.

Ключевые слова: Сеть передачи данных, сеть связи, методика, оценка качества функционирования, математическая модель.

Введение

Железнодорожный транспорт является объектом критической информационной инфраструктуры (КИИ) и подвержен кибервоздействиям [1]. Сети передачи данных (СПД) обеспечивают оперативную и достоверную связь между объектами железнодорожного транспорта, а в киберфизических системах (КФС) играют ключевую роль в поддержании их работоспособности. В настоящее время отсутствуют методики, позволяющие оценивать вероятность своевременной доставки данных в СПД КФС ОАО «РЖД», что подчерки-

вает необходимость разработки подходов к комплексной оценке качества их функционирования.

Существуют исследования, посвященные аспектам защищенности СПД, анализу процессов функционирования сети и ее компонентов в различных условиях. Однако вопросы своевременной доставки данных часто остаются вне рассмотрения.

В работе [2] были предложены показатели устойчивости, основанные на связности графов. Сеть связи декомпозировалась на составные элементы, а устойчивость определялась вероятностью наличия хотя бы одного пути с требуемым качеством обслуживания (QoS).

В работе [3] представлена универсальная метрика для оценки эффективности сетей связи, основанная на соотношении полезного эффекта к затратам. Показатели качества были распределены по классам согласно заданным критериям, а в итоге получен обобщенный показатель Ливн, применимый для оценки объема сети. Однако при расчетах не учитывались важнейшие показатели, такие как время доставки данных и надежность.

Основным результатом работы [4] является методика оценки устойчивости сети специального назначения, включающая обобщенный показатель устойчивости функционирования. Однако в этой методике отсутствует учет кибервоздействий злоумышленников, что не позволяет использовать ее для комплексной оценки надежности и безопасности связи в сетях специального назначения.

Исследования [5–7] посвящены оценке качества функционирования телекоммуникационных сетей, но вопросы надежности передачи данных остались вне рассмотрения. Между тем требования к СПД могут существенно различаться в зависимости от их назначения. В частности, СПД КФС предъявляют особенно высокие требования к надежности и безопасности, которые превышают стандарты, применяемые к менее критичным объектам. Анализ работ [2–7] показывает, что оценка вероятности передачи данных за время, не превышающее заданное, в них не проводилась.

Согласно данным работы [8], уровень исходной защищенности СПД зависит прежде всего от ее технических и эксплуатационных характеристик. В применении к СПД КФС ОАО «РЖД» можно выделить факторы, снижающие ее защищенность:

1. Распределенность сети: СПД КФС ОАО «РЖД» охватывает несколько регионов, что делает ее уязвимой к внешним воздействиям и снижает уровень безопасности.

2. Многоточечный доступ к сетям общего пользования: СПД КФС имеет многочисленные точки доступа к сети общего пользования, используемой для обмена данными между подразделениями железнодорожного транспорта. Это повышает риск утечек и атак, снижая общий уровень защищенности.

3. Разнообразие операций с данными: СПД КФС выполняет широкий спектр операций, включая модификацию, обработку и передачу данных, что создает множество потенциальных точек уязвимости.

4. Интеграция со сторонними СПД: поскольку СПД КФС получает и передает данные между различными железнодорожными службами, она интегрирована в общую СПД, в которую могут входить сторонние системы, увеличивая риск несанкционированного доступа.

Эти особенности подчеркивают необходимость разработки методики оценки качества функционирования СПД КФС с учетом специфики ее работы и требований, предъявляемых к объектам КИИ.

Согласно [9, 10], информационная безопасность определяется как состояние защищенности передаваемой информации, обеспечиваемое мерами по поддержанию ее конфиденциально-

сти, целостности и доступности при передаче, обработке и хранении в СПД. В условиях возможных кибервоздействий [11] и технических отказов возникает необходимость оценки вероятностно-временных характеристик передачи данных.

Разработка методики комплексной оценки качества функционирования СПД КФС ОАО «РЖД» в условиях кибервоздействий и технических отказов является актуальной задачей. Существующие методы управления информационной безопасностью часто оказываются недостаточными для эффективного противодействия угрозам, связанным с блокированием или нарушением доставки данных. Это может приводить к сбоям в управлении перевозками, а в случае КФС — к серьезным последствиям вплоть до аварий и катастроф, поскольку именно через СПД осуществляется управление ее объектами.

Таким образом, необходимо разработать методику, позволяющую комплексно оценивать качество функционирования СПД в условиях киберугроз и технических сбоев. Для комплексной оценки качества функционирования СПД КФС необходимо учитывать вероятность своевременной передачи данных за время, не превышающее заданное.

СПД КФС ОАО «РЖД» обеспечивает передачу трафика различных категорий срочности. К сообщениям 1-й категории срочности относятся команды управления и критические команды. К данным 2-й категории срочности и ниже относятся данные о состоянии пути, карты маршрута и другая служебно-техническая информация. Согласно требованиям руководящих документов [12–15], для заданного времени своевременной передачи данных $T_{зад}$ устанавливаются ограничения. Для данных 1-й категории срочности: $T_{зад} \le 1\,(\text{с})$ с заданной вероятностью $P_{св} = 0,999$. Для данных 2-й категории срочности и ниже: $T_{зад} \le 5\,(\text{с})$ с заданной вероятностью $P_{св} = 0,99$.

В настоящее время отсутствуют методики расчета, удовлетворяющие указанным требованиям. Поэтому актуальной задачей является разработка методики, способной комплексно оценивать качество функционирования СПД КФС ОАО «РЖД» в условиях кибервоздействий злоумышленников и возможных технических отказов.

Структура и содержание методики

Исходные данные, используемые в методике, соответствуют нормативным и руководящим документам, а также требованиям ГОСТ по защите информации [8, 16–20]. Эти данные описывают: конфигурацию защищаемой СПД КФС ОАО «РЖД», принципы и возможности функционирования СОВ, алгоритмы работы СОВ, состояние среды общего доступа. Часть исходных данных была получена в результате моделирования функционирования СПД КФС ОАО «РЖД» в условиях кибервоздействий злоумышленников с использованием [21–25].

В техническом задании (ТЗ) на разработку информационных систем (ИС) установлены требования к своевременности предоставления запрашиваемой (или выдаваемой принудительно) выходной информации. Оцениваемые показатели, характеризующие надежность и своевременность передачи данных (и/или выполнения технологических операций), не должны быть хуже заданных значений. При этом показатели должны учитывать специфику системы [17].

Основным показателем оценки выбрана вероятность своевременной передачи данных за время, не превышающее заданное: $P_{св}\left\{t_{пер} \le T_{зад}\right\}$. Это позволяет разработать методику оценки качества функционирования СПД КФС в условиях кибервоздействий и возможных технических отказов.

Критерий оценки: $P_{св}\left\{t_{пер} \le T_{зад}\right\}$. Выбранный показатель рассчитывается с использованием разработанных авторами частных моделей [21–25].

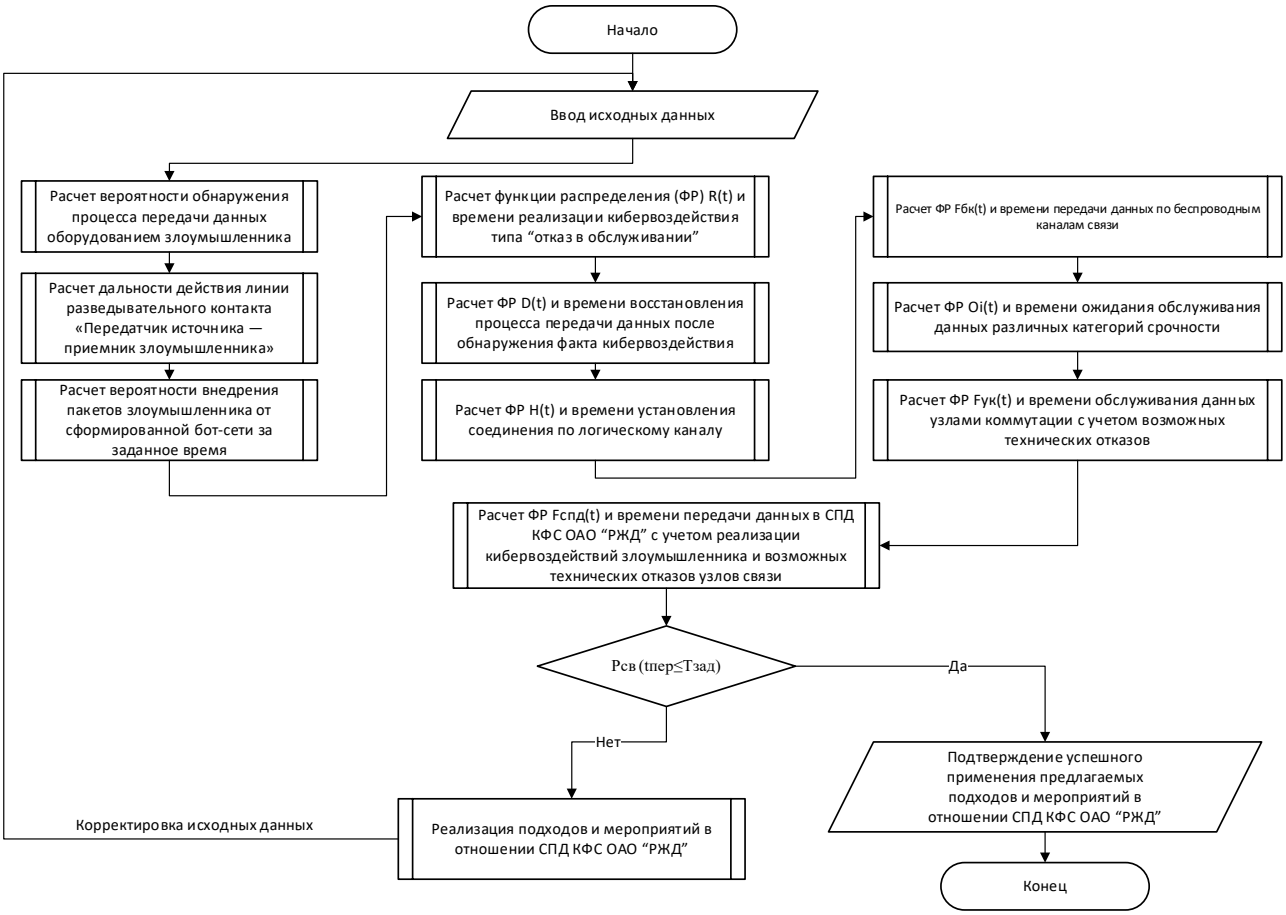

Рис. 1. Блок-схема алгоритма методики комплексной оценки качества функционирования СПД КФС ОАО «РЖД»

Последовательность вычисления показателя вероятности своевременной доставки данных представлена на рис. 1 в виде блок-схемы алгоритма.

Методика определения комплексной оценки функционирования СПД КФС ОАО «РЖД» содержит следующие блоки:

Блок 1: ввод исходных данных.

Блок 2: расчет вероятности обнаружения передачи данных злоумышленником. Вероятность определяется с учетом технических мер защиты, реализованных в СПД КФС ОАО «РЖД», с использованием нормативных документов [8, 16–20].

Блок 3: расчет дальности действия линии разведывательного контакта «Передатчик источника — приемник злоумышленника» определяется энергией (мощностью) передатчика и может быть рассчитана с помощью следующей формулы [26]:

$$D_{\max} = \sqrt{\frac{P_{\text{пер}} G_{\text{пер}} G_{\text{пр}} \lambda^2 \eta}{(4\pi)^2 \delta_{\min} R T_{\Sigma} \Delta f L}},$$

где $P_{\text{пер}}$ — мощность передатчика;

$G_{\text{пер}}$ — коэффициент усиления антенны передатчика;

$G_{\text{пр}}$ — коэффициент усиления антенны приемника;

λ — длина волны передатчика;

η — коэффициент потерь в среде распространения;

$\delta_{\min}$ — минимально допустимое превышение сигнала над шумом по мощности;

R — постоянная Больцмана;

T_Σ — суммарная шумовая температура на входе приемника;

Δf — полоса сигнала;

L — коэффициент запаса на неучитываемые факторы (обычно лежит в пределах от 3 до 10).

Блок 4: расчет вероятности внедрения пакетов злоумышленника от сформированной бот-сети за заданное время, при условии, что поступившие пакеты от бот-сети сразу поступают на обслуживание. Вероятность рассчитывается с учетом технических мер защиты, реализуемых в СПД типовой КФС ОАО «РЖД», с использованием [8, 16–20].

Вероятность внедрения пакетов данных злоумышленника рассчитывается с использованием [17]:

$$P_{\text{внедр}} = e^{-\sigma T_{\text{п.з}}}(1+\sigma T_{\text{п.з}}),$$

где σ — частота поступления пакетов данных злоумышленника от сформированной бот-сети;

$T_{\text{п.з}}$ — заданное время.

Блок 5: расчет функции распределения $R(t)$ и времени реализации кибервоздействия типа «отказ в обслуживании». Функцию распределения целесообразно представить в виде гамма-функции, используя параметры формы и масштаба, кроме того, функции распределения остальных процессов представим аналогичным образом.

Функция распределения:

$$R(t) = \frac{\chi^{\psi}}{\Gamma(\psi)}\int_0^t t^{\psi-1}e^{-\chi t}dt,$$

где $\chi = \dfrac{M_{1r}}{D_r}$ — параметр масштаба;

$\psi = \dfrac{M_{1r}^2}{D_r}$ — параметр формы;

M_{1r} — математическое ожидание реализации кибервоздействия;

D_r — дисперсия реализации кибервоздействия.

Блок 6: расчет функции распределения $D(t)$ и времени восстановления процесса передачи данных после обнаружения факта кибервоздействия.

Функция распределения:

$$D(t) = \frac{K^W}{\Gamma(W)}\int_0^t t^{W-1}e^{-Kt}dt,$$

где K — параметр масштаба;

W — параметр формы.

Блок 7: расчет функции распределения $H(t)$ и времени установления соединения по логическому каналу [21].

Функция распределения:

$$H(t) = \frac{\varsigma^{\upsilon}}{\Gamma(\upsilon)}\int_0^t t^{\upsilon-1}e^{-\varsigma t}dt,$$

где ν — параметр формы;

ς — параметр масштаба.

Блок 8: расчет функции распределения $F_{\text{бк}}(t)$ и времени передачи данных по беспроводным каналам связи [21, 22].

Функция распределения:

$$F_{\text{бк}}(t) = \frac{\lambda^{\alpha}}{\Gamma(\alpha)}\int_0^t t^{\alpha-1}e^{-\lambda t}dt,$$

где α — параметр формы;

λ — параметр масштаба.

Блок 9: расчет функции распределения $O_i(t)$ и времени ожидания обслуживания данных различных категорий срочности [23].

Функция распределения:

$$O_i(t) = \frac{\mu^{\beta}}{\Gamma(\beta)}\int_0^t t^{\beta-1}e^{-\mu t}dt, i = 1, I,$$

где β — параметр формы;

μ — параметр масштаба;

i — категория срочности передаваемых данных.

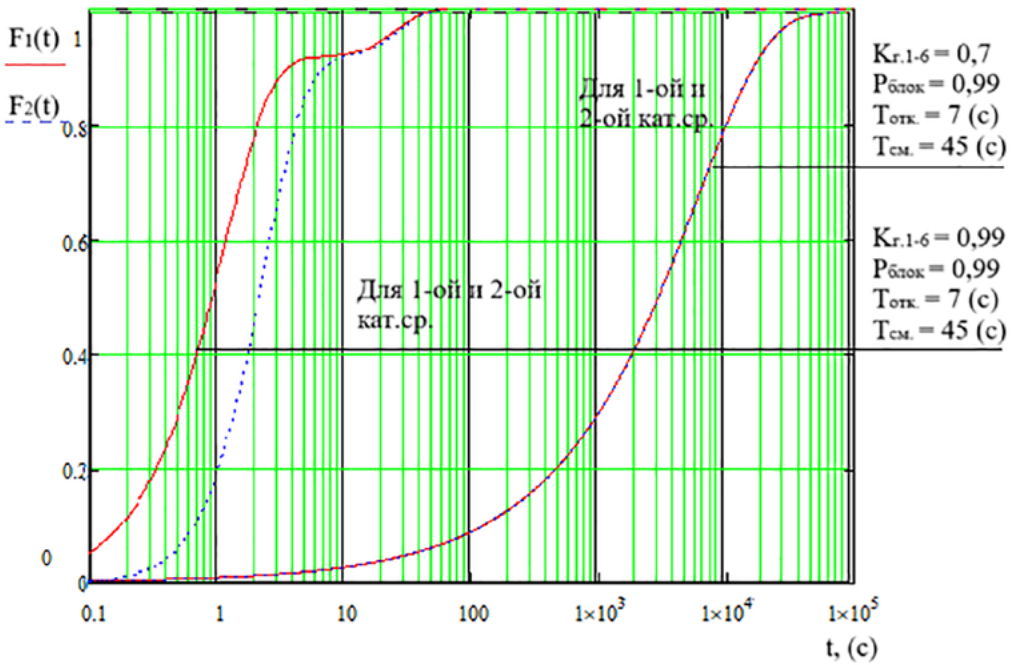

Рис. 2. Вероятностно-временные характеристики своевременной доставки данных для 1-й и 2-й категорий срочности в различных условиях

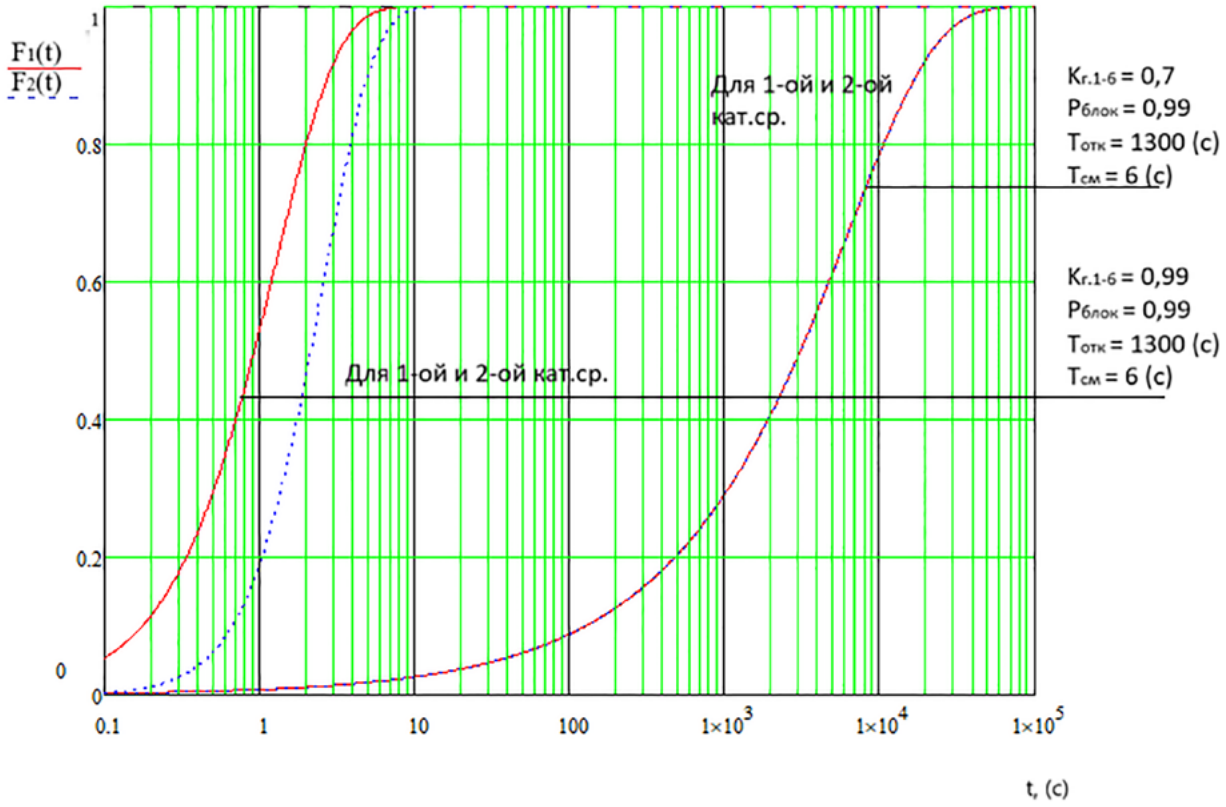

Рис. 3. Вероятностно-временные характеристики своевременной доставки данных для 1-й и 2-й категорий срочности в различных условиях

Блок 10: расчет функции распределения $F_{\text{ук}}(t)$ и времени обслуживания данных узлами коммутации с учетом возможных технических отказов.

Функция распределения:

$$F_{\text{ук}}(t) = \frac{Z^E}{\Gamma(E)} \int_0^t t^{E-1} e^{-Zt} dt,$$

где E — параметр формы;

Z — параметр масштаба.

Блок 11: расчет функции распределения $F_{\text{спд}}(t)$ и времени передачи данных в СПД КФС ОАО «РЖД» с учетом кибервоздействий злоумышленника и технических отказов узлов связи [24, 25]. Результаты расчета представлены на рис. 2, 3.

Получим итоговую функцию распределения:

$$F_{\text{спд}}(t) = \frac{N^M}{\Gamma(M)} \int_0^t t^{M-1} e^{-Nt} dt,$$

где M — параметр формы;

N — параметр масштаба.

Блок 12: расчет показателя оценки вероятности своевременной передачи данных за время, не превышающее заданное $P_{\text{св}}\left\{t_{\text{пер}} \le T_{\text{зад}}\right\}$. Расчет вероятности своевременной передачи за время является функцией распределения, полученной в блоке 11. В соответствии с [17], для систем, в которых возможны отказы при передаче данных, дополнительно учитываются показатели, характеризующие вероятность их потери в процессе обслуживания. Это актуализирует задачу разработки оригинальных математических моделей. Выполняется сравнение вычисленных значений из блока 11 с установленными нормативами. Полученный показатель $P_{\text{св}}\left(t_{\text{пер}}\right)$ сопоставляется с требуемыми значениями: для сообщений 1-й категории срочности $T_{\text{зад}} = 1\,(\text{с})$ при $P_{\text{св}} = 0{,}999$, для сообщений 2-й категории срочности $T_{\text{зад}} = 5\,(\text{с})$ при $P_{\text{св}} = 0{,}99$. Если условие выполняется, осуществляется переход к блоку 13, где подтверждается применимость предложенных подходов и мероприятий в СПД КФС ОАО «РЖД». В противном случае необходимо внедрение дополнительных мер, направленных на сокращение времени передачи данных, с последующей корректировкой исходных данных.

Вероятностно-временные характеристики своевременной доставки данных для 1-й и 2-й категорий срочности представлены на рис. 2, 3.

Результаты, полученные с использованием предложенной методики оценки качества функционирования СПД КФС ОАО «РЖД» в условиях кибервоздействий злоумышленника и возможных технических отказов, показывают, что показатель вероятности своевременной доставки данных за заданное время для двух категорий срочности не соответствует требованиям руководящих документов.

При времени реализации кибервоздействия $T_{\text{отк}} = 7(c)$, времени реализации смены маршрута $T_{\text{см}} = 45(\text{с})$ и различных значениях коэффициентов готовности узлов связи $K_{\text{г.1–6}} = 0{,}7$ и $K_{\text{г.1–6}} = 0{,}99$ получим: время передачи данных $t_{\text{пер}} = 63\,000(\text{с}) \le T_{\text{зад}} = 1(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0{,}999$ для 1-й категории срочности, $t_{\text{пер}} = 41\,000(\text{с}) \le T_{\text{зад}} = 5(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0{,}99$ для 2-й категории срочности, $t_{\text{пер}} = 40(\text{с}) \le T_{\text{зад}} = 1(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0{,}999$ для 1-й категории срочности, $t_{\text{пер}} = 38(\text{с}) \le T_{\text{зад}} = 5(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0{,}99$ для 2-й категории срочности.

При $T_{\text{отк}} = 1300(\text{с})$, $T_{\text{см}} = 6(\text{с})$ и различных значениях коэффициентов готовности узлов связи $K_{\text{г.1–6}} = 0{,}7$ и $K_{\text{г.1–6}} = 0{,}99$ получим: $t_{\text{пер}} = 63\,000(c) \le T_{\text{зад}} = 1(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0{,}999$ для 1-й категории срочности, $t_{\text{пер}} = 41\,000(\text{с}) \le T_{\text{зад}} = 5(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0{,}99$ для 2-й категории

срочности, $t_{\text{пер}} = 8(\text{с}) \le T_{\text{зад}} = 1(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0,999$ для 1-й категории срочности, $t_{\text{пер}} = 8,6(\text{с}) \le T_{\text{зад}} = 5(\text{с})$ с заданной вероятностью $P_{\text{св}} = 0,99$ для 2-й категории срочности.

Разработанная методика оценки качества функционирования СПД КФС ОАО «РЖД» в условиях кибервоздействий злоумышленников и возможных технических отказов позволяет не только оценить показатель вероятности своевременной доставки данных за заданное время, но и выбрать рациональные мероприятия, направленные на снижение времени доставки данных. Кроме того, методика позволяет выработать организационно-технические предложения по повышению защищенности СПД КФС ОАО «РЖД».

Заключение

1. Разработана методика оценки качества функционирования СПД КФС ОАО «РЖД», функционирующая в условиях кибервоздействий злоумышленников и возможных технических отказов. Методика отличается возможностью определения показателя оценки вероятности своевременной доставки данных за заданное время $P_{\text{св}}\left\{T_{\text{пер}} \le T_{\text{зад}}\right\}$.

2. Поскольку СПД КФС функционирует в составе общетехнологической СПД ОАО «РЖД» и использует ее ресурсы, в сети передается разнородный трафик, что увеличивает время передачи данных по маршрутам. Для предотвращения увеличения времени передачи одним из предлагаемых направлений является организация выделенной СПД, использующей канальный ресурс общетехнологической СПД ОАО «РЖД». Это приведет к тому, что передаваемый трафик станет однородным, а самоподобие трафика исчезнет.

3. В случае организации выделенной СПД сеть становится детерминированной, а число маршрутов передачи данных ограничивается. Это позволяет ограничить время передачи трафика объектам управления КФС. Следовательно, время передачи данных по маршрутам будет определяться временем передачи критической информации, так как оно связано с реакцией КФС на предотвращение аварийных ситуаций и минимальным временем прохождения информации по маршруту. Эти ограничения позволяют внедрить временные метки.

4. Для управления объектами КФС передаваемый трафик имеет отличительные характеристики: пакеты обладают однородной структурой и ограниченным коротким размером. Данные признаки позволяют отличать пакеты данных, поступившие от бот-сети злоумышленника, и изолировать их.

5. Однако даже в случае организации выделенной сети доступ злоумышленника к ней сохраняется. Злоумышленник способен копировать структуру пакетов, передаваемых в СПД, для организации атаки типа «отказ в обслуживании» (DDoS). В соответствии с этим необходимо использовать методы аутентификации по принципу «свой-чужой». Для этого в структуру пакета включается опознавательная группа, адрес которой изменяется по определенным правилам. Эти правила всегда опережают действия злоумышленника по отправке пакетов в сеть.

6. Местоположение каждого узла связи и базовой станции в СПД строго известно. Это позволяет рассчитывать время прохождения трафика по заданному маршруту с учетом задержек при прохождении узлов связи. Таким образом, становится возможной аутентификация по положению в пространстве.

7. Использование интеллектуальных агентов в СПД обеспечивает обнаружение аномалий при строго ограниченном трафике. При попытке передачи пакетов злоумышленника уровень аномалий резко возрастает, что приводит к оповещению системы обнаружения вторжений о несанкционированном доступе в СПД. В этом случае

необходимо принимать меры по аутентификации проходящего трафика.

8. При высоких значениях времени восстановления УК снижается общая надежность СПД. Для своевременной доставки данных необходимо проводить комплекс мероприятий для снижения времени восстановления процесса передачи данных, для мониторинга целесообразно применять интеллектуальных агентов.

Список источников

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

2. Михайлов Р. Л. Оценка устойчивости сети связи в условиях воздействия на нее дестабилизирующих факторов / Р. Л. Михайлов, С. И. Макаренко // РТС. — 2013. — № 4(12). — С. 69–79.

3. Карганов В. В. Показатель оценки эффективности систем связи и их элементов / В. В. Карганов, А. Г. Расчесова, В. А. Кудряшов // Информатика, телекоммуникации и управление. — 2016. — № 1(236). — С. 7–14.

4. Одоевский С. М. Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой / С. М. Одоевский, П. В. Лебедев // Системы управления, связи и безопасности. — 2021. — № 1. — С. 152–189.

5. Бабиков В. Н. Разработка моделей и методик оценки эффективности комплексной системы защиты информации: дисс. … канд. техн. наук: 05.13.19 / В. Н. Бабиков. — СПб., 2006. — 147 с.

6. Бухарин В. В. Способ защиты информационно-вычислительных сетей от компьютерных атак / В. В. Бухарин, А. В. Кирьянов, Ю. И. Стародубцев // Труды МАИ: электронный научный журнал. — 2012. — № 57.

7. Захарченко С. С. Показатели эффективности выявления уязвимостей при использовании метода проверки на модели / С. С. Захарченко, А. А. Корниенко, С. Е. Ададуров // Труды IV-й Международной научно-практической конференции «Интеллекттранс-2014». — 2014. — С. 211–213.

8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена заместителем директора ФСТЭК России 15.02.08. — 70 с.

9. ГОСТ Р 53953. Электросвязь железнодорожная. Термины и определения. — М., 2010. — 52 с.

10. Стандарт ОАО «РЖД». Управление информационной безопасностью. Общие положения. СТО РЖД 1.18.002—2009. — 30 с.

11. Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов: учебное пособие / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова. — М.: Горячая линия-Телеком, 2013. — 220 с.

12. ГОСТ Р 50922—2017. Информационная технология. Управление качеством обслуживания в сетях связи.

13. ГОСТ Р 51323—2009. Информационная технология. Методы и средства обеспечения безопасности информации. Защита от несанкционированного доступа к информации.

14. СТО РЖД 718048.1—2014. Комплексные системы управления движением поездов. Требования к проектированию, строительству и эксплуатации.

15. СТО РЖД 718048.2—2014. Комплексные системы управления движением поездов. Требования к средствам связи и передачи данных.

16. Шабалин Н. Г. Концепция информационной подсистемы многоуровневой системы управления и обеспечения безопасности движения поездов (АСУ МС) / Н. Г. Шабалин; под ред. Н. Г. Шабалина. — М.: ВНИИУП, 2003. — 56 с.

17. 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.

18. Концепция обеспечения кибербезопасности информационных и управляющих систем в ОАО «РЖД» (проект редакция 1.0). — М.: ОАО «РЖД», 2013. — 285 с.

19. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли. — М., 2010. — 48 с.

20. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Решение Коллегии Гостехкомиссии России № 7.2/02.03.2001.

21. Болдинов А. М. Математическая модель канала управления стандарта радиосвязи GSM-R / А. М. Болдинов, А. А. Привалов, А. А. Привалов // Известия Петербургского университета путей сообщения. — 2022. — Т. 19. — № 4. — С. 743–751.

22. Привалов А. А. Математическая модель процесса передачи команд управления по радиоканалам автоматизированных систем / А. А. Привалов, А. А. Привалов, А. М. Болдинов // Информация и космос. — 2023. — № 4. — С. 71–83.

23. Makhmudov F. Mathematical Model of the Process of Data Transmission over the Radio Channel of Cyber-Physical Systems / F. Makhmudov, A. Privalov, A. Privalov et al. // Mathematics. — 2024. — Vol. 12. — Iss. 10. — P. 1452.

24. Привалов А. А. Математическая модель функционирования сети передачи данных киберфизической системы в условиях кибервоздействия злоумышленника / А. А. Привалов, А. М. Болдинов, Е. В. Скуднева, А. А. Привалов // Информация и космос. — 2024. — № 3. — С. 74–84.

25. Болдинов А. М. Комплексная модель сети передачи данных киберфизической системы / А. М. Болдинов // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т., Санкт-Петербург, 27–28 февраля 2024 года. — СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2024. — С. 117–121.

26. Ярочкин В. И. Информационная безопасность: учебник для студентов вузов / В. И. Ярочкин. — М.: Академический Проект; Гаудеамус, 2-е изд. — 2004. — 544 с.

Дата поступления: 02.03.2025
Решение о публикации: 10.04.2025

Контактная информация:
ПРИВАЛОВ Андрей Андреевич — д-р воен. наук, проф.; aprivalov@inbox.ru
БОЛДИНОВ Алексей Максимович — аспирант; 23boldinov98@gmail.com

A Methodology for a Comprehensive Assessment of the Quality of the Data Transmission Network Functioning of Cyber–Physical Systems at JSCo "Russian Railways"

A. A. Privalov[1], A. M. Boldinov[2]

[1]Military Order of Zhukov Academy of the National Guard Troops of the Russian Federation, 1, L. Pilyutova Str., Saint Petersburg, 198206, Russian Federation
[2]Emperor Alexander I Petersburg State Transport University, 9, Moskovsky pr., Saint Petersburg, 190031, Russian Federation

For citation: Privalov A. A., Boldinov A. M. A Methodology for a Comprehensive Assessment of the Quality of the Data Transmission Network Functioning of Cyber-Physical Systems at JSCo "Russian Railways". *Proceedings of Petersburg State Transport University*, 2025, vol. 22, iss. 2, pp. 316–328. (In Russian) DOI: 10.20295/1815-588X-2025-2-316-328

Summary

Purpose: To develop a methodology for assessing the quality of data transmission network functioning (DTN) of cyber-physical systems (CPS) at JSCo "RZD" in the event of cyberattacks by malicious actors and possible technical failures. **Methods:** The authors used specific and general mathematical models. These included a mathematical model of the radio channel, incorporating connection establishment and maintenance processes; a cyberattack model of the "Denial of Service" type; a model for detecting cyberattacks, followed by the restoration of data transmission; and a model for data transmission via various routes; a model of a communication node in the context of cyberattacks and potential technical failures; a model for data transmission over wired communication channels using the TCP protocol, as well as a comprehensive model of the DTN of the CPS at JSCo "RZD" in the event of malicious cyberattacks and technical failures. **Results:** The methodology developed allows for the evaluation of the quality of DTN functioning of the CPS at JSCo "RZD" in the event of cyberattacks and technical failures. Measures to prevent disruptions in data transmission to the CPS control objects have been identified. The methodology is presented in the form of a flowchart algorithm, where each block illustrates the calculation of time distribution functions based on specific mathematical models. **Practical significance:** The proposed methodology is intended for a comprehensive assessment of the quality of DTN functioning of the CPS at JSC "RZD" in the event of cyberattacks and technical failures. It is particularly beneficial for research organizations and companies involved in the development and improvement of unmanned and robotic systems, as it provides the approaches for designing reliable and resilient data transmission networks.

Keywords: Data transmission network, communication network, methodology, quality of functioning assessment, mathematical model.

References

1. *Federal'nyy zakon "O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii" ot 26.07.2017 № 187-FZ* [Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 № 187-FZ]. (In Russian)

2. Mikhaylov R. L., Makarenko S. I. *Otsenka ustoychivosti seti svyazi v usloviyakh vozdeystviya na nee destabiliziruyushchikh faktorov* [Assessment of the Stability of a Communication Network under the Impact of Destabilizing Factors]. RTS, 2013, Iss. 4(12), pp. 69–79. (In Russian)

3. Karganov V. V., Raschesova A. G., Kudryashov V. A. Pokazatel' otsenki effektivnosti sistem svyazi i ikh elementov [Indicator for Assessing the Efficiency of Communication Systems and Their Elements]. *Informatika, telekommunikatsii i upravlenie* [Informatics, Telecommunications and Management]. 2016, Iss. 1(236), pp. 7–14. (In Russian)

4. Odoevskiy S. M., Lebedev P. V. Metodika otsenki ustoychivosti funktsionirovaniya sistemy tekhnologicheskogo upravleniya infokommunikatsionnoy set'yu spetsial'nogo naznacheniya s zadannoy topologicheskoy i funktsional'noy strukturoy [Methodology for assessing the sustainability of the functioning of the technological control system of a special-purpose infocommunication network with a given topological and functional structure]. *Sistemy upravleniya, svyazi i bezopasnosti* [Control, Communications and Security Systems]. 2021, Iss. 1, pp. 152–189. (In Russian)

5. Babikov V. N. *Razrabotka modeley i metodik otsenki effektivnosti kompleksnoy sistemy zashchity informatsii: diss. ... kand. tekhn. nauk: 05.13.19* [Development of models and methods for assessing the effectiveness of an integrated information security system: diss. ... Cand. Sciences: 05.13.19]. St. Petersburg, 2006, 147 p. (In Russian)

6. Bukharin V. V., Kir'yanov A. V., Starodubtsev Yu. I. Sposob zashchity informatsionno-vychislitel'nykh setey ot komp'yuternykh atak [Method for protecting information and computing networks from computer attacks]. *Trudy MAI: elektronnyy nauchnyy zhurnal* [Proceedings of MAI: electronic scientific journal]. 2012, Iss. 57. (In Russian)

7. Zakharchenko S. S., Kornienko A. A., Adadurov S. E. Pokazateli effektivnosti vyyavleniya uyazvimostey pri ispol'zovanii metoda proverki na modeli [Performance

indicators of vulnerability detection using the model checking method]. *Trudy IV Mezhdunarodnoy nauchno-prakticheskoy konferentsii "Intellekttrans-2014"* [Proceedings of the IV-th International scientific and practical conference "Intellecttrans-2014"]. 2014, pp. 211–213. (In Russian)

8. *Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh (vypiska). Utverzhdena zamestitelem direktora FSTEK Rossii 15.02.08* [Basic model of threats to personal data security during their processing in personal data information systems (extract). Approved by the Deputy Director of the FSTEC of Russia on 15.02.08]. 70 p. (In Russian)

9. *GOST R 53953. Elektrosvyaz' zheleznodorozhnaya. Terminy i opredeleniya* [GOST R 53953. Railway telecommunications. Terms and definitions]. Moscow, 2010, 52 p. (In Russian)

10. *Standart OAO "RZhD". Upravlenie informatsionnoy bezopasnost'yu. Obshchie polozheniya. STO RZhD 1.18.002—2009* [Standard of JSC "Russian Railways". Information security management. General provisions. STO RZD 1.18.002—2009]. 30 p. (In Russian)

11. Shelukhin O. I., Sakalema D. Zh., Filinova A. S. *Obnaruzhenie vtorzheniy v komp'yuternye seti (setevye anomalii). Uchebnoe posobie dlya vuzov: uchebnoe posobie* [Detection of intrusions in computer networks (network anomalies). Textbook for universities: textbook]. Moscow: Goryachaya liniya-Telekom Publ., 2013, 220 p. (In Russian)

12. *GOST R 50922—2017. Informatsionnaya tekhnologiya. Upravlenie kachestvom obsluzhivaniya v setyakh svyazi* [GOST R 50922—2017. Information technology. Quality of service management in communication networks]. (In Russian)

13. *GOST R 51323—2009. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti informatsii. Zashchita ot nesanktsionirovannogo dostupa k informatsii* [GOST R 51323—2009. Information technology. Methods and means of ensuring information security. Protection against unauthorized access to information]. (In Russian)

14. *STO RZhD 718048.1—2014. Kompleksnye sistemy upravleniya dvizheniem poezdov. Trebovaniya k proektirovaniyu, stroitel'stvu i ekspluatatsii* [STO RZhD 718048.1—2014. Integrated train control systems. Requirements for design, construction and operation]. (In Russian)

15. *STO RZhD 718048.2—2014. Kompleksnye sistemy upravleniya dvizheniem poezdov. Trebovaniya k sredstvam svyazi i peredachi dannykh* [STO RZD 718048.2—2014. Integrated train control systems. Requirements for communication and data transmission facilities]. (In Russian)

16. Shabalin N. G. *Kontseptsiya informatsionnoy podsistemy mnogourovnevoy sistemy upravleniya i obespecheniya bezopasnosti dvizheniya poezdov (ASU MS); pod red. N. G. Shabalina* [Concept of the information subsystem of the multi-level train control and safety system (ACS MS); edited by N. G. Shabalin]. Moscow: VNIIUP Publ., 2003, 56 p. (In Russian)

17. *GOST RV 51987—2002. Informatsionnaya tekhnologiya. Kompleks standartov na avtomatizirovannye sistemy. Tipovye trebovaniya i pokazateli kachestva funktsionirovaniya informatsionnykh sistem. Obshchie polozheniya* [GOST RV 51987—2002. Information technology. Set of standards for automated systems. Typical requirements and performance indicators for information systems. General provisions]. Moscow: Gosstandart Rossii Publ., 2002, 54 p. (In Russian)

18. *Kontseptsiya obespecheniya kiberbezopasnosti informatsionnykh i upravlyayushchikh sistem v OAO "RZhD" (proekt redaktsiya 1.0)* [Concept of ensuring cybersecurity of information and control systems in JSC Russian Railways (draft version 1.0)]. Moscow: OAO "RZhD", 2013, 285 p. (In Russian)

19. *Model' ugroz i narushitelya bezopasnosti personal'nykh dannykh, obrabatyvaemykh v tipovykh informatsionnykh sistemakh personal'nykh dannykh otrasli* [Model of threats and violators of security of personal data processed in typical information systems of personal data of the industry]. Moscow, 2010, 48 p. (In Russian)

20. *Spetsial'nye trebovaniya i rekomendatsii po tekhnicheskoy zashchite konfidentsial'noy informatsii (STR-K). Reshenie Kollegii Gostekhkomissii Rossii № 7.2/02.03.2001* [Special requirements and recommendations for technical

protection of confidential information (STR-K). Decision of the Board of the State Technical Commission of Russia № 7.2/02.03.2001]. (In Russian)

21. Boldinov A. M., Privalov A. A., Privalov A. A. Matematicheskaya model' kanala upravleniya standarta radiosvyazi GSM-R [Mathematical model of the control channel of the GSM-R radio communication standard]. *Izvestiya Peterburgskogo universiteta putey soobshcheniya* [Proceedings of Petersburg Transport University]. 2022, vol. 19, Iss. 4, pp. 743–751. (In Russian)

22. Privalov A. A., Privalov A. A., Boldinov A. M. Matematicheskaya model' protsessa peredachi komand upravleniya po radiokanalam avtomatizirovannykh sistem [Mathematical model of the process of transmitting control commands via radio channels of automated systems]. *Informatsiya i kosmos* [Information and Space]. 2023, Iss. 4, pp. 71–83. (In Russian)

23. Makhmudov F., Privalov A. et al. Mathematical Model of the Process of Data Transmission over the Radio Channel of Cyber-Physical Systems. Mathematics, 2024, vol. 12, Iss. 10, p. 1452.

24. Privalov A. A., Boldinov A. M., Skudneva E. V., Privalov A. A. Matematicheskaya model' funktsionirovaniya seti peredachi dannykh kiberfizicheskoy sistemy v usloviyakh kibervozdeystviya zloumyshlennika [Mathematical Model of the Operation of the Data Transmission Network of a Cyber-Physical System under the Conditions of an Intruder's Cyber Impact]. *Informatsiya i kosmos* [Information and Space]. 2024, Iss. 3, pp. 74–84. (In Russian)

25. Boldinov A. M. Kompleksnaya model' seti peredachi dannykh kiberfizicheskoy sistemy [Complex model of the data transmission network of a cyber-physical system]. *Aktual'nye problemy infotelekommunikatsiy v nauke i obrazovanii: cbornik nauchnykh statey XIII Mezhdunarodnoy nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii v 4 t., Sankt-Peterburg, 27–28 fevralya 2024 goda* [Actual problems of infotelecommunications in science and education: collection of scientific articles of the XIII International scientific-technical and scientific-methodical conference in 4 volumes, St. Petersburg, February 27–28, 2024]. St. Petersburg: Sankt-Peterburgskiy gosudarstvennyy universitet telekommunikatsiy im. prof. M. A. Bonch-Bruevicha Publ., 2024, pp. 117–121. (In Russian)

26. Yarochkin V. I. *Informatsionnaya bezopasnost': uchebnik dlya studentov vuzov, 2-e izd.* [Information security: textbook for university students, 2nd ed]. Moscow: Akademicheskiy Proekt; Gaudeamus Publ., 2004, 544 p. (In Russian)

Received: March 02, 2025
Accepted: April 10, 2025

Author's information:
Andrey A. PRIVALOV — Dr. Sci. in Military, Professor;
aprivalov@inbox.ru
Aleksey M. BOLDINOV — Postgraduate Student;
23boldinov98@gmail.com