Методология расчета доступности как функция монитора безопасности динамической технической системы*

Е. Ф. Жарко, Е. А. Абдулова, В. Г. Промыслов, К. В. Семенков

Институт проблем управления им. В. А. Трапезникова РАН, Москва, Россия

Аннотация. В работе рассмотрена архитектура функций безопасности динамических технических систем (ДТС) и показана связь с основными задачами монитора безопасности. В работе обоснована доступность как ключевое свойство безопасности ДТС в контексте интеллектуальной среды и предложена риск-ориентированная методология расчета доступности как функция монитора безопасности ДТС в интеллектуальной транспортной среде.

Ключевые слова: функция безопасности, динамическая техническая система, интеллектуальная транспортная среда, доступность, оценка риска.

DOI 10.14357/20718632240306 **EDN** OCGVBA

Введение

Интеллектуальная транспортная среда включает технические и программные решения для повышения эффективности, безопасности и удобства транспортных систем. Ее основные компоненты:

– интеллектуальные транспортные системы (управление и оптимизация транспортных потоков с помощью современных технологий);

– удаленные и беспилотные системы управления транспортными средствами;

– инфраструктурные элементы (датчики движения, информационные табло, системы Vehicle-to-Infrastructure);

– коммуникационные системы (технологии Vehicle-to-Vehicle и связи с инфраструктурой для обмена информацией в реальном времени);

– информационные системы для пользователей (мобильные приложения и онлайн-сервисы о маршрутах и авариях).

Интеллектуальная транспортная среда активно развивается и интегрируется в городскую инфраструктуру, поддерживая концепции умных городов и способствуя повышению качества жизни, безопасности и устойчивому развитию транспортных систем. Развитие динамических технических систем (ДТС) в составе интеллектуальных транспортных систем (ИТС) представляет важное направление современной научно-технической мысли [1]. Городская инфраструктура ежегодно насыщается высокотехнологичными устройствами и системами, обладающими потенциалом значительного повышения эффективности, удобства и безопасности транспортного движения. Однако интеграция

* Исследование выполнено за счет гранта Российского научного фонда № 23-19-00338, https://rscf.ru/project/23-19-00338/

этих систем вместе с преимуществами несет ряд серьезных рисков и вызовов, что подчеркивает важность исследований в области безопасности.

Современные транспортные системы становятся все более сложными и взаимосвязанными и включают множество динамических технических устройств, работающих в режиме реального времени, таких как автоматизированные системы управления движением, интеллектуальные светофоры и датчики мониторинга состояния дорог и трафика. Сбои, отказы, кибератаки на элементы инфраструктуры представляют реальную угрозу безопасности [2]. Автономные системы используют сложные алгоритмы и программное обеспечение (ПО), ошибки в которых могут привести к авариям. Исследования безопасности ДТС помогают обеспечивать надежность функционирования систем, выявлять уязвимости и разрабатывать методы защиты, создавать актуальные стандарты и методы контроля для надежной работы компонентов ДТС, и, что немаловажно, формировать доверие общества к ИТС.

Динамические технические системы изменяются со временем под влиянием внутренних и внешних факторов. Они способны адаптироваться, изменять структуру и функции в ответ на внешние условия. В ИТС такие системы обеспечивают гибкость и оперативность реагирования на потребности транспортной инфраструктуры. Перечислим основные свойства ДТС [3].

– *Изменчивость* - способность изменять состояние и параметры в зависимости от внешних воздействий, включая трафик и погодные условия.

– *Адаптивность* - механизмы корректировки действий на основе данных в реальном времени.

– *Прогнозируемость* - предсказание будущих состояний на основе текущих и исторических данных.

– *Устойчивость* - стабильное функционирование и восстановление после нарушений или сбоев.

– *Сложность* - работа множества взаимосвязанных компонентов и подсистем для достижения общей цели.

ИТС формируют сетевую структуру для обеспечения более безопасного и эффективного передвижения. Важной задачей является взаимодействие всех компонентов системы, что требует постоянного развития технологий и инфраструктуры.

1. Сущность и классификация функций безопасности

В стратегии национальной безопасности Российской Федерации подчеркивается, что приоритеты безопасность в рамках национальных интересов имеют комплексный характер. В настоящей работе внимание сосредоточено на безопасности в контексте информационного уровня ДТС, что обосновано значимостью информации для ДТС как интеллектуальной транспортной системы.

Функции безопасности (ФБ) в транспортных системах заключаются в выполнении мер, защищающих пользователей и инфраструктуру от угроз и минимизирующих последствия реализации этих угроз. Они включают технические и организационные меры процедуры и технические решения для защиты людей, имущества и информации от преступных действий, террористических актов, аварий и стихийных бедствий, обеспечивая безопасную эксплуатацию транспортных средств и инфраструктуры. Функции безопасности требуют постоянного внедрения новых технологий и адаптации к новым угрозам. На Рис. 1 представлена архитектура функций безопасности в концепции транспортных систем.

2. Функции безопасности и монитор безопасности ДТС в интеллектуальной транспортной среде

Перечислим основные функции безопасности.

1. Обнаружение угроз направлено на идентификацию возможных угроз безопасности в реальном времени. Угрозы могут быть обнаружены на ранних стадиях, благодаря различным датчикам и системам мониторинга, например:

– системам видеонаблюдения с функцией распознавания лиц и объектов, которые могут выявить подозрительные действия или ситуации;

– системам анализа сетевого трафика с применением методов машинного обучения,

которые могут выявить аномалии трафика, указывающие на кибератаки.

2. Предотвращение угроз подразумевает различные мероприятия, направленные на минимизацию рисков, связанных с обнаруженными угрозами, например:

– *контроль доступа* с использованием биометрии, умных карт и других методов аутентификации для управления доступом к критически важным системам и данным;

– *шифрование данных* для защиты конфиденциальной информации в процессе передачи и при хранении.

3. Реагирование на инциденты включает в себя ряд шагов по контролю и минимизации последствий инцидентов безопасности, как то:

– *аварийное оповещение* – мгновенная отправка оповещений соответствующим службам и пользователям о возникшей угрозе или инциденте;

– *активные меры реагирования*, когда показания монитора безопасности могут использоваться в качестве входных данных для систем управления, например, автоматизированные системы могут временно блокировать доступ или перенаправлять потоки данных для предотвращения распространения угрозы.

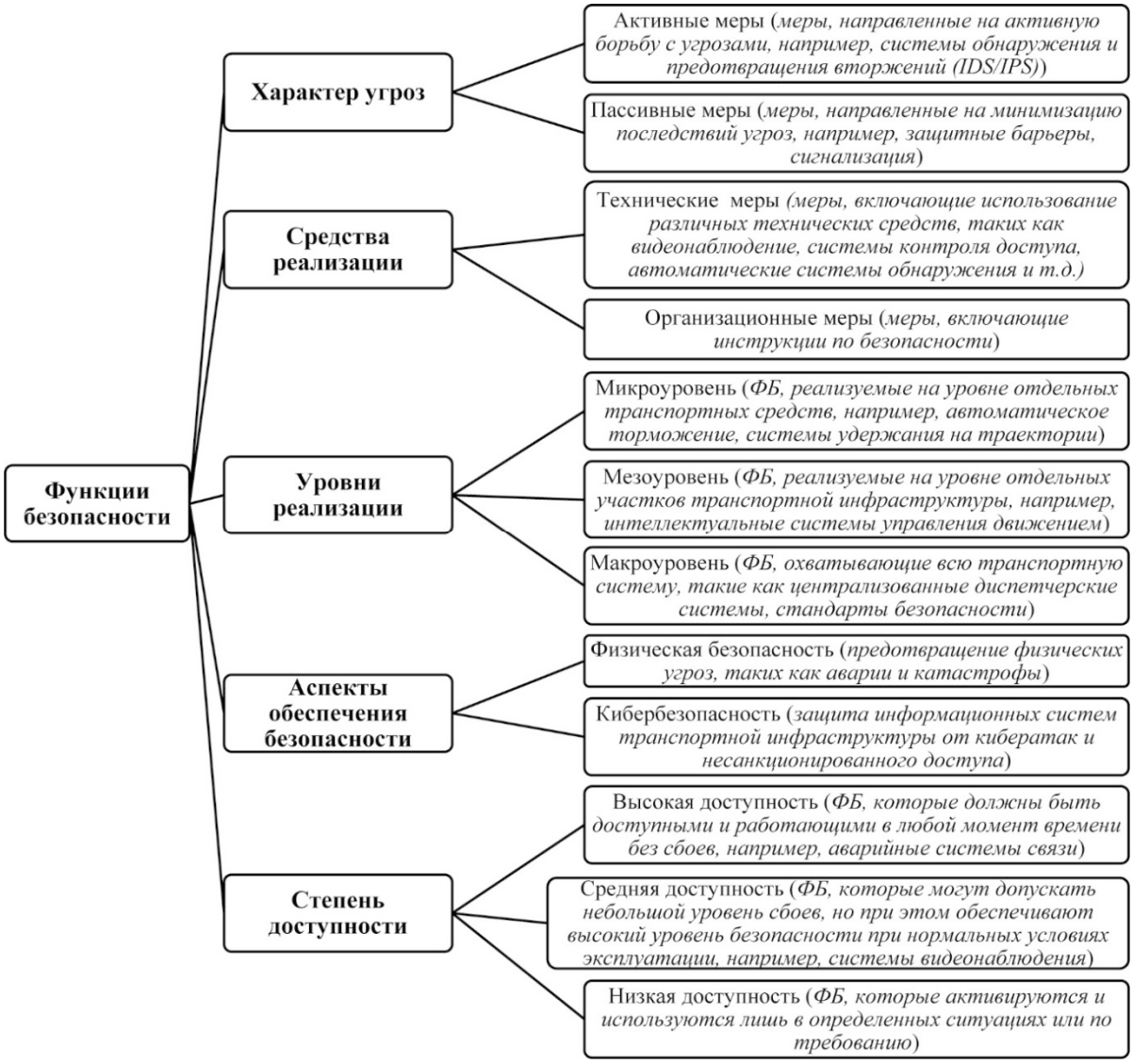

Рис. 1. Архитектура функций безопасности ДТС

4. Восстановление после инцидентов включает мероприятия по восстановлению нормальной работы системы после инцидента, как то:

– *регулярное резервное копирование и отработанные процедуры восстановления информационной инфраструктуры ИТС,* чтобы обеспечить функционирование ДТС при устранении последствий отказа;

– *анализ инцидентов* для выявления их причин и разработки мер по предотвращению повторных случаев.

Для обеспечения безопасности в динамической технической системе необходим постоянный и всесторонний мониторинг. Это позволяет своевременно выявлять угрозы и принимать оперативные меры для их нейтрализации.

ИТС включает в себя системы мониторинга, относящиеся к двум видам:

инфраструктурный мониторинг - отслеживание состояния транспортной инфраструктуры, включая дорожные покрытия, мосты и туннели;

транспортный мониторинг - контроль состояния транспортных средств, включая их местоположение, скорость, траекторию и техническое состояние.

Применение современных технологий позволяет осуществлять высокоэффективный мониторинг безопасности. К таким технологиям относятся:

интернет вещей - интеграция данных от множества недорогих беспроводных датчиков и устройств позволяет собирать и обрабатывать детализированную информацию о ДТС;

большие данные и анализ данных - хранение и анализ огромных массивов данных для выявления и прогнозирования потенциальных угроз.

Мониторинг может классифицироваться по различным признакам.

Проактивный мониторинг предназначен для предотвращения инцидентов до их возникновения путем прогнозирования и анализа паттернов поведения.

Реактивный мониторинг сосредоточен на выявлении и разрешении уже произошедших инцидентов.

Использование передовых методов мониторинга безопасности играет ключевую роль в эффективном управлении ИТС. К ним относятся:

– *аналитика машинного обучения и искусственного интеллекта* для анализа данных и обнаружения аномалий в реальном времени;

– *глубокое обучение и нейронные сети* для распознавания и предсказания угроз [4].

Безопасность и мониторинг безопасности являются основополагающими компонентами интеллектуальной транспортной среды. Для обеспечения надежной и безопасной работы подобных систем важно применять интегрированный подход, включающий современные технологии и методы управления. Внедрение таких решений помогает минимизировать риски, связанные с безопасностью, и обеспечивает надежное функционирование транспортной системы.

Монитор безопасности в интеллектуальной транспортной среде должен отображать широкий спектр функций безопасности, чтобы обеспечить всесторонний контроль и быструю реакцию на любые инциденты. В силу важности функций безопасности концепция монитора безопасности должна закладываться на самых ранних этапах разработки ДТС. На Рис. 2 представлены основные задачи, которые может выполнять монитор безопасности, и приведена их связь с архитектурой функций безопасности (Рис. 1). Дополнительно в мониторе безопасности должны быть предусмотрены возможности для настроек и адаптации системы в зависимости от меняющихся условий и требований безопасности.

Таким образом, полнофункциональный монитор безопасности должен обеспечивать оператора системы полезной и актуальной информацией для эффективного управления безопасностью в реальном времени и оперативной реакции на угрозы.

3. Доступность как ключевое свойство безопасности ДТС

Общие подходы к безопасности ДТС как цифровой системы обработки информации можно выразить в рамках классической модели «Конфиденциальность-Целостность-Доступность» (КЦД) [5], которая включает в себя названные три основные свойства. Если необходимо, можно использовать расширенные модели (например, модель Маконахи [6]), которые дают более развернутое атрибутирование

Обобщенные задачи МБ	Результаты выполнения задачи	Архитектура ФБ				
		Характер угроз	Средства реализации	Уровни реализации	Аспекты обеспечения безопасности	Степень доступности
Мониторинг состояния системы	**Общее состояние системы**: показатели функционирования ключевых компонентов системы в реальном времени **Диагностические параметры**: информация о текущем состоянии оборудования, включая наличие ошибок и аномалий **Журнал событий**: хронология событий и действий для анализа и принятия решений.	технические сбои, ошибки конфигурации, перегрузка ресурсов	пассивные технические меры (ПО мониторинга, показания датчиков, протоколы событий)	все уровни: аппаратный, программный, сетевой	кибербезопасность (доступность, целостность)	высокая (постоянный мониторинг)
Обнаружение угроз в реальном времени	**Аналитика видеонаблюдения:** трансляция и анализ видеопотока с камер, включая распознавание лиц и регистрационных знаков. **Анализ сетевого трафика:** данные о состоянии сетевого трафика и обнаруженных угрозах, таких как DDoS-атаки или попытки несанкционированного доступа. **Уведомления и оповещения**: автоматические уведомления о выявленных угрозах и инцидентах безопасности. **Интерфейс для ответных действий**: моментальная возможность отправки ответных сигналов	вредоносное ПО, сетевые атаки, несанкционированный доступ	активные и пассивные технические меры (системы обнаружения/предотвращения вторжений (IDS/IPS), антивирусное ПО, анализ поведения пользователей и сущностей (UEBA)	микро- и мезоуровень (сетевой, узловой, приложений)	кибербезопасность (конфиденциальность, целостность, доступность)	высокая (обнаружение в режиме реального времени)
Контроль доступа	**Система мониторинга доступа**: информация о текущих попытках доступа, успешных и неуспешных аутентификациях. **Контроль уровней доступа**: отображение текущих активных уровней доступа и их владельцах.	несанкционированный доступ, кража данных, нарушение политик безопасности	пассивные технические меры (системы идентификации и аутентификации, управление правами доступа, журналы доступа)	микро-, мезо-, макроуровни (физический, сетевой, приложений, данных)	кибербезопасность (конфиденциальность, целостность)	высокая (постоянный контроль)
Мониторинг транспортных средств	**Геолокация**: отображение в реальном времени координат, скоростей и траекторий транспортных средств. **Состояние транспортных средств**: информация о техническом состоянии, включая сообщения об ошибках и диагностические данные.	угон, несанкционированное использование, нарушение маршрутов	пассивные технические (GPS-трекинг, системы удаленного управления, датчики состояния транспортных средств)	микро- и мезоуровни (физический, сетевой)	физическая безопасность, контроль использования активов	высокая (непрерывный мониторинг в режиме реального времени)
Шифрование и защита данных	**Статус шифрования**: текущие статусы шифрования данных в системе. **Проверка целостности данных**: информация о проверках целостности данных и результаты этих проверок.	несанкционированный доступ, утечка данных	пассивные технические меры (алгоритмы шифрования, управление ключами, контроль доступа)	микроуровень, мезоуровень (аппаратный, программный, сетевой)	кибербезопасность (конфиденциальность, целостность)	постоянная защита данных
Прогнозирование и аналитика	**Прогнозирование угроз:** модели и прогнозы на основе аналитики больших данных и машинного обучения. **Статистические отчеты**: анализ прошлых событий и трендов для расследования инцидентов и повышения безопасности. **Инструменты анализа данных**: возможность детализации и углубленного анализа данных, визуализация данных с использованием графиков и диаграмм	новые и неизвестные угрозы, сложные атаки	пассивные технические меры (машинное обучение, анализ больших данных, системы SIEM)	мезо- и макроуровни (программный, сетевой)	физическая безопасность, кибербезопасность (конфиденциальность, целостность, доступность)	средняя (непрерывный анализ и прогнозирование)
Интеграция с другими системами	**Синхронизация с внешними системами безопасности**: Информация о взаимодействии с полицейскими, спасательными и медицинскими службами. **Протоколы обмена данными**: Информация о текущем состоянии протоколов обмена между различными системами.	сложные многовекторные атаки, скоординированные угрозы	пассивные технические меры (API, протоколы обмена данными, единая консоль управления)	мезо- и макроуровни (сетевой, программный)	кибербезопасность (комплексная защита, централизованное управление)	средняя (постоянная интеграция и обмен данными)

Рис. 2. Связь задач монитора безопасности с архитектурой ФБ

информационной безопасности, однако, как показывает практика, для базового анализа в основном достаточно модели КЦД. Далее мы будем опираться на нее.

Свойства безопасности не всегда могут анализироваться независимо, они могут конфликтовать или дополнять друг друга. Например, строгие меры контроля доступа, такие как многоуровневая аутентификация, могут затруднить доступ легальных пользователей, снижая удобство и скорость доступа. Приоритетность свойств триады КЦД также может варьироваться в зависимости от предметной области. Сначала наиболее высокий приоритет получила конфиденциальность, что отразилось в название модели, но для ДТС доступность выходит на первое место. Доступность играет ключевую роль в безопасности транспортных систем по следующим причинам:

– **Непрерывность операций.** Транспортные системы зависят от непрерывности работы для обеспечения безопасности. Так, например, системы управления движением и сигнальные системы должны быть всегда доступны для предотвращения аварий.

– **Реальное время и взаимодействие с человеком.** Доступность определяется необходимостью обработки информации в темпе характерного времени динамических процессов в ДТС, связанных с физическими объектами.

– **Требования к доверию.** Высокая доступность ДТС повышает уровень доверия со стороны пользователей, что, в свою очередь, способствует стабильной и безопасной эксплуатации транспортной инфраструктуры.

Поддержание высокой доступности в транспортных системах требует сочетания технологических решений (резервные системы, отказоустойчивые архитектуры), организационных процедур (планы восстановления, управление инцидентами) и управления на основе регулярной оценки риска для ДТС.

Доступность в контексте безопасности во многом переплетается с надежностью [7], поэтому нужно дать определение термина доступность, которое используется в данной работе и в предлагаемой базовой модели управления рисками нарушения доступности в ДТС.

Определение. Доступность – это способность системы или ее компонента выполнить требуемое действие в заданных условиях в заданный момент времени, если предоставлены необходимые внешние ресурсы.

Данное определение аналогично определению доступности для промышленных сетей [8] с той разницей, что в зависимости от конкретной задачи рассматриваем доступность всей ДТС или ее локальную форму в виде доступности отдельного компонента.

Для обеспечения доступности необходимо научиться ее измерять и оценивать риск ее нарушения. Для этого определим базовую модель риска нарушения доступности и рассмотрим возможный вид целевой функции для минимизации риска нарушения доступности ДТС.

4. Базовая модель риска нарушения доступности

Формальное описание системы. Будем рассматривать ДТС как систему, обладающую свойствами ограниченности, функциональности и вложенности.

Пусть ДТС состоит из конечного множества субъектов $S = \{s_i\}$, $i = \overline{1,n}$, выполняющих конечный набор функций $\Phi = \{\phi_j\}$, $j = \overline{1,m}$. Для каждой функции определено множество субъектов системы, участвующих в выполнении функции ϕ_i, через отображение:

$$Q : S \to S. \quad (1)$$

Тогда система может быть описана кортежем:

$$\Xi = \langle \Phi, S, Q \rangle. \quad (2)$$

Поскольку ДТС является динамической системой, то основные элементы системы Ξ, за исключением, может быть, набора функций Φ, могут меняться во времени, и описание системы должно включать в качестве параметра время. Поэтому ограничимся рассмотрением системы на интервале времени, когда кортеж Ξ не меняется.

Определим для такой системы базовую модель управления риском доступности. Для этого применим базовую модель управления рисками информационных систем [9], переформулировав ее с учетом внешнего и внутреннего контекста ДТС.

Предположим, что система Ξ спроектирована таким образом, что функции связаны друг с другом только посредством общих субъектов, реализующих функции в составе системы. Например, субъект может реализовывать одновременно функцию промежуточного хранения видеоданных других субъектов для передачи в монитор безопасности и функцию управления другими субъектами в группе.

Отметим, что, вообще говоря, субъекты в S могут оказывать влияние друг на друга. В самом деле, если более одного субъекта задействовано в выполнении какой-либо функции, то, с точки зрения функционального контекста ДТС, они связаны. Поэтому будем считать, что один субъект может оказывать определенное воздействие на другие субъекты, например, меняя его состояние или, что более важно для нас, осуществляя передачу риска.

Предположим, что воздействие одного субъекта на другой пассивно, т.е. ограничено рамками решений, заложенных проектировщиком системы, и известно или, по крайней мере, его можно потенциально оценить. Допущение о пассивности воздействия фактически предполагает отсутствие внутреннего нарушителя в модели угроз.

Под ресурсом будем понимать любой делимый, измеримый актив. Ресурсы не обязательно должны быть материальными, как, например, топливный ресурс транспортного средства. Это могут быть логические ресурсы, например, время жизни системы до сброса ее параметров в начальное состояние. Далее, для сокращения выкладок, будем предполагать, что ресурс – это скаляр, хотя все выкладки легко расширяются, если выделяемый каждому субъекту ресурс является вектором. Для задачи управления риском доступности предположим, что:

1) система обладает некоторым ресурсом $X \geq 0$, который распределяется на части $\{x_i\}$, $x_i \geq 0$, $\sum_{i=1}^{n} x_i \leq X$, между субъектами системы Ξ, чтобы управлять доступностью. Ресурс X всегда распределяется целенаправленно, его распределение является инструментом управления доступностью.

2) На систему действуют некоторые внешние, деструктивные силы, обладающие ресурсом $Y \geq 0$, который также можно разместить на субъектах: $\{y_i\}$, $y_i \geq 0$, $\sum_{i=1}^{n} y_i \leq Y$. Деструктивные силы могут иметь различную природу. Это могут быть как природные факторы, например, погодные условия, так и целенаправленно действующие нарушители, например, хакеры, пытающиеся нарушить функционирование ДТС. Ресурс Y в зависимости от деструктивного воздействия может быть распределен как случайно, так и целенаправленно.

3) Конфигурация Q не подвержена деструктивному воздействию.

Таким образом, каждому субъекту s_i системы Ξ поставлена в соответствие пара величин (x_i, y_i), определяющих ресурс:

$$P: S \to \{X, Y\}. \tag{3}$$

Принятое предположение о том, что субъекты могут воздействовать друг на друга, означает, что риск для каждого отдельного субъекта (локальный риск) может зависеть от риска для других субъектов, т.е. локальный риск для субъекта $s_i \in S$ будет зависеть от векторов $x = \{x_i\}$ и $y = \{y_i\}$.

Определение: Функция локального риска – это вещественная функция $\rho_i(x_1,...,x_n; y_1,...,y_n)$, определенная для каждого субъекта s_i системы Ξ и зависящая от распределения ресурсов по субъектам. По аналогии с работой [9] примем, что локальные функции риска удовлетворяют условиям неотрицательности, монотонности по отношению к ресурсам и ограниченности сверху и снизу.

*Определени*е: Функция риска, связанного с нарушением доступности для функции системы $\phi_j \in \Phi$ – это функция вида:

$$\tilde{\rho}_j(x, y, Q) = \prod_{i \in Q_j} \rho_i(\cdot,\cdot,\cdot), \; j = \overline{1,n}, \tag{4}$$

где $Q_j \subseteq S$, подмножество субъектов системы Ξ, участвующих в выполнении функции системы ϕ_j, а Π – монотонное преобразование.

Сопоставим каждому дискретному состоянию системы Ξ вектор функций риска нарушения доступности системы с учетом конфигурации системы Q:

$$\rho_{\Sigma}(x,y,Q)=\{\tilde{\rho}_j(x,y,Q)\},\ j=\overline{1,m}. \quad (5)$$

Кроме собственно расчета рисков, можно при текущих вводных сформулировать задачу минимизации рисков, которую монитор безопасности может решать и выдавать результаты решения в качестве рекомендаций в систему управления ДТС.

Введем обозначения:

$$\mathrm{X}(X)=\{(x_i)\}\in\mathbb{R}_n : x_i\geq 0,\ i\in\mathbb{N},\ \sum_{i=1}^{n}x_i\leq X$$

– множество допустимых распределений ресурса X между субъектами в системе Σ;

$$\Upsilon(Y)=\{(y_i)\}\in\mathbb{R}_n : y_i\geq 0,\ i\in\mathbb{N},\ \sum_{i=1}^{n}y_i\leq Y$$

– множество допустимых распределений ресурса Y между субъектами в системе Σ;

$Q'=\{Q\}$ – множество допустимых конфигураций системы Σ.

Тогда целевая функция управления риском Θ при обеспечении доступности системы Ξ может быть сформулирована в виде выбора таких распределений ресурса X и конфигурации Q с учетом знаний о распределении деструктивного ресурса Y, при которых норма вектор-функций риска нарушения доступности системы минимальна (5):

$$\Theta=\inf_{x\in\mathrm{X},Q\in Q'}\left\|\rho_{\Sigma}(x,y,Q)\right\|_{y\in\Upsilon}. \quad (6)$$

Мы полагаем, что знаем, как деструктивный ресурс распределен по субъектам в системе, и что «позитивное» (со стороны системы) управление риском посредством перераспределения деструктивного ресурса невозможно.

Базовая модель оценки риска нарушения доступности не учитывает в явном виде возможность дублирования функций в системе, вместе с тем дублирование является типичным приемом повышения надежности для ДТС. Для учета дублирования функций сформулируем следующее утверждение.

Утверждение: Пусть ДТС – это система вида $\Xi=\langle\Phi,S,Q\rangle$, и пусть функция $\phi_j\in\Phi=\{\phi_j\}$, $j\in\mathbb{N}$ дублируется l раз таким образом, что для любой функции один субъект системы может быть задействован в выполнении только одного дубля этой функции. Тогда для j-ой функции субъекты системы, участвующие в выполнении каждого дубля, образуют непересекающиеся подмножества множества S, и риск для j-ой функции может быть записан как:

$$\tilde{\rho}_j(x,y,Q)=\inf_{1\leq i\leq l}\left(\inf_{S_i\subset S}\left(\tilde{\rho}_j(x_i,y_i,Q)\right)\right). \quad (7)$$

Доказательство утверждения (7) очевидно и следует из того, что утверждение является формой формулы Фубини [10].

5. Практические аспекты расчета доступности

Рассмотрим конкретные виды функций локального риска, а также их взаимодействие при определении риска нарушения доступности (4). Расчет доступности системы включает этапы от определения требований до анализа данных, используя подходы, алгоритмы и математические модели. Текущие подходы к оценке доступности включают:

1) *Аналитический подход* - использование математического анализа для определения времени безотказной работы и возможных простоев:

– рассмотрение архитектуры системы: анализ компонентов системы и их взаимосвязей;

– оценка надежности компонентов.

2) *Статистический подход* - анализ эмпирических данные из предыдущей эксплуатации системы:

– сбор данных: регистрация событий отказов и времени восстановления;

– анализ данных: использование статистических методов для вычисления показателей доступности.

3) *Моделирование и симуляция* - использование моделей для имитации работы системы и оценки ее доступности. Фактически, в оценке риска доступности используются весь огромный спектр известных моделей. Укажем наиболее часто используемые на практике модели:

– марковские модели для анализа переходов состояний системы;

– теория массового обслуживания (ТМО) и ее приложения для вычислительных систем [11];

– теория сетевых исчислений (англ. Network Calculus) [12].

В зависимости от подхода, значения функции локального риска будут определяться через соответствующие показатели, например: отношение времени безотказной работы (или полезного времени) к общему времени работы, включая время простоев: $A = t_{up} / \left(t_{up} + t_{dow} \right)$, где t_{up} – время безотказной работы, t_{dow} – время простоя, вероятность нежелательного события для доступности в компоненте и т.д.

Кроме вида функции локального риска, важен переход от локального риска субъекта системы к риску нарушения доступности конкретной функции системы. Так же как в предыдущем случае, невозможно полностью перечислить все применимые подходы и методы, выделим основные, которые используются на практике. Для многокомпонентных систем возможные композиции функций локального риска при выполнении j-ой функции в системе могут задаваться, например, на основе доступности отдельных компонентов, работающих параллельно или последовательно.

– Последовательная система:

$$\tilde{\rho}_j \left(x, y, Q \right) = \rho_1 \left(\cdot, \cdot, \cdot \right) \times \rho_2 \left(\cdot, \cdot, \cdot \right) \times ... \times \rho_n \left(\cdot, \cdot, \cdot \right). \quad (8)$$

– Параллельная система:

$$\tilde{\rho}_j \left(x, y, Q \right) = \inf \left(\rho_i \left(\cdot, \cdot, \cdot \right) \right). \quad (9)$$

Источники данных для расчета локального риска нарушения доступности так же разнообразны, однако, как минимум, для ДТС они включают:

– *Мониторинг показателей системы в реальном времени* - время прохождения данных между субъектами системы, характеристики потоков данных.

– *Журналы и логирование* - аудит журналов, содержащих информацию о текущих доступах в системе, времени работы и простоя, отказах и их причинах.

– *Тестирование искусственных отказов* - данные, полученные в ходе преднамеренного создания условий для отказа системы.

Формирование конкретных функций локального риска, а также учет их взаимодействия при определении риска нарушения доступности, так же как и выбор методов мониторинга доступности, требуют всестороннего анализа ДТС. Основная цель – обеспечить надежное функционирование системы, минимизировать простои и удовлетворить требованиям пользователей.

6. Примеры оценки риска доступности ДТС

Пример 1. Этот пример адаптирован из стандарта системной инженерии по информационной безопасности [13]. Пусть анализируется ДТС, где выделенный субъект подключен к сети интернет для удаленного доступа. Данный субъект реализует единственную функцию принятия заказа и дальнейшего распределения его между субъектами.

Пусть для системы предусмотрено максимальное время непрерывной эксплуатации T_{MAX}, после чего состояние системы обнуляется, и она перезапускается. Предположим, что выделенный элемент подвержен угрозам типа «отказ в обслуживании» с применением атаки «SYN-flooding». Атака заключается в передаче из сети интернет на атакуемый субъект большого количества специально сформированных TCP пакетов с установленным SYN-флагом. Пакеты вызывают переполнение таблицы адресов абонентов, ожидающих установления связи с системой, и, как результат, нарушение доступности ДТС для легальных удаленных абонентов. Оценим риск нарушения доступности при реализации данной атаки, применяя подходы теории массового обслуживания [11].

Данная атака может быть описана в рамках модели ТМО очередью ограниченной длины. Длина очереди соответствует размеру таблицы, хранящей адреса абонентов, ожидающих установления связи. Атакуемый элемент системы, если происходит переполнение таблицы, отказывает и автоматически перезапускается после истечения фиксированного промежутка времени. Вероятность того, что ПО атакуемого элемента в момент времени t перестанет принимать новые пакеты информации, в результате чего атака будет реализована, определяют из соотношения:

$$p(t) = 1 - \exp\left(\lambda_{pkt} - t/J_{tbl}\right).$$

где λ_{pkt} – интенсивность поступления TCP-пакетов с установленным флагом SYN; J_{tbl} – предельный размер таблицы, хранящей адреса абонентов в очереди на установления связи. В соответствии с моделью (2), ресурсами системы (3) будем считать размер таблицы J_{tbl} и деструктивный ресурс λ_{pkt}. Так как по условию атаке подвергается единственный субъект системы, подключенный к интернету, выполняющий единственную анализируемую функцию, то все другие локальные риски будут равны нулю и управление риском (6) сводится к обеспечению доступности единственного субъекта, на который осуществляется атака.

Положим, что в отсутствие дополнительных мер защиты риск нарушения доступности для функции распределения заказов прямо пропорционален вероятности отказа субъекта, принимающего заказы за максимальное время непрерывной эксплуатации ДТС. Тогда риск нарушения доступности функции принятия и распределения заказа:

$$\rho_{\Sigma}(x, y, Q) \sim \int_0^{T_{MAX}} p\left(J_{tbl}, \lambda_{pkt}, Q, t\right) dt.$$

Пример 2. Рассмотрим ДТС, в которой субъекты обмениваются друг с другом потоковыми видеоданными. Множество субъектов системы, участвующих в выполнении функции (1), задано потоками, которым они принадлежат $F = \{f_1 ... f_3\}$. Потоки в системе заданы топологией Q_1 и маршрутами $\mathrm{P} = \{\mathrm{P}_1 ... \mathrm{P}_3\}$, в виде последовательностями ребер в графе G (Рис. 3):

– $\mathrm{P}_1 = \{(s_1, s_2), (s_2, s_3)\}$,

– $\mathrm{P}_2 = \{(s_2, s_3)\}$,

– $\mathrm{P}_3 = \{(s_3)\}$.

Все субъекты в системе реализуют одинаковую дисциплину обработки потоков - без задержки с постоянной скоростью C. Ограничения на видеопотоки $F = \{f_1 ... f_3\}$ представлены в виде линейных огибающих $\alpha(t) = rt + b,\ i = \overline{1,3}$ с неравномерностью потока b и скоростью r. Система выполняет функции

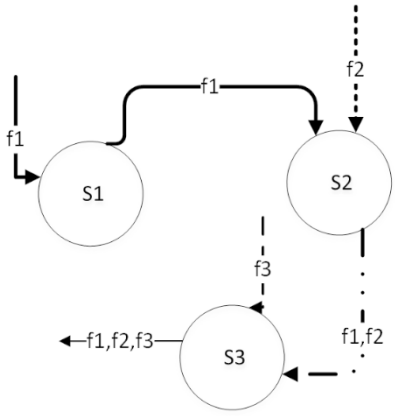

Рис. 3. Граф G с маршрутами потоков ДТС примера

обработки $\phi_j \in \Phi = \{\phi_j\},\ j = \overline{1,3},$ каждая функция в системе выполнятся субъектами, принадлежащими потоку в F.

Для каждого i-ого субъекта в системе, который участвует в выполнении j-ой функции, определим пару $\left(d_{i,j}, d_{i,j\max}\right)$, где $d_{i,j}$ – актуальная задержка в субъекте при обработке информации, $d_{i,j\max}$ – максимально допустимая задержка в субъекте при выполнении функции. Риск нарушения доступности мы считаем приемлемым, если задержка при данной конфигурации системы Q и производительности субъектов и параметров обрабатываемых потоков не превосходит максимально допустимой задержки, определенной в задании на каждый субъект.

Тогда, функция риска нарушения доступности j-ой функции:

$$\tilde{\rho}_j(x, y, Q) = \inf_{i \in Q_j \subseteq S} l\left(d_{i,j}, d_{i,j\max}\right), \qquad (10)$$

где $l\left(d, d_{\max}\right)$ – барьерная функция:

$$l\left(d, d_{\max}\right) = \begin{cases} 1, & 0 \le d \le d_{\max}, \\ 0, & d > d_{\max}. \end{cases}$$

Заметим, что вид функции риска (10) является формой последовательного соединения субъектов (8). Предположим, что в системе отсутствуют потери, и что видеопоток в промежуточных субъектах системы на пути от источника к адресату не дополняется информацией. В этом случае для решения задачи можно применить теорию сетевых исчислений [10].

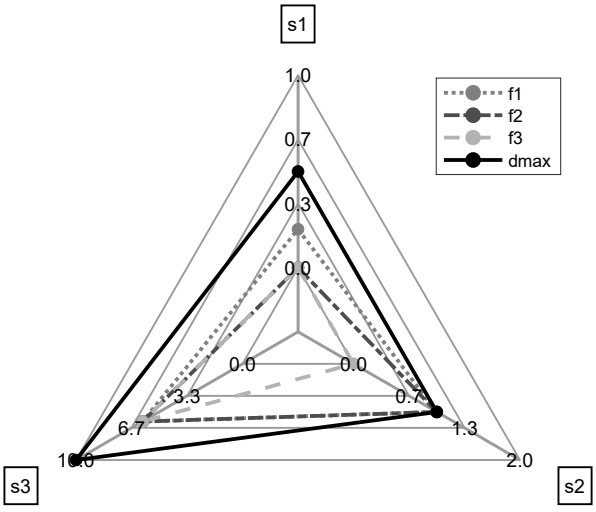

Рис. 4. Максимальная задержка (с) для потоков в системе

Неравномерность потока $i=\overline{1,3}$ после обработке на m-ом субъекте для равна [14]:

$$\delta_i^m = \delta_i^{m'} + r\frac{\sum_{j\in m, j\neq i}\delta_j^{m'}}{C-\sum_{\in m, j\neq i} r'},$$

где $\delta_i^{m'}$ неравномерность потока $i=\overline{1,3}$ на входе субъекта.

Пусть для системы (Рис. 3) заданы следующие параметры: $C=100$ кБ/с, $r=30$ кБ/с, $b=20$ кБ, ограничения по задержке для серверов 1-3 $d_{\max}=\{0.5;1;10\}$ с. Результаты расчета приведены на Рис. 4. Видно, что вектор-функция нарушения доступности с учетом всех 3-х функций системы (10) – это нулевой вектор: $\rho_\Sigma(x,y,Q)=\{0;0;0\}$. Соответственно, целевая функция управления риском будет равна нулю и риск нарушения доступности для всех функций, которые реализуются системой, равен нулю.

Заключение

Обеспечение безопасности динамических технических систем (ДТС) в интеллектуальной транспортной среде — одна из ключевых задач, возникающих при создании и эксплуатации этих систем. Для решения этой задачи система должна, помимо прямого назначения, выполнять функции безопасности, т.е. реализовывать технические и организационные меры для защиты людей, имущества и информации от преступных действий, террористических актов, аварий и стихийных бедствий. В таком случае система управления ДТС в интеллектуальной транспортной среде должна обладать средствами контроля встроенных в нее функций безопасности. Набор средств контроля функций безопасности, реализованных в рамках цифровой подсистемы управления, мы называем монитором безопасности.

В соответствии со стратегией национальной безопасности Российской Федерации, безопасность имеет многоплановый характер. В работе внимание сосредоточено на безопасности в контексте информационного уровня ДТС. Безопасность в этом случае сводится к свойствам классической модели КЦД (конфиденциальность-целостность-доступность), и основное внимание, в соответствии с современными подходами [8], уделяется свойству доступности. Также в соответствии с современными подходами и нормами для контроля доступности предлагается использовать риск-ориентированный подход.

В работе приведена архитектура функций безопасности (Рис. 1), функции безопасности структурированы по различным критериям. Для обеспечения полноты контроля функций безопасности было проведено сопоставление основных задач монитора безопасности и функций безопасности (Рис. 2). Чтобы представить на мониторе безопасности риски нарушения доступности функций системы было дано формальное описание базовой модели доступности ДТС,

введены функции локального риска, риска нарушения доступности для отдельной функции системы, риска нарушения доступности для всей системы, целевая функция управления риском. В функциях риска учитывается распределение ресурсов системы и деструктивных воздействий различной природы.

Монитор безопасности, помимо расчета и отображения функций риска, может решать задачу минимизации риска нарушения доступности (5) и выдавать в систему управления ДТС рекомендации по оптимальному для минимизации риска распределению ресурсов ДТС в ИТС.

Рассмотренные в работе виды функций риска и примеры расчета функций риска для системы иллюстрируют предлагаемый риск-ориентированный подход.

Предлагаемые классификация функций безопасности и определение функции риска могут использоваться при создании мониторов безопасности динамических технических систем в интеллектуальной транспортной среде.

Литература

1. Gaidar S.M., et al. Mathematical Method for Optimising the Transport and Logistics Industry // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russian Federation. – 2022. – Pp. 1–5.
2. Jharko E., et al. Some Safety Issues in an Intelligent Transport Environment // 2023 International Russian Automation Conference (RusAutoCon), Sochi, Russian Federation. – 2023. – Pp. 453–459.
3. Blanchard, B.S., Fabrycky W. Systems Engineering and Analysis. – 5th Edition. – Prentice-Hall International Series in Industrial and Systems Engineering. 2013. 846 p.
4. Mynuddin M., et al. Automatic Network Intrusion Detection System Using Machine Learning and Deep Learning // 2024 IEEE International Conference on Artificial Intelligence and Mechatronics Systems (AIMS), Bandung, Indonesia. – 2024. – Pp. 1–9.
5. Smith R.E. A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles // IEEE Security & Privacy. – 2012. – 10(6). – Pp. 20–25.
6. Maconachy W.V., et al. A Model for Information Assurance: An Integrated Approach // 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY. – 2001. – Pp. 306–310.
7. ГОСТ Р 27.102-2021. Надежность в технике. Надежность объекта. Термины и определения. Термины и определения. – М.: Российский институт стандартизации. – 2021. – 40 с.
8. ГОСТ Р 56205-2014. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. – М.: Стандартинформ. – 2014. – 77 с.
9. Калашников А.О., Аникина Е.В. Модели управления информационными рисками сложных систем // Информация и безопасность. – 2020. – Т. 23, №2(4). – С. 191-202.
10. Le Boudec J.-Y., Thiran P. Network Calculus: A Theory of Deterministic Queuing Systems for the Internet // Lecture Notes in Computer Science. –2001. – Vol. 2050. – 274 p.
11. Вишневский В.М. Теоретические основы проектирования компьютерных сетей – М.: Техносфера. – 2003. – 512 с.
12. Промыслов В.Г., Семенков К.В. Применение метода Network Calculus для расчета временных характеристик систем управления с циклическим алгоритмом работы // Проблемы управления. – 2021. – №4. – С. 50-65.
13. ГОСТ Р 59346-2021. Системная инженерия. Защита информации в процессе определения системных требований. – М.: Стандартинформ. – 2021. – 66 с.
14. Cruz R.L. A calculus for network delay. II. Network analysis // IEEE Transactions on Information Theory. – 1991. – Vol. 37(1). – Pp. 132-141.

Жарко Елена Филипповна. Институт проблем управления им. В. А. Трапезникова РАН, Москва, Россия. Кандидат технических наук, старший научный сотрудник. Область научных интересов: моделирование, верификация, системы поддержки принятия решений, робототехника. E-mail: zharko@ipu.ru

Абдулова Екатерина Алексеевна. Институт проблем управления им. В. А. Трапезникова РАН, Москва, Россия. Научный сотрудник. Область научных интересов: моделирование, информационная безопасность, верификация, системы поддержки принятия решений, робототехника. E-mail: consoft@ipu

Промыслов Виталий Георгиевич. Институт проблем управления им. В. А. Трапезникова РАН, Москва, Россия. Кандидат физико-математических наук, ведущий научный сотрудник. Область научных интересов: моделирование, промышленная автоматизация, робототехника, программные системы. E-mail: vp@ipu

Семенков Кирилл Валерьевич. Институт проблем управления им. В. А. Трапезникова РАН, Москва, Россия. Кандидат физико-математических наук, старший научный сотрудник. Область научных интересов: кибербезопасность, имитационное моделирования, промышленная автоматизация. E-mail: semenkov@ipu.ru

Methodology for Calculating Availability as a Function of the Safety Monitor of a Dynamic Technical System

E. Ph. Jharko, E. A. Abdulova, V. G. Promyslov, K. V. Semenkov

V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia

Abstract. The paper considers the classification of safety functions of dynamic technical systems (DTS) according to various criteria and shows the connection with the main tasks of a safety monitor. It presents accessibility as a critical property of DTS safety and proposes a risk-based methodology for calculating accessibility as a function of DTS safety in an intelligent transport environment.
Keywords: safety function, dynamic technical system, intelligent transport environment, accessibility.

DOI 10.14357/20718632240306 **EDN** OCGVBA

References

1. Gaidar S.M., et al. Mathematical Method for Optimising the Transport and Logistics Industry // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russian Federation. 2022. P. 1–5.
2. Jharko E., et al. Some Safety Issues in an Intelligent Transport Environment // 2023 International Russian Automation Conference (RusAutoCon), Sochi, Russian Federation. 2023. P. 453–459.
3. Blanchard, B.S., Fabrycky W. Systems Engineering and Analysis (5th Edition). Prentice-Hall International Series in Industrial and Systems Engineering. 2013. 846 p.
4. Mynuddin M., et al. Automatic Network Intrusion Detection System Using Machine Learning and Deep Learning // 2024 IEEE International Conference on Artificial Intelligence and Mechatronics Systems (AIMS), Bandung, Indonesia. 2024. P. 1–9.
5. Smith R.E. A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles // IEEE Security & Privacy. 2012; 10(6):20–25.
6. Maconachy W.V., et al. A Model for Information Assurance: An Integrated Approach // 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY. 2001. P. 306–310.
7. GOSR R 27.102-2021. Dependability in technics. Dependability of item. Terms and definitions. Moscow: Rossiyskiy institut standartizatsii. 2021. 40 p.
8. GOST R 56205-2014. Industrial communication networks. Network and system security. Part 1-1. Terminology, concepts and models. . Moscow: Standardinform. 2014. 77 p.
9. Kalashnikov A.O., Anikina A.V. Information risk management models of complex systems // Informatsiya i bezopasnost'. 2020; 23(2(4)):191-202 (In Russ).
10. Le Boudec J.-Y., Thiran P. Network Calculus: A Theory of Deterministic Queuing Systems for the Internet // Lecture Notes in Computer Science. 2001; 2050. 274 p.
11. Vishnevskiy V.M. Theoretical foundations of computer network design. Moscow: Tekhnosfera. 2003. 512 p.
12. Промыслов В.Г., Семенков К.В. Применение метода Network Calculus для расчета временных характеристик систем управления с циклическим алгоритмом работы // Проблемы управления. 2021. N4. С. 50-65.
13. GOST R 59346-2021. System engineering. Protection of information in system requirements definition process. Moscow: Standardinform. 2021. 66 p.
14. Cruz R.L. A calculus for network delay. II. Network analysis // IEEE Transactions on Information Theory. 1991; 37(1):132-141.

Jharko Elena Ph. PhD, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. 165, Profsouznay str., Moscow, 117997, Russia. E-mail: zharko@ipu.ru.

Abdulova Ekaterina A. V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. 165, Profsouznay str., Moscow, 117997, Russia. E-mail: consoft@ipu.ru.

Promyslov Vitaly G. PhD, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. 165, Profsouznay str., Moscow, 117997, Russia. E-mail: E-mail: vp@ipu.ru.

Semenkov Kirill V. PhD, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. 165, Profsouznay str., Moscow, 117997, Russia. E-mail: semenkov@ipu.ru