

Industrial Transport of Kazakhstan
ISSN 1814-5787 (print)
ISSN 3006-0273 (online)
Vol. 23. Is. 3. Number 91 (2026). Pp. 65–77
Journal homepage: <https://prom.mtgu.edu.kz>
<https://doi.org/10.58420.ptk.2026.91.03.006>
UDC / УДК / ООЖ 81.93.29

CYBER-RESILIENCE MODEL FOR DISTRIBUTED INDUSTRIAL TRANSPORT INFORMATION SYSTEMS

*A. Omirgazynov**

Al-Farabi Kazakh National University, Kazakhstan.

E-mail: aidarkhan0126@mail.ru

Aidarkhan Omirgazynov — PhD student, Al-Farabi Kazakh National University, 71 al-Farabi Ave., Almaty 050040, Almaty, Kazakhstan.

E-mail: aidarkhan0126@mail.ru, <https://orcid.org/0009-0000-0693-9084>.

© A. Omirgazynov

Abstract. Industrial transport information systems combine telemetry from rolling stock and trackside devices, communication links and dispatching servers, so a loss of data availability or integrity affects traffic control. The aim is to build a cyber-resilience model of such a system in which detection, isolation and recovery are assessed together with their effect on latency and availability. The methods are STRIDE threat modelling, partitioning of the system into zones and conduits following the IEC 62443-3-2 concept, and message-level discrete-event simulation. The material comprises 240 runs of a system with 80 telemetry sources in two zones. A baseline architecture with manual response was compared with a proposed architecture combining per-source rate limiting, detectors at zone conduits, message authentication, automatic isolation and a hot-standby server. In four of the five attack and fault scenarios the proposed architecture kept mean availability at or above 0.996, whereas baseline availability was 0.20–0.80 under the assumed manual response times; detection took 0.65–3.65 s. No benefit was obtained when infection spread only within one zone. Authentication added the assumed 0.5 ms to median latency, but at 1.8 messages per second per source and 5 ms per check the total load exceeded server capacity and availability was lost entirely. The novelty lies in the joint assessment of cyber-resilience indicators and of the operational cost of security controls, with attacks and benign faults treated separately. The practical value is a procedure for selecting controls with the system's capacity in mind. The results come from simulation with declared parameters and must be verified against data from an operating enterprise.

Keywords: cyber-resilience, industrial transport, zones and conduits, anomaly detection, automatic isolation, discrete-event simulation

For citation: Omirgazynov A. (2026). Cyber-Resilience Model for Distributed Industrial Transport Information Systems // Industrial Transport of Kazakhstan. Vol. 23. No. 91. Pp. 65–77. <https://doi.org/10.58420.ptk.2026.91.03.006> (In Russ.).

Conflict of interest: The author declares no conflict of interest.

ӨНЕРКӘСІПТІК КӨЛІКТІҢ ҮЛЕСТІРІЛГЕН АҚПАРАТТЫҚ ЖҮЙЕСІНІҢ КИБЕРТҰРАҚТЫЛЫҚ МОДЕЛІ

*А.А. Өмірғазынов**

Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.

E-mail: aidarkhan0126@mail.ru



Өмірғазынов Айдархан Абайұлы — докторант, әл-Фараби атындағы Қазақ ұлттық университеті, әл-Фараби даңғ., 71, 050040, Алматы, Қазақстан
E-mail: aidarkhan0126@mail.ru, <https://orcid.org/0009-0000-0693-9084>.

© Өмірғазынов А.А.

Аннотация. Өнеркәсіптік көліктің ақпараттық жүйелері жылжымалы құрам мен жол құрылғыларының телеметриясын, байланыс арналарын және диспетчерлік серверлерді біріктіреді, сондықтан деректердің қолжетімділігі мен тұтастығының бұзылуы тасымалды басқаруға әсер етеді. Зерттеудің мақсаты – өнеркәсіптік көліктің үлестірілген ақпараттық жүйесінің кибертұрақтылық моделін құру; модельде анықтау, оқшаулау және қалпына келтіру олардың кідіріс пен қолжетімділікке әсерімен бірге бағаланады, сондай-ақ модельді шабуылдар мен ақаулар сценарийлерінде зерттеу. STRIDE бойынша қатерлерді модельдеу, IEC 62443-3-2 тұжырымдамасы бойынша жүйені аймақтар мен арналарға бөлу және жеке хабарламалар деңгейіндегі дискретті-оқиғалық модельдеу қолданылды. Тәжірибелік материал – екі аймақтағы 80 телеметрия көзінен, желі ядросынан және диспетчерлік серверден тұратын жүйе моделінің 240 рет іске қосылуының нәтижелері; қолмен әрекет етуге негізделген базалық архитектура мен көздердің қарқындылығын шектеу, аймақ арналарындағы детекторлар, хабарламалардың түпнұсқалығын тексеру, автоматты оқшаулау және сервердің ыстық резерві бар ұсынылған архитектура салыстырылды. Бес сценарийдің төртеуінде ұсынылған архитектура орташа қолжетімділікті 0,996-дан төмен емес деңгейде сақтады, ал базалық архитектураның қолжетімділігі қолмен әрекет ету туралы қабылданған болжамдарда 0,20–0,80 болды; анықтау уақыты 0,65–3,65 с құрады. Жұқтыру тек бір аймақ ішінде таралғанда артықшылық алынбады. Түпнұсқалықты тексеру медианалық кідірісті берілген 0,5 мс-қа арттырды, алайда бір көзге секундына 1,8 хабарлама жүктеме кезінде және тексеруге 5 мс жұмсалғанда жалпы ағын сервердің өткізу қабілетінен асып, қолжетімділік толық жоғалды. Жұмыстың жаңалығы – өнеркәсіптік көліктің ақпараттық жүйесі үшін кибертұрақтылық көрсеткіштері мен қорғаныс шараларының пайдалану құнын шабуылдар мен ақауларды бөлек ескере отырып бірлесіп сандық бағалау. Практикалық маңызы – жүйенің өткізу қабілетін ескеріп қорғаныс шараларын таңдау тәртібі. Нәтижелер алдын ала белгіленген параметрлермен модельдеу арқылы алынды және жұмыс істеп тұрған кәсіпорын деректерінде тексеруді қажет етеді.

Түйін сөздер: кибертұрақтылық, өнеркәсіптік көлік, аймақтар мен арналар, аномалияларды анықтау, автоматты оқшаулау, дискретті-оқиғалық модельдеу

Дәйексөз үшін: Өмірғазынов А.А. (2026). Өнеркәсіптік көліктің үлестірілген ақпараттық жүйесінің кибертұрақтылық моделі // Қазақстан өндіріс көлігі. Том. 23. № 91. 65–77 бет. <https://doi.org/10.58420.ptk.2026.91.03.006> (Орыс. тіл.).

Мүдделер қақтығысы: Автор мүдделер қақтығысының жоқтығын мәлімдейді.

МОДЕЛЬ КИБЕРУСТОЙЧИВОСТИ РАСПРЕДЕЛЁННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРОМЫШЛЕННОГО ТРАНСПОРТА

*А.А. Өмірғазынов**

Казахский национальный университет имени аль-Фараби, Алматы, Казахстан.

E-mail: aidarkhan0126@mail.ru

Өмірғазынов Айдархан Абайұлы — докторант, Казахский национальный университет имени аль-Фараби, пр. аль-Фараби, 71, 050040, Алматы, Казахстан
E-mail: aidarkhan0126@mail.ru, <https://orcid.org/0009-0000-0693-9084>.

© Өмірғазынов А.А.

Аннотация. Информационные системы промышленного транспорта объединяют телеметрию подвижного состава и путевых устройств, каналы связи и диспетчерские серверы, поэтому нарушение доступности или целостности данных отражается на управлении перевозками. Цель исследования – построить модель киберустойчивости распределённой информационной системы промышленного транспорта, в которой обнаружение, локализация и восстановление оцениваются вместе с их влиянием на задержку и доступность, и исследовать её на сценариях атак и отказов. Использованы моделирование угроз по STRIDE, разбиение системы на зоны и каналы по концепции IEC 62443-3-2 и дискретно-событийное моделирование на уровне отдельных сообщений. Экспериментальный материал – 240 прогонов модели системы из 80 источников телеметрии в двух зонах, ядра сети и диспетчерского сервера; сравнивались базовая архитектура с ручным реагированием и предлагаемая архитектура с ограничением интенсивности источников, детекторами на каналах зон, проверкой подлинности сообщений, автоматической изоляцией и горячим резервом сервера. В четырёх из пяти сценариев воздействия предлагаемая архитектура сохраняла среднюю доступность не ниже 0,996, тогда как у базовой архитектуры при принятых допущениях о ручном реагировании она составляла 0,20–0,80; время обнаружения составило от 0,65 до 3,65 с. При распространении заражения только внутри одной зоны выигрыша не получено. Проверка подлинности увеличивала медианную задержку на заданные 0,5 мс, однако при нагрузке 1,8 сообщения в секунду на источник и затратах 5 мс на проверку суммарный поток превышал пропускную способность сервера и доступность терялась полностью. Новизна работы состоит в совместной количественной оценке показателей киберустойчивости и эксплуатационной цены защитных мер для информационной системы промышленного транспорта с раздельным учётом атак и отказов. Практическое значение – порядок выбора мер защиты с учётом пропускной способности системы. Результаты получены моделированием с объявленными параметрами и требуют проверки на данных действующего предприятия.

Ключевые слова: киберустойчивость, промышленный транспорт, зоны и каналы, обнаружение аномалий, автоматическая изоляция, дискретно-событийное моделирование

Для цитирования: А.А. Әмірғазынов. Модель киберустойчивости распределённой информационной системы промышленного транспорта // Промышленный транспорт Казахстана. Т. 23. №. 91. Стр. 65–77. <https://doi.org/10.58420.ptk.2026.91.03.006> (На русс.).

Конфликт интересов: Автор заявляет об отсутствии конфликта интересов.

Введение.

Промышленный транспорт предприятий внутризаводские железнодорожные пути, погрузочные фронты, парки маневровых локомотивов и вагонов – всё чаще управляется через распределённые информационные системы. Источники телеметрии на подвижном составе и путевых устройствах передают данные через каналы связи в диспетчерский сервер, где формируется картина состояния перевозок. В такой системе соединяются элементы информационных технологий, промышленного интернета вещей и операционных технологий, а отказ или атака на один из уровней проявляется в потере, задержке или искажении данных на другом (Stouffer и др., 2023).

Для транспорта эта проблема подтверждается отраслевыми обзорами. ENISA в первом анализе угроз транспортному сектору ЕС рассмотрела инциденты в авиации, морском, железнодорожном и автомобильном транспорте за январь 2021 г. – октябрь 2022 г. (ENISA, 2023). Железнодорожная отрасль получила собственную техническую спецификацию по кибербезопасности, действующая редакция которой CLC/TS 50701:2023 (CLC/TS 50701, 2023). В Казахстане правовая база в 2026 г. обновлена: Закон № 418-V получил наименование «О кибербезопасности» (Закон РК № 418-V, 2015), а единые требования в области ИКТ содержат отдельную главу о требованиях к автоматизированным

системам управления технологическими процессами (Постановление Правительства РК № 832, 2016).

Нормативные документы задают требования, но не отвечают на инженерный вопрос: насколько конкретная архитектура сокращает время обнаружения и восстановления и чего это стоит в задержке и доступности. Киберустойчивость, по определению NIST SP 800-160 Vol. 2, связана со способностью системы предвидеть неблагоприятные условия, выдерживать их, восстанавливаться и адаптироваться (Ross и др., 2021), и её предлагается измерять, а не декларировать (Kott, Linkov, 2021: 80–85). Для информационных систем промышленного транспорта таких измерений в рассмотренной литературе мы не нашли.

Для систем промышленного транспорта важны не только классические свойства информационной безопасности, но и своевременность данных. Телеметрия о положении и состоянии подвижного состава полезна диспетчеру лишь в течение ограниченного времени, поэтому задержка доставки, потеря части сообщений или приём поддельных данных одинаково ухудшают картину перевозок. Защитные меры – проверка подлинности, фильтрация трафика, изоляция узлов – сами потребляют ресурсы и добавляют задержку, а значит, их выбор требует количественной оценки как выигрыша, так и цены.

Объект исследования распределённая информационная система промышленного транспорта, включающая источники телеметрии, каналы зон, ядро сети и диспетчерский сервер. Предмет архитектура обнаружения, локализации и восстановления и её влияние на показатели безопасности и эксплуатации. Цель построить модель, позволяющую сравнить архитектуры по времени обнаружения и восстановления, доступности, потерям, задержке и числу принятых поддельных сообщений при заданных сценариях атак и отказов. Задачи: определить границы системы и модель угроз; сформулировать базовую и предлагаемую архитектуры; реализовать дискретно-событийную модель; провести вычислительный эксперимент с повторениями и анализ чувствительности к параметрам, которые не были измерены.

Новизна работы состоит в том, что архитектуры сравниваются на одной и той же модели по согласованному набору показателей – времени обнаружения и восстановления, доступности, потерям в окне воздействия, задержке и числу принятых поддельных сообщений, а все параметры, которые не удалось измерить, объявлены явно и проверены в анализе чувствительности. Статья построена следующим образом: в обзоре литературы рассмотрены нормативная база, подходы к моделированию угроз и испытательные стенды в разделе Материалы и методы описаны границы системы, модель угроз, архитектуры и параметры модели; в разделе Результаты приведены показатели по сценариям и анализ чувствительности; в разделах Обсуждение и Заключение рассмотрены механизмы выигрыша, цена защитных мер и ограничения исследования.

Работы по количественной киберустойчивости предлагают общие схемы показателей. Kott и Linkov обосновывают необходимость измерять устойчивость через изменение функции системы во времени (Kott, Linkov, 2021: 80–85); Adewumi и соавторы предлагают показатели устойчивости для критической инфраструктуры с интернетом вещей (Adewumi и др., 2024: 265–280). Такие схемы задают язык описания, но не привязаны к конкретной транспортной информационной системе и не включают цену защитных мер.

Транспортные исследования устойчивости сосредоточены на системах управления движением поездов на основе радиосвязи (СВТС). Lu и соавторы предложили оценку безопасности СВТС через показатели устойчивости (Lu и др., 2021), Gao и соавторы – стратегию устойчивого управления при злонамеренных воздействиях с использованием связи между поездами (Gao и др., 2022: 21015–21033). Обзоры Soderi и соавторов описывают угрозы и средства защиты железнодорожных систем в условиях их взаимосвязанности (Soderi и др., 2023a: 6764–6779) и требования к безопасности СВТС (Soderi и др., 2023b: 92312–92321). Эти работы касаются систем сигнализации и управления

движением, тогда как диспетчерские и телеметрические системы промышленного транспорта предприятий остаются вне их рамок.

Методическая база для анализа угроз хорошо разработана. STRIDE в сочетании с оценкой DREAD применялся к распределённой системе управления нефтеперерабатывающего завода (Kim и др., 2022: 991–1003), нотации деревьев и графов атак систематизированы в обзоре Lallie и соавторов (Lallie и др., 2020). Для промышленных систем управления составлена матрица тактик MITRE ATT&CK for ICS (MITRE, 2026), а концепция зон и каналов закреплена в IEC 62443-3-2 (IEC 62443-3-2, 2020) и перенесена на железнодорожные системы в руководстве ENISA (ENISA, 2022). Требования к уровням безопасности систем задаёт IEC 62443-3-3 (IEC 62443-3-3, 2013).

Для экспериментальной проверки используются испытательные стенды. Conti и соавторы составили обзор стендов и наборов данных для исследований безопасности промышленных систем управления (Conti и др., 2021: 2248–2294); ICSSIM предлагает каркас виртуального стенда на контейнерах (Dehlaghi-Ghadim и др., 2023); моделирование на цифровых двойниках интегрируется в центр мониторинга безопасности (Dietz и др., 2020: 1–9), хотя сам двойник становится объектом угроз (Alcaraz, Lopez, 2022: 1475–1503). Работы по обнаружению вторжений сообщают точность и время обработки: облегчённые нейросетевые детекторы для промышленных систем (Kravchik, Shabtai, 2022: 2179–2197), многоуровневая гибридная система для интернета транспортных средств (Yang и др., 2022: 616–632). Механизмы изоляции – микросегментация с принципом нулевого доверия – оцениваются отдельно (Basta и др., 2022: 1–7; Federici и др., 2023).

Таким образом, в рассмотренной литературе каждая часть задачи изучена по отдельности: показатели устойчивости, модели угроз, стенды, детекторы, изоляция. Не найдено работ, в которых для информационной системы промышленного транспорта на одном стенде совместно оценивались бы обнаружение, изоляция и восстановление, а показатели безопасности (время обнаружения и восстановления, число принятых поддельных сообщений) рассматривались вместе с эксплуатационной ценой мер (задержка, потери, доступность) и с отделением атак от неумышленных отказов. Этот пробел определяет исследовательский вопрос: какая архитектура обнаружения, локализации и восстановления повышает киберустойчивость распределённой информационной системы промышленного транспорта при заданных сценариях и какова её цена для задержки и доступности?

Материалы и методы.

Исследование выполнено в пять этапов: определение границ системы; моделирование угроз; формулирование двух архитектур; дискретно-событийный эксперимент; анализ чувствительности. Проверялась гипотеза H1: предлагаемая архитектура даёт меньшее время обнаружения и время восстановления и более высокую доступность, чем базовая, во всех сценариях. Одновременно задано инженерное требование: в нормальном режиме 95-й процентиль задержки доставки телеметрии не должен превышать срок полезности данных, принятый в модели равным 1 с.

Границы системы. В модель включены 80 источников телеметрии в двух зонах (40 – подвижной состав, 40 – путевые устройства), по одному каналу на зону, ядро сети и диспетчерский сервер. Логика сигнализации и централизации, относящаяся к функциональной безопасности, в границы не входит: промышленная безопасность рассматривается только как категория последствий. Сценарии описаны через их воздействие на трафик, без технических приёмов реализации атак.

Модель угроз построена по STRIDE с отнесением каждой угрозы к сценарию эксперимента и мере защиты (таблица 1). Угрозы отказа от авторства и раскрытия информации в эксперимент не включены, поэтому со сценариями связаны четыре категории (S, T, D, E): первая относится к журналированию, вторая – к

конфиденциальности, которая не является целевым свойством диспетчерской телеметрии в данной постановке.

Таблица 1 — Модель угроз и сценарии эксперимента

Категория STRIDE	Сценарий модели	Воздействие на систему	Мера в предлагаемой архитектуре
Отказ в обслуживании (D)	S1: перегрузка канала зоны потоком 400 сообщ./с от одного узла в течение 600 с	Потеря и задержка телеметрии зоны	Ограничитель интенсивности по источнику; детектор на канале; изоляция
Подмена (S)	S2: 5 поддельных сообщ./с без действительного ключа от имени других узлов	Ложные данные в диспетчерской	Проверка подлинности на сервере; счётчик отказов; изоляция
Искажение (Т), повышение привилегий (Е)	S3: распространение заражения с узла на узлы обеих зон; заражённые узлы передают искажённую телеметрию с действительными ключами	Ложные данные; рост числа скомпрометированных узлов	Блокировка попыток в чужую зону на канале; счётчик блокировок; изоляция
То же	S3b: распространение только внутри своей зоны	То же	Те же меры; попытки внутри зоны каналу не видны
Не атака	S4: отказ диспетчерского сервера	Полная потеря приёма телеметрии	Горячий резерв; переключение по пропуску сигналов контроля
Отказ от авторства (R), раскрытие (I)	Не моделируются	—	—

Источник: составлено автором по методике STRIDE. Сокращения: S, T, R, I, D, E – категории STRIDE; S1–S4, S3b – сценарии модели.

Архитектуры. Базовая архитектура – плоская сеть с защитой периметра, без обнаружения на внутренних каналах, с ручным реагированием: операторы замечают нарушение через 300 с, блокируют источник ещё через 300 с, перезапускают сервер за 600 с, очищают заражённый узел за 1800 с. Предлагаемая архитектура (рисунок 1) делит систему на зоны с каналами, на входе канала ставит ограничитель интенсивности по источнику (5 сообщ./с, ёмкость 10 сообщений) и детектор, на сервере – проверку подлинности сообщений (0,5 мс на сообщение), добавляет контроллер изоляции и горячий резерв сервера. Ручное реагирование сохраняется как резервный механизм: в обеих архитектурах на 1500-й секунде (300 + 300 с после начала сценария) распространение заражения останавливается, а все заражённые и ещё не изолированные узлы отключаются для очистки. Значения показателей базовой архитектуры поэтому получаются арифметически из принятых времён ручного реагирования и длительности воздействия, а не из поведения модели.

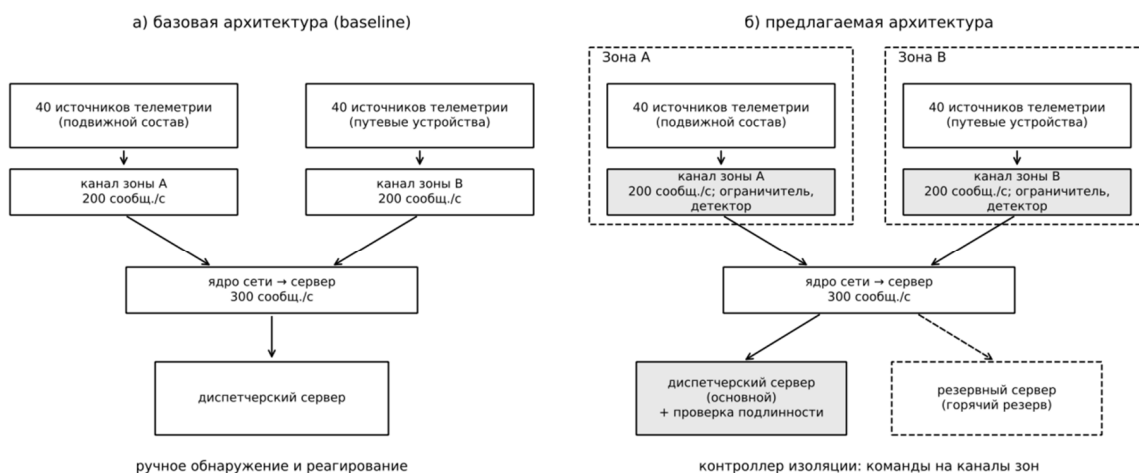


Рис. 1. Базовая и предлагаемая архитектуры информационной системы

Источник: составлено автором. Затенены элементы, добавленные в предлагаемой архитектуре; пунктиром показаны границы зон и резервный сервер.

Алгоритм обнаружения, локализации и восстановления (рисунок 2) работает по четырём признакам. Детектор на канале считает сообщения каждого источника за секунду и формирует сигнал тревоги, если счёт превышает порог две секунды подряд; порог – максимальный секундный счёт среди всех источников за первые 600 с прогона (до воздействия) плюс единица, то есть он определяется по данным каждого прогона, а не задаётся вручную. Сервер формирует сигнал тревоги при трёх отказах проверки подлинности от одного источника за 10 с, канал – при трёх заблокированных попытках соединения узла с чужой зоной за 10 с. По тревоге контроллер через 2 с изолирует источник на канале. В сценариях S1 и S2 изоляция действует до конца прогона; в сценарии S3 изолированный узел возвращается после очистки через 1800 с. Отказ сервера определяется по трём пропущенным сигналам контроля с периодом 1 с, переключение на резерв занимает 2 с.

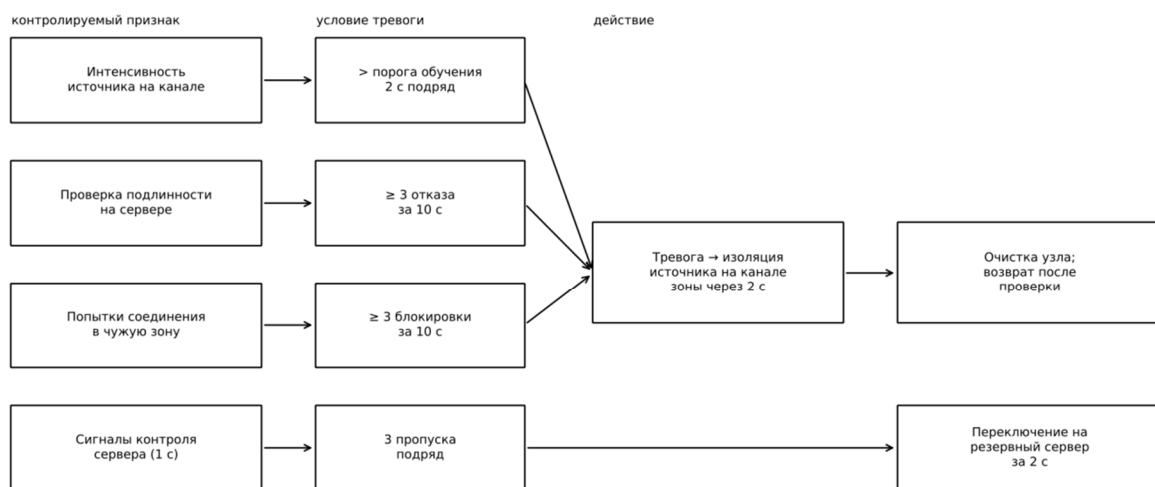


Рис. 2. Алгоритм обнаружения, локализации и восстановления

Источник: составлено автором.

Модель. Каждое сообщение проходит три очереди с обслуживанием в порядке поступления, детерминированным временем обслуживания и конечным буфером: канал зоны (200 сообщ./с, буфер 500), ядро (300 сообщ./с, буфер 500), сервер (2,5 мс на сообщение, буфер 1000), с задержкой 2 мс на переход. Источники генерируют сообщения как пуассоновский поток интенсивностью 1 сообщ./с. Длительность прогона – 3600 с, воздействие начинается на 900-й секунде и в сценариях S1 и S2 длится 600 с. В сценарии S3 каждый заражённый узел делает в среднем 2 попытки соединения в секунду с успехом 0,05 и передаёт 1 искажённое сообщение в секунду. Сообщение считается доставленным в срок, если задержка не превышает 1 с. Значения параметров (таблица 2) не измерялись на предприятии: это объявленные допущения модели, ключевые из них варьируются в анализе чувствительности.

Таблица 2 — Параметры модели

Параметр	Значение	Варьирование в анализе чувствительности
Источники телеметрии, шт. (зона А / зона В)	40 / 40	–
Интенсивность источника, сообщ./с	1,0	1,0; 1,5; 1,8
Пропускная способность канала зоны / ядра, сообщ./с	200 / 300	–

Параметр	Значение	Варьирование в анализе чувствительности
Время обработки на сервере, мс	2,5	–
Затраты на проверку подлинности, мс	0,5	0; 0,5; 2; 5
Срок полезности телеметрии, с	1,0	–
Ручное обнаружение / блокировка / перезапуск / очистка, с	300 / 300 / 600 / 1800	обнаружение: 60; 300; 900
Задержка изоляции после тревоги, с	2	2; 10; 30; 120
Вероятность заражения при попытке (S3)	0,05	0,01; 0,05; 0,2
Ограничитель: скорость, сообщ./с / ёмкость, сообщ.	5 / 10	–
Буферы канала / ядра / сервера, сообщ.	500 / 500 / 1000	–
Длительность S1 и S2, с; поток S1 / S2, сообщ./с	600; 400 / 5	–
S3: попытки соединения, 1/с; искажённые сообщения, сообщ./с	2; 1	–
Очистка узла в предлагаемой архитектуре, с	1800	–

Источник: составлено автором. Параметры ручного реагирования являются допущениями и подлежат замене данными предприятия.

Показатели. Время обнаружения (MTTD) – интервал от начала сценария до тревоги; для базовой архитектуры оно равно параметру ручного обнаружения. Доступность – доля 10-секундных интервалов за 50 минут после периода прогрева (600 с), в которых в срок доставлено не менее 95 % телеметрии и не принято ни одного поддельного сообщения. Время восстановления (MTTR) – интервал от начала сценария до конца последнего недоступного 10-секундного интервала в данном прогоне (разрешение 10 с); среднее по прогонам приводится в таблице 3. Дополнительно вычислялись потери телеметрии в окне 900–1500 с (одинаковом для всех сценариев), число принятых поддельных сообщений, число заражённых узлов, число ложных изоляций, а также медиана и 95-й перцентиль задержки в нормальном режиме – на участке 600–900 с каждого прогона, до начала воздействия.

Протокол. Для каждого из шести сценариев (S0 без воздействия, S1–S4, S3b) и каждой архитектуры выполнено 20 прогонов со значениями random seed от 0 до 19, всего 240 прогонов; анализ чувствительности – по 10 прогонов на значение параметра. Приводятся среднее и полуширина 95%-го доверительного интервала по t-распределению Стьюдента. Модель реализована на Python 3.13.16 с numpy 2.5.3, pandas 3.0.5, PyYAML 6.0.3 и matplotlib 3.11.2 и выполнялась на процессоре Intel Xeon 2,80 ГГц (2 виртуальных ядра, 7 ГБ памяти). Код, конфигурация и результаты всех прогонов сохранены; основной эксперимент занимает около 3 минут.

Результаты.

Сводные результаты основного эксперимента приведены в таблице 3. Без воздействий (S0) обе архитектуры имели доступность 1,000; ни в одном из 120 прогонов предлагаемой архитектуры, включая прогоны со сценариями воздействия, не произошло ложной изоляции добросовестного источника.

Таблица 3 — Показатели киберустойчивости по сценариям

Сценарий	Архитектура	MTTD, с	MTTR, с	Доступность	Потери в окне	Принято поддельных	Заражено узлов
S1	базовая	300 (парам.)	610	0,797	$0,4994 \pm 0,0012$	0	–
	предлагаемая	2,00	0	1,000	$0,0126 \pm 0,0002$	0	–
S2	базовая	300 (парам.)	600 ± 1	$0,7998 \pm 0,0003$	0,000	3005 ± 26	–

Сценарий	Архитектура	MTTD, с	MTTR, с	Доступность	Потери в окне	Принято поддельных	Заражено узлов
	предлагаемая	$0,65 \pm 0,18$	0	1,000	$0,0125 \pm 0,0002$	0	–
S3	базовая	300 (парам.)	2400	0,2000	0,0000	44228 ± 314	80
	предлагаемая	$3,65 \pm 0,68$	$10,5 \pm 1,0$	$0,9965 \pm 0,0003$	$0,0142 \pm 0,0020$	6 ± 1	$1,15 \pm 0,17$
S3b	базовая	300 (парам.)	2400	0,2000	0,0000	22335 ± 184	40
	предлагаемая	300 (парам.)	2400	0,2000	0,0000	22335 ± 184	40
S4	базовая	300 (парам.)	900	0,7000	1,000	0	–
	предлагаемая	3,00	10	0,997	$0,0083 \pm 0,0002$	0	–

Источник: результаты компьютерного моделирования автора, 20 прогонов на ячейку; среднее $\pm$ полуширина 95%-го доверительного интервала (не указана, если меньше единицы последнего знака). «Парам.» – значение задано параметром ручного реагирования; все показатели базовой архитектуры следуют из принятых времён ручного реагирования. Потери – в окне 900–1500 с. Доступность рассчитана за 50 мин после прогрева.

Перегрузка канала (S1) в базовой архитектуре привела к потере около половины телеметрии в окне воздействия ($0,499 \pm 0,001$) и к недоступности на 610 с. В предлагаемой архитектуре ограничитель на входе канала отбрасывал избыточный поток ещё до тревоги детектора, поэтому доступность не снижалась ни в одном прогоне. Абляционный прогон без ограничителя (20 прогонов) дал недоступность в один 10-секундный интервал – пока детектор формировал тревогу и выполнялась изоляция – и среднюю доступность 0,9967. Потери (0,013) соответствуют телеметрии самого изолированного узла. При подмене без ключа (S2) базовая архитектура приняла 3005 ± 26 поддельных сообщений, а предлагаемая не приняла ни одного – в модели проверка подлинности отбраковывает все сообщения без действительного ключа – и обнаружила источник за $0,65 \pm 0,18$ с. Значения базовой архитектуры в S1 и S2 определяются длительностью воздействия: ручная блокировка на 1500-й секунде совпадает с его окончанием.

При распространении заражения между зонами (S3) в базовой архитектуре до ручной блокировки были заражены все 80 узлов, а последующая изоляция и очистка оставили систему недоступной на 2400 с. В предлагаемой архитектуре третья заблокированная попытка выхода в чужую зону за 10 с приводила к тревоге и через 2 с – к изоляции; в среднем заражалось $1,15 \pm 0,17$ узла, время восстановления составило $10,5 \pm 1,0$ с. В сценарии S3b, где распространение шло только внутри зоны, обе архитектуры дали одинаковый результат: 40 заражённых узлов и доступность 0,200. При отказе сервера (S4) предлагаемая архитектура сократила простой до 5 с (3 с на обнаружение и 2 с на переключение на резерв), что с учётом 10-секундных интервалов даёт недоступность 10 с, против 900 с при ручном перезапуске. Кривые устойчивости для одного прогона показаны на рисунке 3.

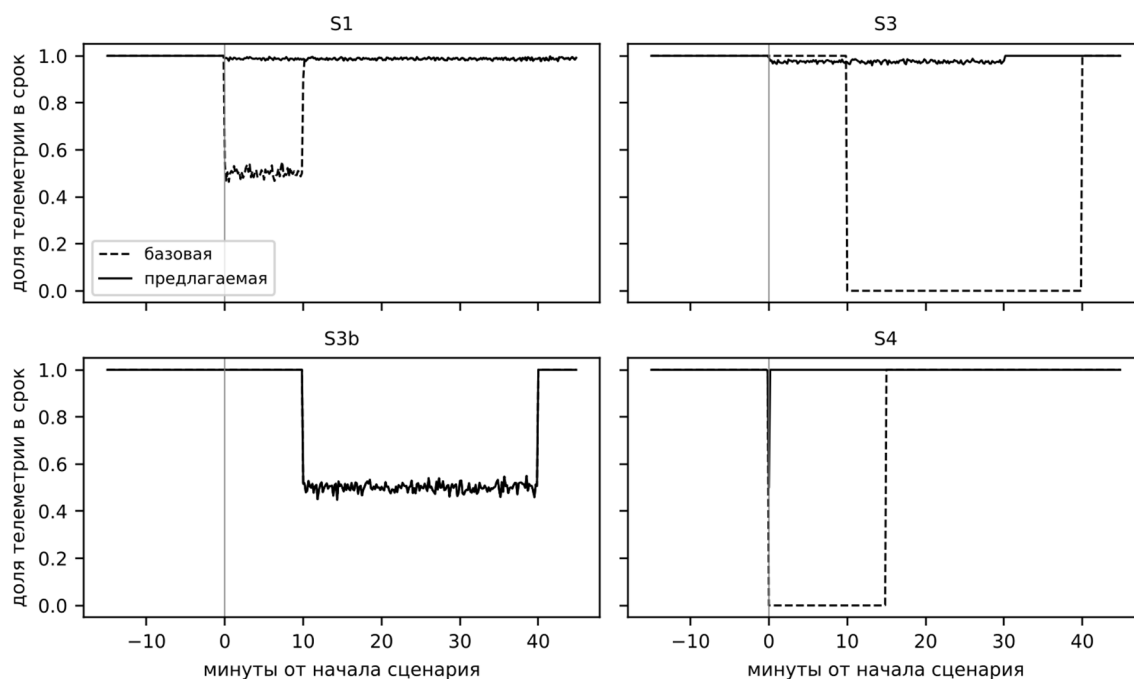


Рис. 3. Доля телеметрии, доставленной в срок, по сценариям (прогон с seed 0)

Источник: результаты компьютерного моделирования автора. Пунктир – базовая архитектура, сплошная линия – предлагаемая; интервалы 10 с. Принятые поддельные сообщения на рисунке не отражены (см. таблицу 3).

Цена защитных мер в нормальном режиме определяется заданными затратами на проверку подлинности: медиана задержки выросла с 16,8 до 17,3 мс, 95-й процентиль – с 21,6 до 22,1 мс, что выполняет инженерное требование с большим запасом. Анализ чувствительности показал, что эта цена растёт нелинейно по мере приближения нагрузки к пропускной способности сервера; сам порог перегрузки следует из арифметики пропускной способности, а модель показывает, как ведут себя задержка и доступность вблизи него. При интенсивности 1,5 сообщ./с на источник и затратах 5 мс на проверку 95-й процентиль задержки составил 130,2 мс, а при 1,8 сообщ./с и тех же затратах суммарный поток (144 сообщ./с) превысил пропускную способность сервера (около 133 сообщ./с), медианная задержка выросла до 7484,5 мс и доступность упала до 0,000. При затратах 2 мс те же нагрузки обслуживались с 95-м процентилем 30,1 и 34,8 мс.

Выводы о базовой архитектуре зависят от принятых параметров ручного реагирования. При обнаружении через 60 с вместо 300 с доступность базовой архитектуры в сценарии S1 выросла с 0,797 до 0,877, оставаясь ниже предлагаемой (1,000); при 300 и 900 с она одинакова, потому что ручная блокировка наступает не раньше окончания воздействия. Задержка изоляции от 2 до 120 с в сценарии S2 на результат не влияла: поддельные сообщения отсекались проверкой подлинности независимо от изоляции. При вероятности заражения 0,2 в сценарии S3 (10 прогонов) всего заражалось в среднем 4,1 узла (от 1 до 14), а средняя доступность предлагаемой архитектуры снижалась до 0,813; распределение двухмодальное: в 3 прогонах из 10 доступность составила около 0,39, в остальных – 0,970–0,997.

Обсуждение.

Гипотеза H1 подтвердилась частично. Для сценариев S1, S2, S3 и S4 предлагаемая архитектура дала меньшее время обнаружения и восстановления и более высокую доступность, но для S3b различий нет. Модель воспроизводит известное ограничение: сегментация по зонам и каналам, рекомендуемая IEC 62443-3-2 и руководством ENISA для железнодорожных систем (IEC 62443-3-2, 2020; ENISA, 2022), защищает от перехода между

зонами, но не видит распространения внутри зоны – в модели у предлагаемой архитектуры нет механизма обнаружения внутризонных попыток, поэтому совпадение с базовой архитектурой ожидаемо. Для таких сценариев нужны средства контроля на самих узлах или более мелкое деление, что согласуется с подходами микросегментации (Basta и др., 2022: 1–7; Federici и др., 2023).

Второе наблюдение касается механизма выигрыша. Абляционный прогон показал, что в сценарии S1 полную доступность сохранял ограничитель интенсивности: без него недоступность составляла один 10-секундный интервал до изоляции. Детектор и изоляция влияли не на доступность, а на прекращение воздействия. Это различие важно для выбора мер: если цель – сохранить приём телеметрии, первичной мерой является ограничение интенсивности на канале зоны; если цель – прекратить воздействие, нужны обнаружение и изоляция.

Третье наблюдение – цена проверки подлинности. В нормальном режиме она равна заданным долям миллисекунды, однако если сервер работает близко к пределу пропускной способности, рост нагрузки переводит его в перегрузку, и тогда защитная мера сама становится причиной отказа в обслуживании. Работы по обнаружению вторжений обычно сообщают время обработки одного пакета (Kravchik, Shabtai, 2022: 2179–2197; Yang и др., 2022: 616–632); наш результат показывает, что этот показатель нужно соотносить с запасом пропускной способности всей цепочки обработки.

По сравнению с работами по устойчивости CBTC (Lu и др., 2021; Gao и др., 2022: 21015–21033) настоящее исследование рассматривает другой класс систем – диспетчерские и телеметрические системы промышленного транспорта – и отделяет атаки от неумышленного отказа сервера. По сравнению с виртуальными стендами (Dehlaghi-Ghadim и др., 2023; Conti и др., 2021: 2248–2294) модель проще: она не воспроизводит протоколы и программное обеспечение, а описывает систему на уровне потоков сообщений. Это ограничение одновременно делает модель прозрачной: каждый результат прослеживается до объявленного параметра.

Основные ограничения исследования перечислены в заключении. Отдельно отметим, что отсутствие ложных изоляций получено на синтетическом трафике и требует проверки на реальном, а соответствие стандартам модель не оценивает: аудит не проводился.

Заключение.

Цель исследования достигнута: построена и исследована на сценариях дискретно-событийная модель распределённой информационной системы промышленного транспорта, позволяющая сравнивать архитектуры по показателям киберустойчивости и по цене защитных мер. Модель угроз по STRIDE связала четыре из шести категорий угроз с пятью сценариями воздействия, а 240 прогонов (20 значений seed на каждую пару «сценарий – архитектура») позволили оценить разброс результатов. Все результаты получены компьютерным моделированием; параметры, не измеренные на предприятии, объявлены как допущения.

Получены следующие результаты. Предлагаемая архитектура в четырёх из пяти сценариев сохранила среднюю доступность не ниже 0,996 при времени обнаружения 0,65–3,65 с, тогда как доступность базовой архитектуры составила 0,797 при перегрузке канала, 0,800 при подмене сообщений, 0,200 при распространении между зонами и 0,700 при отказе сервера. При подмене без ключа базовая архитектура приняла около 3 000 поддельных сообщений, предлагаемая – ни одного; при распространении между зонами число заражённых узлов сократилось с 80 до 1,15 в среднем. При распространении внутри одной зоны выигрыша нет: обе архитектуры показали одинаковые значения. Гипотеза H1 подтвердилась частично.

Анализ механизмов показал, что полную доступность при перегрузке сохраняло ограничение интенсивности на канале зоны: без него возникал один недоступный 10-

секундный интервал до изоляции. Обнаружение и изоляция влияли не на доступность, а на прекращение воздействия. Проверка подлинности добавила около 0,5 мс к медианной задержке (16,8 и 17,3 мс), однако при затратах 5 мс на сообщение и интенсивности 1,8 сообщ./с на источник суммарный поток превысил пропускную способность сервера, и доступность упала до нуля. Показатели базовой архитектуры определяются принятыми временами ручного реагирования: при обнаружении через 60 с вместо 300 с её доступность при перегрузке выросла с 0,797 до 0,877, оставаясь ниже предлагаемой.

Время восстановления в предлагаемой архитектуре составило около 10 с при распространении между зонами и при отказе сервера против 2 400 и 900 с в базовой архитектуре, где оно задано временем ручного устранения. Анализ чувствительности показал и границы выигрыша. При вероятности заражения 0,2 в сценарии распространения средняя доступность предлагаемой архитектуры снижалась до 0,813, причём распределение было двухмодальным: в 3 прогонах из 10 доступность составила около 0,39. Задержка изоляции от 2 до 120 с при подмене сообщений на результат не влияла, так как поддельные сообщения отсекались проверкой подлинности независимо от изоляции. Эти результаты показывают, какие параметры требуют измерения на предприятии в первую очередь.

Практическое значение состоит в том, что модель позволяет до внедрения оценить, какие меры сохраняют приём телеметрии (ограничение интенсивности, горячий резерв), какие прекращают воздействие (обнаружение и изоляция на каналах зон), где нужны средства контроля внутри зон и какой запас пропускной способности требует проверка подлинности. Для предприятий промышленного транспорта это означает, что требования к защитным мерам следует формулировать вместе с требованиями к пропускной способности диспетчерского сервера и к допустимой задержке телеметрии.

Ограничения исследования: трафик синтетический и пуассоновский, времена ручного реагирования заданы, а не измерены, набор сценариев ограничен пятью воздействиями, а результаты относятся к типовой архитектуре. Перспективы работы – замена допущений модели данными действующего предприятия промышленного транспорта, добавление сценариев с распространением внутри зоны и контролем на узлах, а также проверка модели на виртуальном стенде с реальными протоколами. Для такой замены у предприятия необходимо получить фактическое время обнаружения и устранения инцидентов персоналом, интенсивность и структуру потока телеметрии, пропускную способность диспетчерского сервера и затраты на проверку подлинности одного сообщения; по результатам анализа чувствительности выводы зависят именно от таких параметров.

REFERENCES

- Adewumi A., Hammoudeh M., Dargahi T., Jogunola O. (2024). Measuring Cyber Resilience of IoT-Enabled Critical National Infrastructures // *Lecture Notes in Computer Science*. Vol. 14586. — Pp. 265–280. https://doi.org/10.1007/978-3-031-61486-6_16
- Alcaraz C., Lopez J. (2022). Digital Twin: A Comprehensive Survey of Security Threats // *IEEE Communications Surveys & Tutorials*. Vol. 24. No. 3. — Pp. 1475–1503. <https://doi.org/10.1109/COMST.2022.3171465>
- Basta N., Ikram M., Kaafar M.A., Walker A. (2022). Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework // *NOMS 2022 — IEEE/IFIP Network Operations and Management Symposium*. — Pp. 1–7. <https://doi.org/10.1109/NOMS54207.2022.9789888>
- CLC/TS 50701:2023. Railway applications — Cybersecurity. — Brussels: CENELEC, 2023.
- Conti M., Donadel D., Turrin F. (2021). A Survey on Industrial Control System Testbeds and Datasets for Security Research // *IEEE Communications Surveys & Tutorials*. Vol. 23, No. 4. — Pp. 2248–2294. <https://doi.org/10.1109/COMST.2021.3094360>
- Dehlaghi-Ghadim A., Balador A., Moghadam M.H., Hansson H., Conti M. (2023). ICSSIM — A framework for building industrial control systems security testbeds // *Computers in Industry*. Vol. 148. — Art. 103906. <https://doi.org/10.1016/j.compind.2023.103906>
- Dietz M., Vielberth M., Pernul G. (2020). Integrating digital twin security simulations in the security operations center // *Proceedings of the 15th International Conference on Availability, Reliability and Security*. Pp. 1–9. <https://doi.org/10.1145/3407023.3407039>
- European Union Agency for Cybersecurity (ENISA). Zoning and Conduits for Railways. — Athens: ENISA, 2022. — URL: <https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways> (accessed: 10.10.2026).



- European Union Agency for Cybersecurity (ENISA). ENISA Transport Threat Landscape. — Athens: ENISA, 2023. — URL: <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape> (accessed: 10.10.2026).
- Federici F., Martintoni D., Senni V. (2023). A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures // *Electronics*. Vol. 12, No. 3. — Art. 566. <https://doi.org/10.3390/electronics12030566>
- Gao B., Bu B., Wang X. (2022). A Comprehensive Resilient Control Strategy for CBTC Systems Through Train-to-Train Communications Under Malicious Attacks // *IEEE Transactions on Intelligent Transportation Systems*. Vol. 23, No. 11. — Pp. 21015–21033. <https://doi.org/10.1109/TITS.2022.3192510>
- IEC 62443-3-2:2020. Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design. — Geneva: IEC, 2020.
- IEC 62443-3-3:2013. Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels. — Geneva: IEC, 2013.
- Kim K.H., Kim K., Kim H.K. (2022). STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery // *ETRI Journal*. 2022. Vol. 44. No. 6. — Pp. 991–1003. <https://doi.org/10.4218/etrij.2021-0181>
- Kott A., Linkov I. (2021). To Improve Cyber Resilience, Measure It // *Computer*. Vol. 54. No. 2. — Pp. 80–85. <https://doi.org/10.1109/MC.2020.3038411>
- Kravchik M., Shabtai A. (2022). Efficient Cyber Attack Detection in Industrial Control Systems Using Lightweight Neural Networks and PCA // *IEEE Transactions on Dependable and Secure Computing*. Vol. 19, No. 4. — Pp. 2179–2197. <https://doi.org/10.1109/TDSC.2021.3050101>
- Lallie H.S., Debatista K., Bal J. (2020). A review of attack graph and attack tree visual syntax in cyber security // *Computer Science Review*. Vol. 35. — Art. 100219. <https://doi.org/10.1016/j.cosrev.2019.100219>
- Lu R., Dong H., Wang H., Cui D., Zhu L., Wang X. (2021). A Resilience-Based Security Assessment Approach for CBTC Systems // *Complexity*. Vol. — Art. 2175780. <https://doi.org/10.1155/2021/2175780>
- MITRE ATT&CK for ICS: ICS Matrix. — URL: <https://attack.mitre.org/matrices/ics/> (accessed: 10.10.2026).
- Postanovlenie Pravitel'stva Respubliki Kazakhstan ot 20 dekabrya 2016 goda № 832 «Ob utverzhdenii edinykh trebovaniy v oblasti informatsionno-kommunikatsionnykh tekhnologii i obespecheniya informatsionnoi bezopasnosti» [Resolution of the Government of the Republic of Kazakhstan of 20 December 2016 No. 832 “On approval of the unified requirements in the field of information and communication technologies and information security”]. — URL: <https://adilet.zan.kz/rus/docs/P1600000832> (accessed: 10.10.2026). [In Russ.]
- Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160 Vol. 2 Rev. 1. — Gaithersburg: NIST. <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- Soderi S., Masti D., Lun Y.Z. (2023). Railway Cyber-Security in the Era of Interconnected Systems: A Survey // *IEEE Transactions on Intelligent Transportation Systems*. Vol. 24, No. 7. — Pp. 6764–6779. <https://doi.org/10.1109/TITS.2023.3254442>
- Soderi S., Masti D., Hämäläinen M., Iinatti J. (2023). Cybersecurity Considerations for Communication Based Train Control // *IEEE Access*. Vol. 11. — Pp. 92312–92321. <https://doi.org/10.1109/ACCESS.2023.3309005>
- Stouffer K., Pease M., Tang C., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. (2023). Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3. — Gaithersburg: NIST. <https://doi.org/10.6028/NIST.SP.800-82r3>
- Yang L., Moubayed A., Shami A. (2022). MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles // *IEEE Internet of Things Journal*. Vol. 9, No. 1. — Pp. 616–632. <https://doi.org/10.1109/JIOT.2021.3084796>
- Zakon Respubliki Kazakhstan ot 24 noyabrya 2015 goda № 418-V «O kiberbezopasnosti» (zagolovok v redaktsii Zakona RK ot 09.01.2026 № 256-VIII) [Law of the Republic of Kazakhstan of 24 November 2015 No. 418-V “On Cybersecurity” (title as amended by Law No. 256-VIII of 9 January 2026)]. — URL: <https://adilet.zan.kz/rus/docs/Z1500000418> (accessed: 10.10.2026). [In Russian]