УДК 004.056; 004.896; 004.89

Анализ особенностей обеспечения кибербезопасности автономного судовождения

Analysis of cybersecurity features of autonomous ship navigation

Присяжнюк / Prisyazhnyuk S.
Сергей Прокофьевич
(office@itain.ru)
доктор технических наук, профессор,
заслуженный деятель науки РФ.
ЗАО «Институт телекоммуникаций»,
заместитель генерального директора по науке.
г. Санкт-Петербург

Позолотин / Pozolotin S.
Святослав Игоревич
(pozolotin-cvat@yandex.ru)
ЗАО «Институт телекоммуникаций»,
радиоинженер, специалист отдела
прикладных интеллектуальных технологий.
г. Санкт-Петербург

Храбан / Khraban A.
Александр Владимирович
(hraban@itain.spb.ru)
ЗАО «Институт телекоммуникаций»,
ведущий специалист.
г. Санкт-Петербург

Ключевые слова: автономное судно – autonomous ship; кибербезопасность – cybersecurity; Zero Trust; микросегментация – microsegmentation; постквантовая криптография – post-quantum cryptography; FLS-модель – FLS model; машинное обучение – machine learning; Isolation Forest.

Рассматривается задача кибербезопасности автономного судна как киберфизической системы с бортовыми и береговыми контурами управления. Предложена архитектура автономного судовождения через функциональные кластеры и контролируемые межкластерные связи. Для угроз используется многоуровневое описание, включая риск компрометации криптографии при развитии квантовых вычислений. В качестве базовой модели защиты принята микросегментация и непрерывная проверка доверия (Zero Trust), усиленная ML-детекторами на границах сегментов. Показана практическая применимость подхода на примере прототипа детектора аномалий движения судна на Isolation Forest и сценариев атак.

This paper examines the cybersecurity of an autonomous ship as a cyber-physical system with onboard and shore-based control loops. An autonomous ship navigation architecture using functional clusters and controlled intercluster communications is proposed. Threats are described using a multi-level description, including the risk of cryptographic compromise with the development of quantum computing. Microsegmentation and continuous trust verification (Zero Trust), reinforced by ML detectors at segment boundaries, are adopted as the basic security model. The practical applicability of the approach is demonstrated using a prototype vessel motion anomaly detector based on Isolation Forest and attack scenarios.

Краткая история (эволюция) кораблестроения и кораблевождения

Кораблестроение и кораблевождение развивались от механических и визуальных методов к цифровым системам управления. Рост размеров судов и интенсивности перевозок повысил требования к надежности навигации и управлению движением.

Переход к электронике привел к широкому внедрению датчиков, интегрированных навигационных комплексов и автоматизированных систем управления. Далее сформировались судовые IT/OT-контуры: бортовые вычислители, сети передачи данных, средства связи и удаленный мониторинг.

Следующий шаг – автономное судовождение. Оно опирается на сбор телеметрии, вычислительные модули принятия решений и связь с береговыми центрами. При этом киберриски стали сопоставимы по значимости с отказами оборудования, так как вмешательство в данные и команды напрямую влияет на безопасность плавания [1, 2, 3].

Обобщенная архитектура (интеллектуальная, информационно-сетевая) автономных судов

Архитектура автономного судна целесообразно описывается как набор функциональных кластеров, связанных управляемыми каналами обмена. В практической постановке выделяются:

· навигационный кластер (датчики, системы ситуационной осведомленности);

· управляющий кластер (автопилот, контроллеры движения, исполнительные механизмы);

· коммуникационный кластер (внутренние/внешние каналы связи);

· контур политик безопасности (аутентификация/авторизация и enforcement на границах);

· контур мониторинга и аналитики (в т. ч. ML-детекторы).

Для автономного судна важно разделять режимы работы интеллектуального контура: полностью бортовой (автономный), с опорой на внешние сети (например, сервисы обновлений/коррекции), и с управлением/поддержкой со стороны берегового центра. Это влияет на модель доверия и требования к каналам связи [4, 5].

В статье Zero Trust рассматривается как постоянный процесс: политики должны обновляться по мере изменения обстановки, а автоматизация и аналитика используются для динамического пересчета доверия. Также вся IT/OT-инфраструктура интерпретируется как совокупность микросегментов с проверкой и фильтрацией всех межсегментных обращений («предварительное недоверие») [6].

Такая архитектура критически зависит от корректности входных данных (сенсоры/навигация) и выходных команд (управление/исполнители), а также от защищенности межкластерных каналов. Поэтому далее угрозы рассматриваются как воздействия на эти потоки и на механизмы доверия между бортом и берегом.

Модели киберугроз для автономных судов

Киберугрозы автономного судна целесообразно описывать по уровням:

1. Физический и сенсорный (искажение сигналов, отказ/подмена датчиков);

2. Сетевой (перехват, внедрение, горизонтальное перемещение между сегментами);

3. Прикладной/управляющий (подмена команд, несанкционированные изменения конфигурации);

4. Операционный (ошибки персонала, нарушения регламентов, цепочки поставок) [7].

Критичны атаки на навигационные и кинематические данные, потому что они формируют управляющие решения. Для таких воздействий характерны как грубые подмены, так и тонкие манипуляции курсом и скоростью без явной разметки атак, что усложняет детектирование [4, 8].

Отдельный класс – квантовые угрозы. Квантовые вычислительные системы рассматриваются как фактор, способный ускорять атаки на криптографические схемы (в частности, упоминаются алгоритмы Гровера и Шора) [9].

В прикладном смысле это повышает риск компрометации каналов аутентификации, шифрования и подписи, а также поддерживает сценарии «собрать сейчас – расшифровать позже» для долговременных данных.

Эти угрозы задают три требования к защите: (1) минимизировать доверенные связи через сегментацию, (2) проверять каждое обращение по политике

Рис. 1. Упрощенная схема архитектуры кибербезопасности автономного судна

Zero Trust, (3) обеспечить криптоустойчивость каналов и идентификацию с учетом квантового риска. Для этого нужна модель, которая одновременно описывает структуру связей и показывает, какие из них контролируются средствами защиты. В следующем разделе используется FLS-представление, чтобы формально проверить полноту контроля межкластерных взаимодействий.

Модели защиты автономных судов

Базовая линия защиты автономного судна включает сегментацию, контроль доступа и мониторинг. Для формализации полезно использовать модульно-кластерный подход: выделять функциональные модули и декомпозировать взаимодействия между ними на физические (F), синтаксические (L) и семантические (S) отношения с последующей оценкой безопасности статической или динамической топологии [10]. Учитывается иерархия rF→rL→rS. Такой разрез удобен для судовой среды: физический уровень соответствует каналам и интерфейсам; синтаксический – протоколам и криптографии; семантический – смыслу команд и политике авторизаций.

Полная FLS дуга определяется как объединение физических, синтаксических и семантических дуг между модулями; это используется для анализа полноты контроля и поиска «скрытых» взаимодействий [10].

FLS-модель применяется как инструмент верификации: она показывает, что все допустимые межкластерные связи проходят через узлы контроля (policy enforcement/криптошлюзы), а недопустимые связи отсутствуют. Тем самым FLS связывает архитектуру и требования Zero Trust с проверяемым критерием полноты контроля.

Вершины распределяются по кластерам в соответствии с политикой доступа; субъекты из других кластеров трактуются как угрозы.

Критерий конструктивной защиты задается топологически: внешние дуги не должны существовать либо должны быть инцидентны вершинам, обозначающим средства защиты; для критических приложений возможно требование инцидентности всех дуг средствам защиты. При проверке ищутся полные FLS-дуги, входящие в/исходящие из кластера и не контролируемые средствами защиты [10].

Учет квантовой угрозы вводится через веса вершин FLS: для криптографических функций задается оценка стойкости к квантовой атаке; вес ниже порога трактуется как угроза безопасности.

Декомпозиция помогает распределять меры по уровням: на уровне L реализуется криптографическая защита, на уровнях F и L возможна защита с применением квантового распределения ключей, на уровне S – авторизация доступа.

Рис. 2 иллюстрирует, что наличие прямой межкластерной связи без узла контроля трактуется как

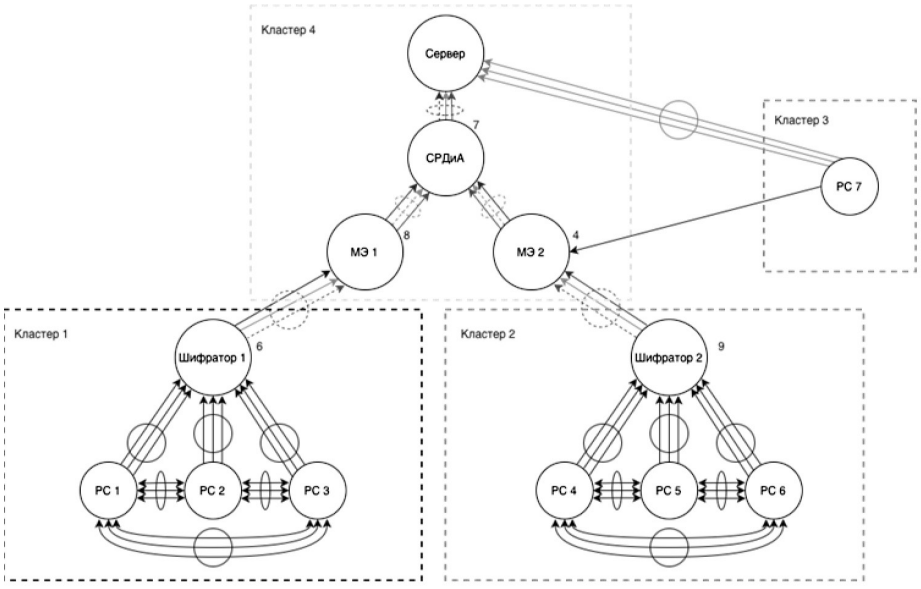

Рис. 2. Кластерная модель защиты информации.
Кластерное FLS-представление сегментированной архитектуры с криптографическими шлюзами и средствами разграничения доступа. Обозначения: МЭ – межсетевой экран; СРДиА – разграничение доступа/аутентификация; «Шифратор» – крипто-шлюз

нарушение критерия конструктивной защиты. В FLS-терминах такая связь соответствует дуге, не инцидентной средствам защиты, и должна быть устранена или замкнута на узел контроля исполнения политик безопасности. Квантовая составляющая учитывается через весовую оценку криптофункций: при снижении «криптовеса» ниже порога связь считается неприемлемой для критических контуров.

Для критических систем формулируется усиленный критерий, соответствующий политике «нулевого доверия»: контроль должен распространяться и на внутренние взаимодействия, а не только на границы периметра [10]. Это согласуется с Zero Trust-подходом в судовой архитектуре.

С учетом квантовых угроз требуется переход к квантово-устойчивым средствам. В модели цифровой платформы для анализа устойчивости к квантовым угрозам многоуровневая система защиты может включать постквантовую криптографию, квантово-устойчивую аутентификацию и динамический мониторинг угроз.

Полученная модель задаёт, какие связи должны быть контролируемыми и какими средствами это обеспечивается (контроль исполнения политик безопасности, криптозащита, мониторинг). Далее эти требования переводятся в набор практических мер: микросегментация и Zero Trust-политики, ML-оценка аномальности как вход в показатель доверия и квантово-устойчивые механизмы для внешних каналов.

Предложения по обеспечению кибербезопасности автономного судовождения

Сегментация и Zero Trust на борту

Предлагается рассматривать судовую IT/OT-инфраструктуру как набор микросегментов по уровням: оборудование (сенсоры/приводы), контроллеры, бортовая сеть и серверы, внешние связи и береговые центры. Между сегментами работают шлюзы контроля исполнения политик безопасности, проверяющие трафик и команды по принципу «предварительного недоверия» [4].

Практический эффект – ограничение «радиуса поражения». Компрометация одного модуля не должна давать контроля над критическими подсистемами; вводятся механизмы быстрой изоляции узлов и перехода на резервирование при подозрении на атаку [4].

ML-детекторы на границах сегментов

В этой работе ML-детектор решает частную задачу: оценивает аномальность потока данных или команд на границе сегмента и формирует величину $A(x,t)$. Это не «решение о доступе», а входной сигнал для интегральной оценки доверия $D(x,t)$. Дальше уже Zero Trust-политика использует $D(x,t)$ для выбора действия (deny/step-up/ограничение/разрешение).

Zero Trust усиливается ML-анализом на ключевых выходах/входах сегментов: на телеметрии датчиков, на командах к исполнительным механизмам, на внешних каналах связи. Это позволяет не ограничиваться стати-

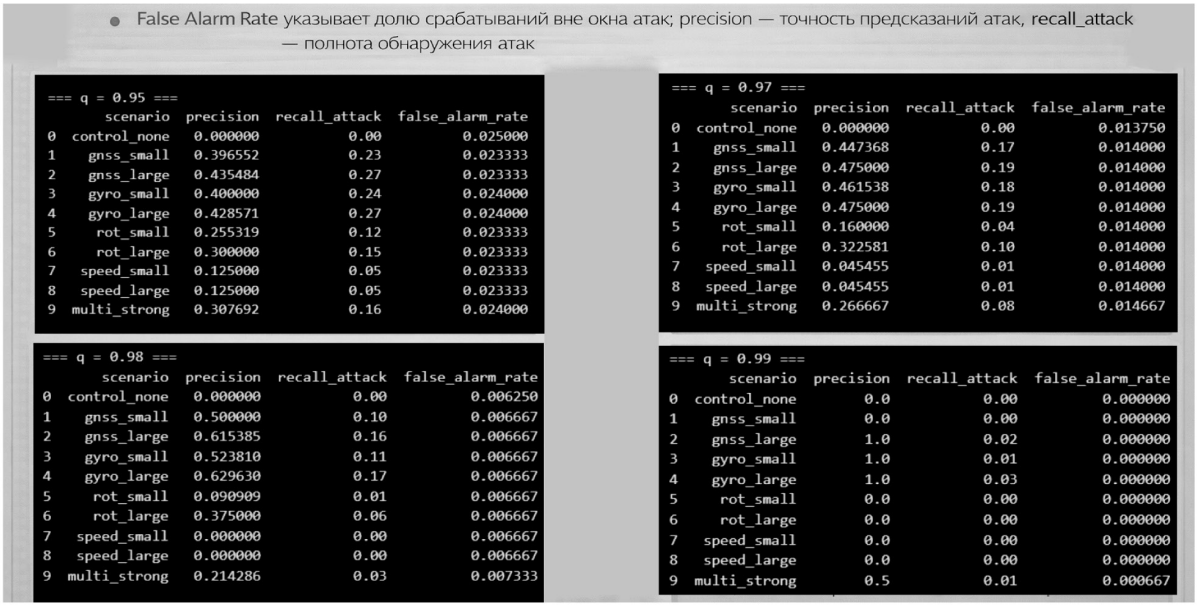

Рис. 3. Метрики детектора аномалий

ческими правилами, а учитывать аномалии поведения. Формализованная модель доверия (trust-score):

$$D(x,t)=wA\cdot(1-A(x,t))+wI\cdot I(x,t)+wG\cdot G(x,t)+wB\cdot B(x,t),$$
$$wA+wI+wG+wB=1.$$

$A(x,t)$ – аномальность (ML), $I(x,t)$ – идентификационно криптографический фактор, $G(x,t)$ – контекст (география/сегмент), $B(x,t)$ – поведенческий фактор. Далее вычисленный $D(x,t)$ связывается с политиками Zero-Trust и принимается решение об ответном действии: запись в журнал, оповещение оператора и усиленный мониторинг или ограничение доступа и переход системы в режим «безопасности» [4].

Выводы

Автономное судовождение требует архитектуры киберзащиты, в которой безопасность встроена в топологию взаимодействий и не опирается на «внутренний периметр». Микросегментация и непрерывная проверка доверия задают основу, а ML-детекторы на границах сегментов повышают чувствительность к аномалиям в телеметрии и командах. Это согласуется с формальным представлением системы через кластеры и FLS-отношения, где запрещенные или неконтролируемые связи рассматриваются как опасные состояния.

Развитие квантовых вычислений усиливает требования к криптографии внешних каналов и цифровых подписей. Поэтому в проектировании целесообразно сразу закладывать постквантовые алгоритмы и криптоагильность, чтобы миграция не стала отдельным высокорисковым проектом.

Литература

1. Автономное судоходство и партнёрство России и Китая // Регион Пауэр Групп [сайт]. – URL : https://regpg.com/news1/autonomous-vessels/ (дата обращения: 27.02.2026).

2. Комашинский, В.И. Искусственный интеллект в модели кибербезопасности «Нулевое доверие» / В.И. Комашинский, С.П. Присяжнюк // Информация и Космос. – 2025. – № 1. – С. 114–124.

3. Российский морской регистр судоходства (РС). Российская технология автоматического судовождения получила принципиальное одобрение РС // Sudostroenie.info [сайт]. – 2020. – URL : https://sudostroenie.info/novosti/32034.html (дата обращения: 27.02.2026).

4. Позолотин, С.И. Применение методов машинного обучения для обеспечения кибербезопасности автономного судовождения : выпускная квалификационная работа специалиста : спец. 25.05.03 «Техническая эксплуатация транспортного радиооборудования» / С.И. Позолотин ; ФГБОУ ВО «ГУМРФ им. адм. С.О. Макарова», Ин-т «Морская академия», факультет навигации и связи, кафедра радиосвязи на мор. флоте. – Санкт-Петербург, 2026. – 182 с.

5. Attribute and User Trust Score-Based Zero Trust Access Control Model in IoV / J. Wang, Z. Wang, J. Song, H. Cheng // Electronics. – 2023. – Vol. 12, No. 23. – Art. 4825.– URL: https://doi.org/10.3390/electronics12234825 (дата обращения: 27.02.2026).

6. Zero Trust Architecture : NIST Special Publication 800-207 / S. Rose, O. Borchert, S. Mitchell, S. Connelly // Gaithersburg, MD : National Institute of Standards and Technology. – 2020. – URL : https://doi.org/10.6028/NIST.SP.800-207 (дата обращения: 27.02.2026).

7. Голушко, А. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года / А. Голушко // Positive Technologies [сайт]. – 2025. – URL : https://ptsecurity.com/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 27.02.2026).

8. Maritime cybersecurity attacks on the rise // Marpoint[Electronic resource]. – URL: https://marpoint.gr/blog/maritime-cybersecurity-attacks-on-the-rise/ (дата обращения: 27.02.2026).

9. Ларина, М.В. Модель цифровой платформы для анализа устойчивости к квантовым угрозам / М.В. Ларина, В.Ю. Скиба // Правовая информатика. – 2025. – № 3. – С. 12–26.

10. Сундеев, П.В. Кластерная модель защиты распределенного реестра / П.В. Сундеев // Вопросы кибербезопасности. – 2025. – № 4 (68). – С. 2–8.

11. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security / V.Yu. Skiba, S.A. Petrenko, K.O. Gnidko, A.S. Petrenko // Computing, Telecommunications and Control. – 2025. – Vol. 18, No. 2. – P. 56–73.