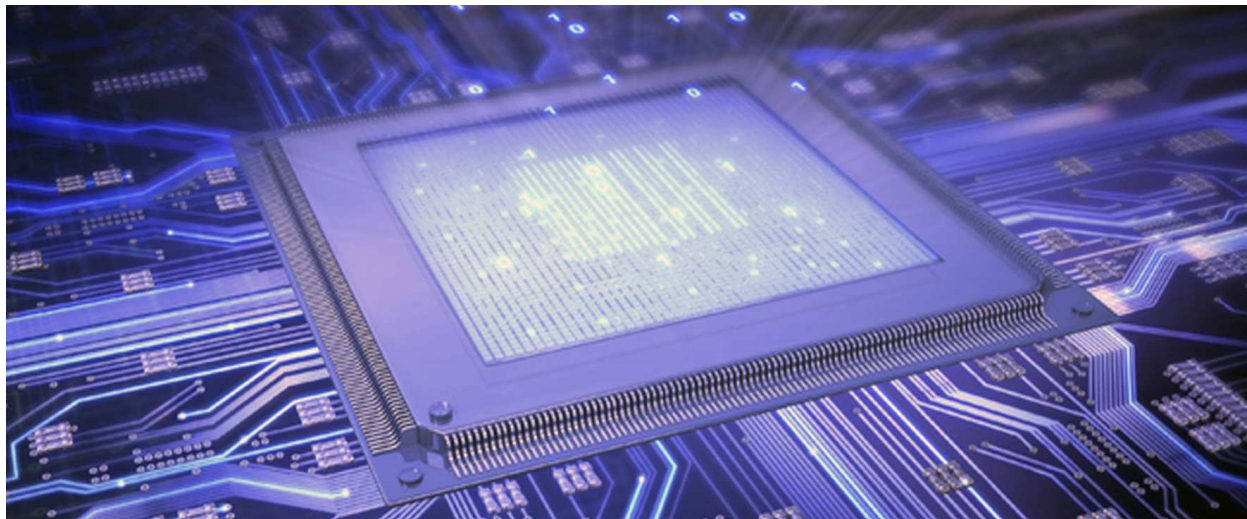




ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 629.12
EDN VUULKL

ПРИМЕРЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ КИБЕРУСТОЙЧИВОСТИ В БОРТОВЫХ ПРОГРАММАХ КОНТРОЛЯ ПАРАМЕТРОВ БЕЗОПАСНОГО МОРЕПЛАВАНИЯ

О.В. Одегова, канд. техн. наук, доцент, ООО «Валком», 196084 Россия, Санкт-Петербург, Ломаная ул., 10, e-mail: odegova@valcom.ru

В.А. Окунев, рук. проектов управления техн. экспертизы, Российский морской регистр судоходства, 191186 Россия, Санкт-Петербург, Миллионная ул., д. 7А, e-mail: okunev.va@rs-class.org

В статье рассматриваются вопросы киберустойчивости специализированного программного обеспечения, предназначенного для расчета критериев безопасного мореплавания и управления загрузкой судна. Подчеркивается, что цифровая трансформация судостроения и эксплуатации судов требует внедрения технических и организационных мер, направленных на обнаружение, реагирование и восстановление после киберинцидентов. Описаны основные киберриски, связанные с бортовым ПО: заражение вредоносными программами, сбой аппаратных средств, нарушение целостности данных и фальсификация информации, что может привести к аварийным ситуациям, экологическим катастрофам и финансовым потерям.

Рассматриваются требования классификационных обществ к киберустойчивости ПО начиная с 2024 г., а также обязанности участников жизненного цикла судна — от проектировщиков и разработчиков до судовладельцев и экипажа. Особое внимание уделено валидации данных, хранению резервных копий, управлению доступом и обновлению программного обеспечения. Предложены конкретные функции для реализации кибербезопасности при разработке бортового ПО, включая идентификацию пользователей, регистрацию событий, контроль целостности данных и восстановление системы после инцидентов. В заключение отмечается, что только системный подход и совместная работа всех участников жизненного цикла позволяют обеспечить надежную киберустойчивость судовых систем и безопасную эксплуатацию судов в современных условиях.

Ключевые слова: киберустойчивость, киберриск, валидация, безопасное мореплавание, распределение обязанностей.

Для цитирования: Одегова О.В. Примеры реализации требований киберустойчивости в бортовых программах контроля параметров безопасного мореплавания / О.В. Одегова, В.А. Окунев // Научно-технический сборник Российского морского регистра судоходства. — 2026. — Т. 56, № 2. — С. 190–198. — EDN VUULKL.

EXAMPLES OF IMPLEMENTING CYBER RESILIENCE REQUIREMENTS IN ONBOARD SOFTWARE FOR THE SAFE SEAGOING

O.V. Odegova, PhD, Associate Professor, 196084 Russia, St. Petersburg, Lomanaya ul., 10, e-mail: odegova@valcom.ru
V.A. Okunev, Project Manager, Technical Expertise Dep., Russian Maritime Register of Shipping, 191186 Russia, St. Petersburg, Millionnaya ul., 7A, e-mail: okunev.va@rs-class.org

The article addresses the issues of cyber resilience of specialized software designed to calculate the criteria of the safe seagoing and ship loading management. The digital transformation of shipbuilding and vessel operations requires the implementation of technical and organizational reactions for detecting, responding to, and recovering from cyber incidents. The main cyber risks associated with onboard software are described, including virus software, hardware failures, data integrity mistakes, and information falsification, which can lead to accidents, environmental disasters, and financial losses.

The requirements of classification societies for software cyber stability starting from 2024 are considered, as well as the responsibilities of participants in the ship's life cycle — from designers and developers to shipowners and crew. Special attention is paid to data validation, backup storage, access management, and software updates. Specific functions are proposed for implementing cybersecurity in the development of on-board software, including user identification, event logging, data integrity monitoring, and system recovery after incidents. In conclusion, it is noted that only a systematic approach and the joint work of all participants in the life cycle can ensure reliable cyber stability of ship systems and safe operation of ships in modern conditions.

Key words: *cyber resilience, cyber risk, validation, safety seagoing, distribution of responsibilities.*

For citation: Odegova O.V., Okunev V.A. Examples of implementing cyber resilience requirements in onboard software for the safe seagoing. *Research Bulletin by Russian Maritime Register of Shipping*. 2026. Vol. 56, No. 2. P. 190–198. EDN VUULKL. (In Russ.)

ВВЕДЕНИЕ

Цифровая трансформация, меняя радикально подходы к проектированию, постройке и эксплуатации судов, создает необходимость обеспечивать условие киберустойчивости как базовое для безопасной работы судна в эксплуатации. Увеличивающаяся производительность компьютерной техники и новые технологии диктуют корректировки возможностей использования современных программных комплексов на борту судна. В состав программного обеспечения (ПО) могут входить программы, обслуживающие интегрированные системы автоматизации судна, различные датчики, навигационные комплексы, расчеты количества груза, принимаемого на борт, комплексы контроля приема и расхода топлива, программы расчетов безопасных режимов мореплавания и многое другое.

Киберинциденты, связанные с бортовым ПО, могут вызывать негативные последствия — от незначительных сбоев до катастрофических сценариев разных категорий — и создавать весомые риски, угрожающие жизни и здоровью экипажа. Так, например, нарушение навигационной безопасности (потеря управления судном, подмена навигационных данных, сокрытие присутствия судна от других участников движения, отказ движительного комплекса) может привести к неверным решениям в управлении движением, что грозит посадкой на мель, столкновением с другим судном или береговой инфраструктурой. Кибератака на балластные или топливные системы может спровоцировать несанкционированный сброс балластных вод или разлив топлива, что приведет к экологическим последствиям. Нарушение целостности данных и мореходности (фальсификация картографической информации или бортовых журналов) обернется вероятностью прокладки небезопасного маршрута или сокрытием следов аварии, а повреждение цифровой модели судна, заложенной в расчет параметров безопасного мореплавания приведет к недостоверным расчетам остойчивости и прочности судна. Если критически важное для эксплуатации ПО выведено из строя, судно может быть объявлено немореходным и задержано в порту, а искажение коммерческих данных рейсовых заданий или коносаментов приведет к срыву сроков поставки, что повлечет за собой эксплуатационные, репутационные и финансовые потери.

Вместе с тем русскоязычной информации, связанной с реализацией конкретных вопросов обеспечения кибербезопасности в процессе эксплуатации судна, крайне мало.

Предлагаемые в данной статье подходы имеют своей целью уточнение представлений о киберустойчивости специализированного ПО [1], предназначенного для выполнения расчетов критериев безопасного мореплавания в текущем состоянии загрузки судна, а также определение ролей участников жизненного цикла судна, имеющих дело с таким ПО.

Расширяя определение, данное в [2], под киберустойчивостью в данном случае можно понимать наличие на судне технических и организационных мер для обнаружения, реагирования и восстановления ПО после инцидентов, способность адаптироваться и извлекать из них уроки, а также способность ПО работать в условиях кибератаки или другого киберинцидента.

1. ОБЩИЕ ТРЕБОВАНИЯ К КИБЕРУСТОЙЧИВОСТИ

Классификационные общества с каждым годом уделяют все большее внимание вопросам киберустойчивости программного обеспечения.

Общие требования по киберустойчивости регламентируются Требованиями Регистра [3]. Требования эти применяются к судам и морским сооружениям, контракт на постройку которых заключен с 1 июля 2024 г. (пассажирские суда и грузовые (обычные и высокоскоростные) валовой вместимостью 500 т, совершающие международные рейсы, а также плавучие буровые установки валовой вместимостью 500 и более и самоходные плавучие морские установки). Но по желанию заказчика эти требования могут быть применены и к иным судам.

Правила относятся к любому программному обеспечению, используемому на судах, в том числе к ПО контроля загрузки судна, предназначенного для расчетов безопасных режимов мореплавания.

2. КИБЕРРИСКИ

Бортовую программу расчета параметров безопасного мореплавания можно классифицировать как систему информационных технологий, то есть как систему, ориентированную на использование данных в качестве информации [4]. В настоящее время наиболее вероятным риском для программного обеспечения, предназначенного для расчетов безопасных режимов мореплавания, является заражение компьютера вредоносным ПО (программы-вымогатели, трояны, вирусы и т.д.) [5] или сбой работы аппаратных средств. Источниками заражения вредоносным ПО могут быть:

- электронная почта;
- переносные USB-накопители данных; переносные мобильные устройства, подключаемые к компьютеризированным системам для обслуживания;
- персональные мобильные устройства, которые могут подключаться экипажем к компьютеризированным системам.

Кибернезащищенность информационной системы несет в себе угрозы как злонамеренных вмешательств (например, взлом или внедрение вредоносного кода), так и непреднамеренных последствий незащищенных действий (например, предоставление разрешений пользователям, не обладающим необходимыми уровнями доступа и компетенциями). В этом смысле ПО может также стать источником уязвимости системы.

ПО контроля загрузки судна [6] может быть установлено на отдельном offline компьютере или поставляться в составе системы автоматизации, когда текущее состояние загрузки, связанное, например, с жидкими грузами, передается в программу с датчиков, установленных в танках и цистернах судна (рис. 1).

Принимая во внимание, что данные в режиме online поступают от компьютеризированной грузовой системы, нарушение работы которой в результате киберинцидента также может повлиять на работу прибора загрузки судна, в ПО расчета параметров безопасного мореплавания целесообразно предусматривать опцию контроля передаваемых данных и информировать пользователя в случае их искажения или повреждения.

Для всех участников жизненного цикла судна существует ряд обязанностей, которые помогают организовать систему защиты от киберинцидентов или их последствий.

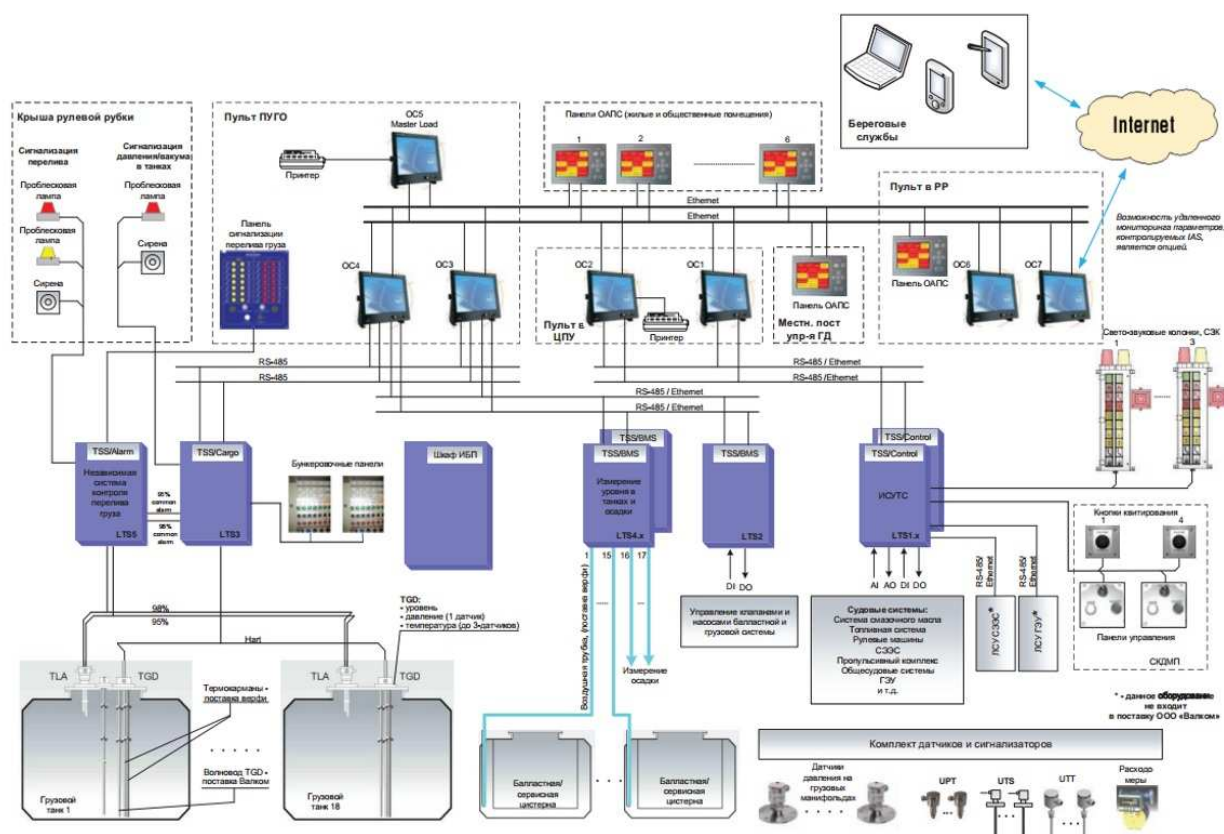


Рис. 1. Схема системы автоматизации судна с грузовым компьютером

3. ВАЛИДАЦИЯ ДАННЫХ

Хранение исходных кодов критически важного ПО — это комплексная процедура разработчика, включающая в себя резервирование и копирование (с применением, например, стратегии комбинирования этапов полного и дифференцированного копирования), а также регулярное тестирование кода. Такой подход гарантирует минимизацию потерь данных в случае киберинцидента на компьютере разработчика. В прямую обязанность разработчика входит хранение ПО для конкретного судна как в период его подготовки, так и при осуществлении гарантии.

Основой информационной части бортовой программы расчета параметров безопасного мореплавания является цифровая модель судна, которая строится на этапе подготовки ПО на базе документов, предоставляемых проектантом. Эта цифровая модель включает в себя геометрию корпуса судна, данные по нагрузке судна порожнем, кривые элементов помещений, участвующих в расчете аварийной остойчивости, а также данные по грузовым помещениям, танкам и цистернам судна. На базе модели судна выполняются расчеты остойчивости и прочности в любом состоянии загрузки. Одной из наиболее важных задач, связанных с разработкой ПО для каждого конкретного судна, является валидация данных, которая позволяет убедиться, что построенная цифровая модель действительно адекватно решает необходимые расчетные задачи и удовлетворяет потребности конечного потребителя продукта — экипажа судна при эксплуатации.

В российском судостроении отсутствуют требования соблюдения стандартов передачи данных между участниками жизненного цикла судна и доступности информации о судовой поверхности и помещениях. Поэтому разработчику бортового ПО приходится проводить моделирование, работая с чертежами поверхности и общего расположения от проектанта в самых разных форматах, включая документы в формате pdf, что не позволяет говорить об унифицированном использовании электронной модели. При наличии сложных по геометрии помещений «альтернативное моделирование», выполняемое разработчиком бортового ПО, приводит к созданию модели, определяющей разницу расчетов проектанта и разработчика ПО. Особенно сложным оказывается моделирование «пустых» (void) помещений, в том случае, когда в проектной документации, передаваемой проектантом, отсутствует информация о геометрических элементах этих помещений [7].

При реализации российского проекта «Доработка и внедрение отечественной судостроительной системы автоматизированного проектирования тяжелого класса как среды проектирования и конструкторско-технологической подготовки производства» должна появиться система автоматизированного проектирования, которая будет охватывать жизненный цикл судна с наполнением и уточнением данных электронной модели на всех его этапах, обеспечивая цифровую непрерывность и актуальность информации.

Правилами классификационного общества [8, с. 35–36, 40] регламентируется диапазон погрешностей, допустимых при расчетах. После построения цифровой модели, основанной на данных проектанта, производителю ПО необходимо оценивать каждый расчетный параметр на совпадение с расчетом, выполненным проектантом и отображенным в «Информации по остойчивости и аварийной остойчивости» для судна. Дополнительную верификацию осуществляет инспектор классификационного общества в момент одобрения ПО для конкретного судна с выдачей акта по форме 6.3.29. Кроме этого, после установки выполняются сдаточные испытания ПО в присутствии инспектора Регистра на борту в соответствии с п. 12.2.5 [8, с. 30]. Эти мероприятия гарантируют, что на момент сдачи (то есть перехода ПО от разработчика непосредственно под контроль экипажа судна) все необходимые условия работоспособности и аутентичности ПО соблюдены.

Риск повреждения цифровой модели судна в процессе эксплуатации может привести как к полному нарушению работоспособности ПО, так и к некорректности в расчетах и, как следствие, к принятию ошибочного решения о возможности выхода судна в рейс в текущем состоянии загрузки. Проверка ПО после установки, выполняемая экипажем совместно с инспектором Регистра, о которой говорилось выше, позволяет снизить риск возникновения киберинцидента, связанного с порчей или неадекватностью цифровой модели судна, и полностью ее верифицировать. После завершения тестирования программного обеспечения, установленного на судне, создаются резервные копии ПО, которые передаются судовладельцу. Сохранность и доступность резервных копий, а также выполнение восстановления программного обеспечения в случае его повреждения возлагается на пользователя ПО с учетом необходимости выполнения функций в эксплуатации, описанных в табл. 1. Однако на практике в процессе эксплуатации со стороны пользователей не уделяется надлежащее внимание мерам для сохранности резервных копий, и судовладелец вынужден обращаться к разработчику бортового ПО для восстановления программ после киберинцидентов, что влияет на оперативность восстановления ПО и возможность судна выполнять свои функции. Учитывая это, разработчик, в целях обеспечения киберустойчивости ПО, может оказывать услуги по хранению резервных копий и организации судовладельцу оперативного доступа к ним на всем жизненном цикле судна.

4. ОБЯЗАННОСТИ СУДОВЛАДЕЛЬЦА

Основным документом судовладельца в части обеспечения кибербезопасности должна стать *Программа кибербезопасности и киберустойчивости судна*, в которой детализированы требования Политики, проводимой судовладельцем в этой связи (далее — Программа), и которая одобряется Регистром. Эффективное управление киберрисками должно начинаться на уровне высшего руководства судоходной компании, которое внедряет культуру осознания киберрисков на всех уровнях организации и обеспечивает целостный и гибкий режим управления киберрисками, который постоянно функционирует и оценивается с помощью эффективных механизмов обратной связи. Каждый риск должен быть оценен по своей значимости и возможным последствиям, а также с точки зрения оперативности восстановления ПО.

Например, когда ПО установлено на отдельном компьютере, на котором нет возможности использования съемных носителей и который не имеет выхода в Интернет, риск кибератаки становится минимальным, а возможным риском следует считать некорректные действия экипажа, которые могут привести к отказу программно-аппаратных средств. Киберриск для компьютера, являющегося частью судовой компьютерной системы, выше, чем для обособленного компьютера, установленного вне судовой сети и изолированного от системы. Однако в такой ситуации становится невозможным восстановить ПО дистанционно или с помощью внешних носителей, что увеличивает время реакции на инцидент, а использование обособленного компьютера лишает судовладельца возможности получения данных о заполнении танков и цистерн судна в режиме online, что очевидно увеличивает время ввода данных по загрузке судна и выполнения расчетов. Подобные рассуждения и оценки должны лечь в основу оценки рисков и возможностей, выполняемых судовладельцем, и привести к формированию списка мероприятий в Программе для описания процесса управления изменениями для ПО, предназначенного для обеспечения безопасности мореплавания и компьютера, на котором это ПО установлено.

Таким образом, в результате оценки возможных рисков для ПО в Программе кибербезопасности и киберустойчивости судна должны появиться:

- определение киберрисков для ПО с описанием возможных последствий, которые в случае сбоя в работе создают риски для судовых операций;
- роль и обязанности персонала по управлению киберрисками; планирование действий в чрезвычайных ситуациях для обеспечения непрерывности судоходных операций;
- разработка и реализация мероприятий по восстановлению ПО;
- определение мер по резервному копированию в целях предупреждения последствий наступления киберинцидента.

Кроме этого, программа кибербезопасности, разрабатываемая судовладельцем, должна включать в себя описание ряда принятых правил для рассматриваемого типа ПО, например:

- управления доступом и обслуживанием (обновлением). В этом смысле может быть рекомендовано обновление ПО только как замена на новую версию (которая также защищена соответствующим Актом проверки классификационного общества) или как восстановление с проверенного источника предыдущей версии;

- использования съемных носителей и сетевого доступа;
- наименьших привилегий (физическому лицу, допущенному к работе с ПО, должны предоставляться только минимальные привилегии, достаточные для выполнения функций, возложенных на это лицо),
- паролей.

В итоге ПО расчетов критериев безопасного мореплавания должно поддерживаться и обновляться в соответствии с процессом по управлению обслуживанием ПО и Политикой обновления, описанным судовладельцем в Программе.

5. ОБЯЗАННОСТИ РАЗРАБОТЧИКА ПО

Разработчику ПО следует сформулировать ряд функций, которые должны быть реализованы для минимизации рисков при кибератаке. Эти требования приведены в табл. 1.

Таблица 1

Реализация требований кибербезопасности при разработке бортового ПО

№	Наименование функции	Реализация требования при разработке ПО
1	Идентификация пользователей в соответствии с правами доступа, отраженными в ведомости судовых КС	Идентификация и аутентификация всех пользователей, которые могут получить доступ к системе напрямую или через удаленные интерфейсы (при их наличии), реализуются запросом пароля при каждом новом обращении к ПО, что предполагает возможность ввода и сохранения надежных паролей для каждого отдельного пользователя, определенного в Программе
2	Управление учетными записями, обеспечивающее защиту от несанкционированного доступа неуполномоченных лиц на судне или от внешних атак	Управление всеми учетными записями авторизованных пользователей, ведение системы паролей и ключей (в том числе с учетом разделения пользователей по уровням доступа, как это будет описано в Программе), включая добавление, активацию, изменение, деактивацию и удаление учетных записей для сдерживания последствий потенциального инцидента, реализуется как отдельный модуль, являющийся составной частью ПО, и предполагает наличие управляемой базы данных авторизованных пользователей
3	Надежность аутентификации по паролю и скрытность при аутентификации	Для зарегистрированных пользователей реализуется настраиваемая надежность конфигурируемых паролей на основе минимальной длины и разнотипности символов, пароль при вводе должен быть скрыт
4	Регистрация событий	События, относящиеся к безопасности (например, запуск ПО, управление доступом, сбой или перезагрузки операционной системы, изменения конфигурации, потеря связи), регистрируются как записи во вспомогательном файле-журнале, сопровождающем ПО, с возможностью предупреждения о переполнении ресурса, используемого для хранения. Журнал доступен в режиме «только чтение» авторизованным физическим лицам и/или инструментам
5	Целостность коммуникации в режиме online	При передаче данных в ПО в режиме online (текущее заполнение танков и цистерн судна) контролируется чистота информации в соответствии с форматом передачи. В случае передачи неформатных данных предупреждение об этом выводится оператору и регистрируется anomальное событие
6	Управление ресурсами	Во избежание переполнения ресурсов ПО предусматривает хранение планов предыдущих рейсов в количестве, определенном судовладельцем в момент заказа ПО, и выдает предупреждение о необходимости перенести старые планы в дополнительное хранилище, если возникает ситуация переполнения ресурса

Продолжение — табл. 1

№	Наименование функции	Реализация требования при разработке ПО
7	Восстановление работоспособности в случае, если функционал ПО был нарушен в результате киберинцидента	В сопроводительной документации описывается возможность создания резервных копий на уровне пользователя и системы (включая информацию о состоянии системы). Например, это может быть требование о создании трех копий данных установочной версии и сохранения их на двух разных типах носителей, при этом одна из копий должна находиться за пределами основного места хранения. Условия авторизованного доступа описываются в Программе. После сбоя или отказа ПО авторизованный пользователь может выполнить его восстановление в соответствии с инструкцией пользователя, поставляемой вместе с ПО

6. ОБЯЗАННОСТИ УЧАСТНИКОВ ЖИЗНЕННОГО ЦИКЛА

Дополнительно к функциям, реализуемым разработчиком ПО и указанным в табл. 1, большое значение имеют также аппаратные меры, которые должны быть приняты во внимание для компьютеров, на которых установлено ПО:

- наличие альтернативного источника питания и возможности переключения устройства на него и обратно без влияния на существующий уровень безопасности. Альтернативный источник питания должен обеспечить время работы, позволяющее провести сохранение результатов текущего сеанса и завершить его безаварийно;
- возможность применения защитных мер для предотвращения, обнаружения и уменьшения воздействий вредоносного кода или неавторизованного ПО, в частности, с учетом того, что ПО расчета безопасных режимов мореплавания является замкнутой системой и не общается с внешними устройствами по сети, достаточно опломбировать внешние порты USB от внешнего доступа.

В жизненном цикле ПО, предназначенного для выполнения расчетов критериев безопасного мореплавания в текущем состоянии загрузки судна, участвуют несколько субъектов. Роль и ответственность каждого из них может быть детализирована в соответствии табл. 2.

Таблица 2

Роль и ответственность участников жизненного цикла

Завод-строитель	Производитель ПО	Судовладелец	Экипаж
Составить ведомость судовых компьютерных средств, использованных при поставке	Поддерживать условия безопасного хранения критически важных кодов ПО. Обеспечить ввод данных цифровой модели судна с возможностью ее верификации. Обеспечить безопасное хранение кодов и моделей в период гарантийного срока. Обеспечить возможности защищенной работы с ПО, описанные в табл. 1 Обеспечить своевременное информирование пользователей и обновление в случае выявления уязвимостей или ошибок в ПО, находящемся в эксплуатации	Выполнить оценку рисков и разработать Программу кибербезопасности и киберустойчивости судна, с детализацией требований Политики, описанных выше. Одобрить Программу в классификационном обществе, поддерживать ее в актуальном состоянии, предъявлять при ежегодных освидетельствованиях	Поддерживать в актуальном состоянии ведомость судовых компьютерных средств. Проводить обновление ПО в соответствии с Политикой обновления, описанной в Программе

ЗАКЛЮЧЕНИЕ

Для обеспечения киберустойчивости ПО необходим системный подход, в котором важна роль каждого из участников жизненного цикла судна. Поэтому недостаточно приобрести судовую компьютеризированную систему, удовлетворяющую требованиям кибербезопасности на момент изготовления и ввода в эксплуатацию, — нужно реализовывать меры по поддержанию надлежащего уровня киберустойчивости судовых систем на постоянной основе в процессе эксплуатации. Кроме этого, важен общий понятийный аппарат и взаимоувязанная терминология, позволяющая всем участникам правильно понимать концепцию построения информационных и коммуникационных инфраструктур, созданных в целях защиты от потенциальных киберугроз [9–12].

Развитие культуры кибербезопасности и механизмов защиты ПО для судов в эксплуатации становится одной из приоритетных задач всех участников жизненного цикла. Только при совместной работе над выполнением условий, необходимых для обеспечения кибербезопасности, такая система на судне будет надежно выполнять свою роль. С учетом этого в статье описаны основные решения, обеспечивающие минимизацию рисков для бортового ПО при кибератаках и определена роль участников жизненного цикла судна. Эти решения проверены при создании специализированного ПО ООО «Валком», предназначенного для выполнения расчетов критериев безопасного мореплавания в текущем состоянии загрузки судна.

СПИСОК ЛИТЕРАТУРЫ

1. Кутейников М.А. Приборы контроля остойчивости. Современные требования / М.А. Кутейников, В.С. Одегов // Научно-технический сборник Российского морского регистра судоходства. — 2016. — № 42/43. — С. 64–69. — EDN WDKNDN.
2. Руководство по обеспечению кибербезопасности / Российский морской регистр судоходства. — СПб., 2021.
3. Правила классификации и постройки морских судов. Часть XXI. Киберустойчивость / Российский морской регистр судоходства. — СПб., 2025.
4. Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2 7, June 2022.
5. Окунев В.А. Нормативные документы по обеспечению кибербезопасности и киберустойчивости морских судов / В.А. Окунев // Научно-технический сборник Российского морского регистра судоходства. — 2024. — № 74. — С. 79–82. — EDN GTFBPC.
6. Сулов А.Н. Влияние исходных данных математической модели бортовых программ на безопасность мореплавания / А.Н. Сулов, О.В. Одегова, Е.А. Жук // Морские интеллектуальные технологии. — 2025. — № 3-1(69). — С. 15–21. — DOI 10.37220/MIT.2025.693.015. — EDN RROXDG.
7. Колмогорцев Е.Л. Опережая время: «Валком» — 25 лет реализации собственных идей / Е.Л. Колмогорцев // Korabel.ru. — 2023. — №1 (59). — С. 154–155.
8. Правила технического наблюдения за постройкой судов и изготовлением материалов и изделий для судов. Часть II. Техническая документация / Российский морской регистр судоходства. — СПб., 2026.
9. Семенов С. Морская кибербезопасность — ситуация, проблемы и риски/ С. Семенов // РСМД. — 8 сент. 2020. — [Электронный ресурс] URL: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/> (дата обращения 16.07.2026).
10. Кляхин В.Н. Обеспечение информационной безопасности процесса полигонных испытаний кораблей и систем вооружений / В.Н. Кляхин, А.Б. Фомичев, С.Г. Чулкин // Судостроение. — 2019. — № 5(846). — С. 49–51. — EDN ZWXXQX.
11. Окунев В.А. Кибербезопасность на морских судах / В.А. Окунев // Сборник научных статей Нац. науч.-практ. конф. проф.-преп. состава ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова», Санкт-Петербург, 30 сент. — 20 окт. 2024 г. — СПб.: ГУМРФ им. адм. С.О. Макарова, 2025. — С. 236–239. — EDN BWRIVO.
12. Волков В.В. Модели кибератак на сеть автоматической идентификационной системы / В.В. Волков, Е.О. Ольховик, Ю.С. Федосенко // Вестник Государственного университета морского и речного флота им. адмирала С.О. Макарова. — 2025. — Т. 17, № 5. — С. 641–652. — DOI 10.21821/2309-5180-2025-17-5-641-652. — EDN DKQYLH.

REFERENCES

1. Kuteynikov M.A., Odegov V.S. Stability control instruments. Up-to-date requirements. *Research Bulletin by Russian Maritime Register of Shipping*. 2016. No. 42/43. P. 64–69. EDN WDKNDN. (In Russ.)
2. Guidelines on Cyber Safety / Russian Maritime Register of Shipping. St. Petersburg, 2021.
3. Rules for the Classification and Construction of Sea-Going Ships. Part XXI. Cyber Resilience / Russian Maritime Register of Shipping. St. Petersburg, 2025.
4. Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2 7, June 2022.
5. Okunev V.A. Regulatory documents on cybersecurity and cyber resilience of sea-going ships. *Research Bulletin by Russian Maritime Register of Shipping*. 2024. No. 74. P. 79–82. EDN GTFBPC. (In Russ.)
6. Suslov A.N., Odegova O.V., Zhuk E.A. The influence of the initial data of the mathematical model of onboard programs on the safety of navigation. *Marine Intellectual Technologies*. 2025. No. 3-1(69) P. 15–21. DOI 10.37220/MIT.2025.693.015. EDN RROXDG. (In Russ.)
7. Kolmogortsev E.L. Operezhayaya vremena: «Valkom» — 25 let realizatsii sobstvennykh idei [Ahead of the Curve: Valkom — 25 Years of Bringing Its Own Ideas to Life]. *Korabel.ru*. 2023. No. 1 (59). P. 154–155.
8. Rules for Technical Supervision during Construction of Ships and Manufacture of Materials and Products for Ships. Part II. Technical Documentation / Russian Maritime Register of Shipping. St. Petersburg, 2026.
9. Semenov S. Morskaya kiberbezopasnost' — situatsiya, problemy i riski [Marine cybersecurity: current situation, problems, and risks]. *RIAC*. Sept. 8, 2020. URL: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/> (accessed 16.07.2026).
10. Klyakhin V.N., Fomichev A.B., Chulkin S.G. Ensuring information safety during field trials of ships and weapon systems. *Sudostroenie [Shipbuilding]*. 2019. No. 5(846). P. 49–51. EDN ZWXXQX. (In Russ.)
11. Okunev V.A. Cybersecurity on ships. *Sbornik nauchnykh statei Nats. nauch.-prakt. konf. prof.-prep. sostava FGBOU VO "GUMRF im. adm. S.O. Makarova [Proceedings of the National Science and Pract. Conf. of the Faculty Members of Admiral Makarov State University of Maritime and Inland Shipping, Sept. 30 — Oct. 20, 2025]*. St. Petersburg: Izd-vo GUMRF im. adm. S.O. Makarova, 2025. P. 236–239. EDN BWRIVO. (In Russ.)
12. Volkov V.V., Ol'khovik E.O., Fedosenko Yu.S. Models of cyberattacks on the automatic identification system network. *Vestnik Gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S.O. Makarova*. 2025. Vol. 17, No. 5. P. 641–652. DOI: 10.21821/2309-5180-2025-17-5-641-652. EDN DKQYLH.

Статья поступила в редакцию 14.04.2026.

Принята к публикации 31.05.2026.