РОССИЙСКИЙ МОРСКОЙ РЕГИСТР СУДОХОДСТВА

Версия: 01.07.2024

ПРАВИЛА

КЛАССИФИКАЦИИ И ПОСТРОЙКИ МОРСКИХ СУДОВ

ЧАСТЬ XXI

КИБЕРУСТОЙЧИВОСТЬ

НД № 2-020101-174

Санкт-Петербург

ПРАВИЛА КЛАССИФИКАЦИИ И ПОСТРОЙКИ МОРСКИХ СУДОВ (ЧАСТЬ XXI)

Настоящая версия части XXI «Киберустойчивость» Правил классификации и постройки морских судов Российского морского регистра судоходства (РС, Регистр) разработана на основании унифицированных требований МАКО E26 (Rev.1 Nov 2023) и E27 (Rev.1 Sep 2023), утверждена в соответствии с действующим положением и вступает в силу 1 июля 2024 года.

ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ[1]

Для данной версии нет изменений для включения в Перечень.

[1] За исключением изменений и дополнений, вводимых Бюллетенями, а также опечаток.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1.1 Требования настоящей части применяются к следующим судам и морским сооружениям[1], контракт на постройку которых заключен 1 июля 2024 года или после этой даты:

.1 пассажирские суда (в том числе высокоскоростные пассажирские суда), совершающие международные рейсы;

.2 грузовые суда валовой вместимостью 500 и более, совершающие международные рейсы;

.3 высокоскоростные грузовые суда валовой вместимостью 500 и более, совершающие международные рейсы;

.4 плавучие буровые установки валовой вместимостью 500 и более;

.5 самоходные плавучие морские установки.

1.1.2 По желанию заказчика требования настоящей части могут быть применены к:

.1 военным кораблям;

.2 грузовым судам валовой вместимостью менее 500 (в том числе высокоскоростным);

.3 судам, не имеющим механических средств движения;

.4 деревянным судам примитивной конструкции;

.5 прогулочным яхтам, не занятым в коммерческих перевозках;

.6 рыболовным судам;

.7 иным судам и морским сооружениям, не указанным в 1.1.1.

1.1.3 Требования настоящей части применяются к судовым ОТ-системам (т.е. к компьютеризированным системам (КС)), использующим данные для управления и/или контроля физических процессов), которые могут быть уязвимы для киберинцидентов, и компрометация которых может привести к возникновению опасных ситуаций для безопасности людей, безопасности судна, и/или представляющих угрозу для окружающей среды.

1.1.4 В частности, требования применяются к КС, используемым для выполнения следующих функций и работы нижеперечисленных систем судна, если они имеются на борту:

.1 система управления пропульсивной установкой;

.2 система управления рулевым устройством;

.3 постановка на якорь и швартовка;

.4 производство и распределение электроэнергии;

.5 система обнаружения и тушения пожара;

.6 система обработки груза;

.7 осушительная и балластная системы;

.8 прибор контроля загрузки;

.9 система сигнализации водонепроницаемых дверей и система обнаружения затопления;

.10 освещение (аварийное, низкорасположенное, сигнально-отличительные фонари и т.д.);

---

[1] В дальнейшем — суда.

.11 любая другая обязательная система, отказ или неисправность которой может представлять риски для эксплуатации судна (например, система аварийного отключения, система безопасности груза, система защиты сосудов под давлением, система обнаружения газа и т.д.).

1.1.5 Дополнительно в область применения настоящей части включены следующие системы:

.1 навигационные системы, требуемые в соответствии с положениями конвенций;

.2 системы внутрисудовой связи и системы радиосвязи, требуемые правилами РС и положениями конвенций.

Примечание. К системам навигации и радиосвязи допускается применение стандарта IEC 61162-460:2024 или других эквивалентных стандартов вместо требований 3.3 при условии выполнении требований разд. 2.

1.1.6 Требования настоящей части также применяются к любому сетевому интерфейсу на основе интернет-протокола (IP) от КС, входящих в область применения настоящей части, к другим системам, таким как:

.1 системы обслуживания пассажиров и посетителей;

.2 компьютерные сети, предназначенные для пассажиров;

.3 административные сети;

.4 системы, обеспечивающие жизнедеятельность экипажа;

.5 любые другие системы, постоянно или временно (например, во время технического обслуживания) подключенные к ОТ-системам.

1.1.7 Категории КС определены в 7.9.4 части XV «Автоматизация» на основе последствий отказа системы для безопасности людей, безопасности судна и/или угрозы для окружающей среды.

1.1.8 Судам, отвечающим требованиям настоящей части, к основному символу класса добавляется знак **CYBER**, указанный в 2.2.64 части I «Классификация».

1.2 ОПРЕДЕЛЕНИЯ И ПОЯСНЕНИЯ

Определения и пояснения, относящиеся к общей терминологии Правил классификации и постройки морских судов[1], указаны в части I «Классификация».

В настоящей части приняты следующие определения и пояснения.

Аутентификация (Authentication) — обеспечение гарантии того, что заявленные характеристики субъекта или объекта являются подлинными.

Виртуальная частная сеть (Virtual private network (VPN)) — виртуальная сеть, построенная поверх существующих физических сетей, которая обеспечивает безопасный коммуникационный туннель для данных, передаваемых между сетями или устройствами с использованием туннелирования, средств контроля безопасности и трансляции конечных адресов, подобно подключению по выделенной линии.

Восстановление (Recovery) — разработка и внедрение надлежащих мер и мероприятий для поддержания устойчивости и сохранения любых функциональных возможностей, которые были нарушены в результате киберинцидента. Функция восстановления поддерживает своевременное возвращение к нормальной работе КС, чтобы уменьшить последствия от киберинцидента.

Вредоносное действие (Offensive cyber manoeuvre) — действие, которое приводит к отказу, деградации, нарушению функционирования, разрушению OT- или IT-систем или манипулированию ими.

Зона безопасности (Security zone) — совокупность подключенных КС, входящих в область применения данного раздела, для которых требуется одна и та же политика управления доступом. Каждая зона состоит из одного интерфейса или группы интерфейсов, к которым применяется политика управления доступом.

Интегрированная система (Integrated system) — система, объединяющая ряд взаимодействующих подсистем и/или оборудования, организованных для достижения одной или нескольких определенных целей.

Информационная технология (Information technology (IT)) — устройства, программное обеспечение (ПО) и связанные с ними сети, ориентированные на использование данных в качестве информации, в отличие от операционной технологии (OT).

Категории систем (I, II, III) (System categories (I, II, III)) — категории систем присваиваются на основе влияния их отказа на возникновение опасных ситуаций для безопасности людей, безопасности судна и/или угрозы для окружающей среды, как указано в 7.9.4 части XV «Автоматизация».

Киберинцидент (Cyber incident) — инцидент, возникающий в результате любого преднамеренного или непреднамеренного вредоносного действия, затрагивающего одну или несколько судовых КС или направленного на их атаку, и который фактически или потенциально приводит к негативным последствиям для судовой системы, сети, компьютера или информации, которую они обрабатывают, хранят или передают, и что может потребовать ответных действий для устранения последствий. Киберинциденты включают в себя несанкционированный доступ, нецелевое использование, изменение, уничтожение или ненадлежащее раскрытие информации, формируемой, архивируемой или используемой в КС или передаваемой в сетях, соединяющих такие системы. Системные сбои, вызванные иными причинами, не являются киберинцидентами.

---

[1] В дальнейшем — настоящие Правила.

Киберустойчивость (Cyber resilience) — способность сокращать случаи возникновения и уменьшать последствия киберинцидентов, возникающих в результате нарушения или ухудшения операционной технологии (ОТ), используемой для безопасной эксплуатации судна, которые потенциально могут привести к возникновению опасных ситуаций для безопасности людей, безопасности судна и/или угрозе для окружающей среды.

Компенсирующая мера (Compensating countermeasure) — альтернативное решение по противодействию, используемое вместо заложенных функциональных возможностей обеспечения безопасности для удовлетворения одного или нескольких требований безопасности или в дополнение к ним.

Компрометация данных (Data compromise) — нарушение безопасности, которое приводит к случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к защищаемым данным, передаваемым, хранимым или обрабатываемым иным образом.

Компьютеризированная система (КС) (Computer based system (CBS)) — программируемое электронное устройство или взаимосвязанный комплекс программируемых электронных устройств, сконструированный для достижения одной или нескольких определенных целей, таких как сбор, обработка, обслуживание, использование, обмен, распространение или удаление информации. Судовые КС включают в себя IT- и OT-системы. КС может представлять собой комбинацию подсистем, соединенных по сети. Судовые КС могут быть подключены напрямую или через общедоступные средства связи (например, Интернет) к береговым КС, к КС и/или иным устройствам других судов.

Контроль (Control) — средства управления рисками, включая политику, процедуры, руководства, практику или организационные структуры, которые могут быть административными, техническими, управленческими или юридическими по своей природе.

Логический сегмент сети (Logical network segment) — то же самое, что и сегмент сети, при этом два или более логических сегмента сети используют одни и те же физические компоненты.

Межсетевой экран (Firewall) — логический или физический барьер, управляемый с помощью заранее определенных правил, для отслеживания и контроля входящего и исходящего сетевых трафиков.

Микропрограмма (Firmware) — программное обеспечение (ПО), встроенное в электронные устройства и обеспечивающее управление, контроль и обработку данных специализированных устройств и систем. Обычно оно автономно и недоступно для действий пользователя.

Ненадежная сеть (Untrusted network) — любая сеть, не входящая в область применения настоящей части.

Операционная технология (Operational technology (OT)) — устройства, датчики, программное обеспечение (ПО) и связанные с ними сети, которые контролируют судовые системы и управляют ими. Системы, относящиеся к операционным технологиям, можно рассматривать как ориентированные на использовании данных для управления или контроля физических процессов.

OT-система (OT system) — компьютеризированная система, обеспечивающая функции управления, сигнализации, контроля, защиты или внутренней связи.

Патч (Patch) — программное обеспечение (ПО), предназначенное для обновления установленного ПО или вспомогательных данных с целью устранения уязвимостей безопасности и других ошибок или улучшения операционных систем или приложений.

Поверхность атаки (Attack surface) — набор всех возможных точек, в которых неавторизованный пользователь может получить доступ к системе, оказать на нее воздействие или извлечь из нее данные. Поверхность атаки включает в себя две категории: цифровую и физическую:

цифровая поверхность атаки (digital attack surface) охватывает все аппаратное и программное обеспечение, которое подключается к сети организации, включая приложения, коды, порты, серверы и веб-сайты;

физическая поверхность атаки (physical attack surface) включает в себя все оконечные устройства, к которым злоумышленник может получить физический доступ, например, настольные компьютеры, жесткие диски, ноутбуки, мобильные телефоны, съемные диски и небрежно выброшенное оборудование.

Поставщик (Supplier) — изготовитель или поставщик аппаратных и/или программных продуктов, компонентов системы или оборудования (аппаратного или программного), состоящего из приложения, встроенных устройств, сетевых устройств, хост-устройств и т.д., работающих вместе как система или подсистема. Поставщик несет ответственность за предоставление системному интегратору программируемых устройств, подсистем или систем.

Протокол (Protocol) — общий свод правил и сигналов, используемых компьютерами в сети для обмена данными. При помощи протоколов осуществляются передача данных, управление сетью и безопасность. В судовых сетях обычно используются протоколы на основе стека TCP/IP и различные полевые шины.

Сегмент сети (Network segment) — совокупность узлов, имеющих один и тот же план сетевых адресов. Сегмент сети является широковещательным доменом.

Примечание. В стеке протоколов TCP/IP план сетевых адресов имеет префикс из их IP-адресов и сетевой маски. Связь между сегментами сети возможна только при использовании службы маршрутизации на сетевом уровне (уровень 3 сетевой модели OSI).

Сетевой коммутатор (коммутатор) (Network switch (Switch)) — устройство, соединяющее элементы в компьютерной сети с помощью коммутации пакетов для приема, обработки и передачи данных на устройство назначения.

Сеть (Network) — соединение между двумя или более компьютерами с целью электронной передачи данных с помощью согласованных протоколов связи.

Система (System) — совокупность взаимодействующих программируемых устройств и/или подсистем, организованных для достижения одной или нескольких определенных целей.

Системный интегратор (System integrator) — конкретное лицо или организация, ответственные за интеграцию систем и изделий, предоставленных поставщиками, в систему, предусмотренную требованиями спецификации судна, а также за предоставление интегрированной системы. Системный интегратор также может быть ответственным за интеграцию систем на судне. До поставки судна эту роль должна взять на себя верфь, если только альтернативная организация не заключила специальный контракт/не приняла на себя эту ответственность.

Службы ответственного назначения (Essential services) — службы, обеспечивающие движение, рулевое управление, а также безопасность судна. Службы ответственного назначения подразделяются на первичные и вторичные:

первичные службы ответственного назначения (primary essential services) — это службы, которые должны непрерывно работать для поддержания движения и рулевого управления;

вторичные службы ответственного назначения (secondary essential services) — это службы, которые необязательно должны непрерывно работать для обеспечения движения и рулевого управления, но которые необходимы для поддержания безопасности судна.

Судовладелец/Компания (Shipowner/Company)[1] — владелец судна или любая другая организация или лицо, такое, как управляющий, агент или фрахтователь по бербоут-чартеру, которые приняли на себя ответственность за эксплуатацию судна от судовладельца и которые при этом согласились принять на себя все обязанности и всю ответственность. На начальном этапе постройки судовладельцем может быть верфь или системный интегратор (строитель или верфь). После сдачи судна владелец может делегировать некоторые обязанности компании, управляющей судном.

Усиление защиты (Hardening) — практика снижения уязвимости системы путем уменьшения ее поверхности атаки.

Эшелонированная защита (Defence in depth) — стратегия информационной безопасности, объединяющая человеческие, технологические и операционные возможности для создания переменных барьеров на нескольких уровнях и направлениях организации.

[1] В дальнейшем — судовладелец.

2 КИБЕРУСТОЙЧИВОСТЬ СУДОВ

2.1 ЦЕЛИ И ОРГАНИЗАЦИЯ ТРЕБОВАНИЙ

2.1.1 Основная цель.

Основной целью настоящей части является обеспечение безопасного и защищенного судоходства, устойчивого к киберрискам.

Безопасное и защищенное судоходство может быть достигнуто благодаря эффективной системе управления киберрисками.

2.1.2 Промежуточные цели.

Для достижения основной цели, установлены следующие промежуточные цели управления киберрисками, которые должны выполняться одновременно и рассматриваться как части единой комплексной системы управления рисками:

.1 идентификация: сформировать полное представление о судовых КС для использования при управлении киберрисками судовых систем, людей, имущества, данных и функциональных возможностей;

.2 защита: разработать и внедрить надлежащие меры безопасности для защиты судна от киберинцидентов и обеспечения непрерывности судоходных операций;

.3 обнаружение: разработать и внедрить надлежащие меры обнаружения и определения возникновения киберинцидента на борту судна;

.4 реагирование: разработать и внедрить надлежащие меры и мероприятия, выполняемые при обнаружении киберинцидента на борту судна;

.5 восстановление: разработать и внедрить надлежащие меры и мероприятия по восстановлению любых функциональных возможностей и служб, необходимых для судоходных операций, которые были нарушены в результате киберинцидента.

2.1.3 Организация требований.

Требования организованы в соответствии с целевым подходом. Для достижения промежуточных целей в настоящем разделе указаны функциональные и технические требования. Эти требования предназначены для единообразного применения заинтересованными сторонами ко всем типам судов таким образом, чтобы обеспечивался допустимый уровень киберустойчивости.

Для каждого требования приводится обоснование.

Для каждого этапа жизненного цикла судна приводятся объем представляемой документации и краткое описание действий, которые должны быть выполнены соответствующими заинтересованными сторонами.

2.2 ТРЕБОВАНИЯ

Данная глава содержит требования в соответствии с пятью промежуточными целями, указанными в 2.1.2, которые должны быть выполнены для достижения основной цели, указанной в 2.1.1.

Требования выполняются заинтересованными сторонами, участвующими в проектировании, постройке и эксплуатации судна. Среди них можно выделить следующие заинтересованные стороны (см. определения в 1.2):

судовладелец;

системный интегратор;

поставщик.

Несмотря на то что требования могут выполняться этими заинтересованными сторонами, для целей настоящего раздела ответственность за их выполнение лежит на заинтересованной стороне, заключившей соответствующий договор с Регистром.

2.2.1 Идентификация.

Требования направлены на определение:

судовых КС, их взаимозависимостей и соответствующих информационных потоков;

ключевых ресурсов, задействованных в управлении, эксплуатации и администрировании КС, а также их ролей и обязанностей.

2.2.1.1 Ведомость судовых КС.

2.2.1.1.1 Требование.

Должна быть разработана и поддерживаться в актуальном состоянии в течение всего срока службы судна Ведомость с указанием аппаратного и программного обеспечения (включая приложения, операционные системы, если таковые имеются, микропрограммы и другие компоненты ПО) КС, входящих в область применения настоящей части, а также сетей, соединяющих такие системы друг с другом и с другими судовыми или береговыми КС.

2.2.1.1.2 Детализация требования.

Ведомость судовых КС должна включать, по крайней мере, КС, указанные в 1.1.3 — 1.1.6, если они имеются на борту.

Ведомость судовых КС должна актуализироваться в течение всего срока службы судна. В ней должны регистрироваться изменения аппаратного и программного обеспечения, которые могут привести к появлению новых уязвимостей или затрагивающие функциональные зависимости или связи между системами.

В случае внесения в Ведомость судовых КС конфиденциальной информации (например, IP-адресов, протоколов, номеров портов) должны приниматься специальные меры для ограничения несанкционированного доступа к такой информации.

2.2.1.1.2.1 Аппаратное обеспечение:

.1 в Ведомость судовых КС должно быть включено все аппаратное обеспечение, входящее в область применения настоящей части, при этом в Ведомости, по крайней мере, должна содержаться информация, указанная в 3.2.1.1;

.2 в Ведомости судовых КС должны быть указаны категории КС и зоны безопасности.

2.2.1.1.2.2 Программное обеспечение (ПО):

.1 в Ведомость судовых КС должно быть включено все ПО, входящее в область применения настоящей части (например, приложения, операционные системы, микропрограммы), при этом в Ведомости, по крайней мере, должна содержаться информация, указанная в 3.2.1.1;

.2 ПО КС, входящих в область применения настоящей части, должно обслуживаться и обновляться в соответствии с процессом по управлению обслуживанием ПО и политикой обновления, описанным судовладельцем в Программе кибербезопасности и киберустойчивости судна (см. 2.3.3.1).

Обоснование. Ведомость судовых КС и соответствующего ПО, используемого в ОТ-системах, имеет важное значение для эффективного управления киберустойчивостью судна, поскольку каждая КС потенциально содержит уязвимости. Для взлома систем злоумышленники могут использовать неучтенное и устаревшее оборудование и ПО. Кроме того, учет КС позволяет судовладельцу понять критичность каждой системы для обеспечения безопасности судна.

2.2.1.1.3 Подтверждение соответствия.

2.2.1.1.3.1 Этап проектирования:

.1 системный интегратор должен представить Регистру Ведомость судовых КС (см. также 2.3.1.3);

.2 Ведомость судовых КС должна включать в себя ведомости всех отдельных КС, входящих в область применения настоящей части, а также все иное оборудование, поставляемое системным интегратором.

2.2.1.1.3.2 Этап постройки:

.1 системный интегратор должен поддерживать актуальность Ведомости судовых КС.

2.2.1.1.3.3 Этап ввода в эксплуатацию:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать, что:

Ведомость судовых КС полностью актуализирована к моменту сдачи судна;

все КС, входящие в область применения настоящей части, корректно отражены в Ведомости судовых КС;

ПО КС, входящих в область применения настоящей части, регулярно обновляется.

2.2.1.1.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должен быть описан процесс управления изменениями для всех КС, входящих в область применения настоящей части, учитывающий как минимум следующие требования:

управление изменениями (см. 2.3.3);

изменения аппаратного и программного обеспечения (см. 2.2.1.1.2);

.2 в Программе кибербезопасности и киберустойчивости судна судовладельцем также должен быть описан процесс управления обновлениями ПО, учитывающий как минимум следующие требования:

уязвимости и киберриски (см. 2.2.1.1.2);

патчи безопасности (см. 2.2.2.6.2.2);

.3 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, а именно того, что:

соблюдается одобренный процесс управления изменениями;

известные уязвимости и функциональные зависимости учтены в ПО КС;

поддерживается актуальность Ведомости судовых КС;

.4 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.1.1.3.4.3;

.5 очередное освидетельствование.

Судовладелец должен продемонстрировать Регистру выполнение требований 2.2.1.1.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.2 Защита.

Требования направлены на разработку и внедрение надлежащих мер защиты, обеспечивающих снижение или сдерживание последствий потенциального инцидента.

2.2.2.1 Зоны безопасности и сегментация сети.

2.2.2.1.1 Требование:

.1 все КС, входящие в область применения настоящей части, должны быть сгруппированы по зонам безопасности с четко определенной политикой безопасности и функциональным возможностям обеспечения безопасности. Зоны безопасности должны быть либо изолированы (т.е. иметь физическое разделение), либо соединяться с другими зонами безопасности или сетями с помощью оборудования, обеспечивающего контроль данных, передаваемых между зонами (например, межсетевые экраны, симплексные последовательные линии, TCP/IP-диоды, сухие контакты и т.д.);

.2 границу зоны безопасности должен пересекать только разрешенный трафик.

2.2.2.1.2 Детализация требования:

.1 зона безопасности может содержать несколько КС и сетей, каждая из которых должна соответствовать требованиям безопасности, приведенным в настоящем разделе и в разд. 3;

.2 сеть(и) зоны безопасности должны быть логически и/или физически сегментированы от других зон или сетей;

.3 КС, обеспечивающие необходимую функциональную безопасность, должны быть сгруппированы в отдельные зоны безопасности и должны быть физически сегментированы от других зон безопасности;

.4 системы навигации и связи не должны находиться в той же зоне безопасности, что системы обслуживания механизмов и грузовые системы. Если системы навигации и радиосвязи одобрены в соответствии с иными эквивалентными стандартами (см. 1.1.5), то они должны находится в отдельной зоне безопасности;

.5 беспроводные устройства должны находиться в отдельных зонах безопасности с учетом требований 2.2.2.5;

.6 системы, сети и КС, не входящие в область применения настоящей части, считаются ненадежными сетями и должны быть физически сегментированы от зон безопасности, требуемых настоящим разделом. В качестве альтернативы допускается включение этих ОТ-систем в зону безопасности других КС, если они отвечают требованиям, установленными для этой зоны безопасности;

.7 должна обеспечиваться возможность изоляции зоны безопасности без ущерба для основной функциональности КС в этой зоне.

О б о с н о в а н и е . Нарушение периметра возможно, даже в случае защиты сети межсетевым экраном и наличием системы обнаружения вторжений (intrusion detection system (IDS)) или системы предотвращения вторжений (intrusion prevention system (IPS)) для контроля входящего трафика. Сегментация сети затрудняет злоумышленнику проведение атаки по всей сети.

Основные преимущества зон безопасности и сегментации сети заключаются в уменьшении поверхности атаки, предотвращении бокового перемещения злоумышленников через системы и повышении производительности сети. Концепция распределения КС по зонам безопасности позволяет группировать КС в соответствии с их параметрами риска.

2.2.2.1.3 Подтверждение соответствия.

2.2.2.1.3.1 Этап проектирования:

.1 системный интегратор должен представить Регистру Схему зон безопасности и каналов связи, а также Описание мер обеспечения кибербезопасности (см. 2.3.1.1 и 2.3.1.2);

.2 Схема зон безопасности и каналов связи должна отражать каким образом КС, входящие в область применения настоящей части, сгруппированы в зоны безопасности и включать в себя следующее:

четкое обозначение зон безопасности;

упрощенную схему КС, входящих в область применения настоящей части, с указанием зоны безопасности, к которой отнесена КС, и физического места расположения КС/оборудования;

ссылки на одобренные ревизии топологических схем КС, предоставленных поставщиками (см. 3.2.1.2);

отражение сетевых взаимодействий между системами в одной зоне безопасности;

отражение любых сетевых взаимодействий между системами в различных зонах безопасности (каналов связи);

отражение любых взаимодействий между системами в зоне безопасности и ненадежными сетями (каналов связи);

.3 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

краткое описание КС, входящих в зону безопасности. На Схеме зон безопасности и каналов связи должно быть возможно определить каждую КС;

сетевые взаимодействия между КС, входящих в одну и ту же зону безопасности. Описание мер обеспечения кибербезопасности должно включать в себя цель и параметры (протоколы и потоки данных) обмена данными;

сетевые взаимодействия между КС различных зон безопасности. Описание мер обеспечения кибербезопасности должно включать цель и параметры (протоколы и потоки данных) обмена данными. В описании мер обеспечения кибербезопасности должны быть указаны устройства, ограничивающие зоны безопасности, а также определен трафик, которому разрешено пересекать границу зоны (например, правила брандмауэра);

любые взаимодействия КС в зонах безопасности с ненадежными сетями. Описание должно включать в себя дискретные и последовательные интерфейсы, цели и параметры (протоколы и потоки данных) сетевого обмена данными на основе IP. В Описании мер обеспечения кибербезопасности должны быть указаны устройства ограничивающие зоны безопасности, а также определен трафик, которому разрешено пересекать границу зоны (например, правила брандмауэра).

2.2.2.1.3.2 Этап постройки:

.1 системный интегратор должен поддерживать актуальность Схемы зон безопасности и каналов связи.

2.2.2.1.3.3 Этап ввода в эксплуатацию:

.1 системный интегратор должен представить Программу испытаний киберустойчивости судна и продемонстрировать Регистру, что:

зоны безопасности соответствуют одобренной документации (Схеме зон безопасности и каналов связи, Описанию мер обеспечении кибербезопасности, Ведомости судовых КС и другой применимой документации, предоставленной поставщиком). Эта проверка может быть осуществлена внешним осмотром, сканированием сети или другими способами, подтверждающими, что установленное оборудование сгруппировано в зоны безопасности в соответствии с одобренной документацией;

границу зоны безопасности может пересекать только траффик, который задокументирован в одобренном Описании мер обеспечения кибербезопасности. Эта проверка может быть осуществлена оценкой правил межсетевого экрана или сканированием портов.

2.2.2.1.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должен быть описан процесс управления оборудованием, ограничивающим зоны безопасности (например, межсетевыми экранами), учитывающий как минимум следующие требования:

принцип наименьшей функциональности (см. 2.2.2.2.1.3);

разрешенный траффик (см. 2.2.2.1.1.2);

защита от событий типа «отказ обслуживания» (denial of service (DoS)) (см. 2.2.2.2.1.2);

проверка записей контроля безопасности (см. 2.2.3.1.2);

.2 первое ежегодное освидетельствование.

Судовладелец должен продемонстрировать Регистру, что Схема зон безопасности и каналов связи поддерживается в актуальном состоянии, а также представить записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, а именно того, что границы зон безопасности управляются в соответствии с вышеуказанными требованиями;

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.2.1.3.4.2;

.4 очередное освидетельствование.

Судовладелец должен продемонстрировать Регистру выполнение требований 2.2.2.1.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.2.2 Меры обеспечения безопасности сети.

2.2.2.2.1 Требование:

.1 зоны безопасности должны быть защищены межсетевыми экранами или эквивалентными средствами, как указано в 2.2.2.1.

.2 должна обеспечиваться защита сетей от возникновения чрезмерного потока данных и других факторов, способных оказать негативное влияние на работу сетевых ресурсов;

.3 КС, входящие в область применения настоящей части, должны строиться в соответствии с принципом наименьшей функциональности, т.е. быть сконфигурированными на предоставление только необходимых функциональных возможностей и на запрет или ограничение использования второстепенных функций. Функции, порты, протоколы и службы, не являющиеся необходимыми, должны быть отключены или запрещены иным образом.

2.2.2.2.2 Детализация требования.

При проектировании сети с целью минимизации риска событий типа «отказ в обслуживании» (DoS) и сетевого шторма/высокой скорости трафика, необходимо предусмотреть средства ограничения скорости потока данных до уровня, соответствующего предполагаемому потоку данных, проходящему через сеть. При оценке скорости потока данных необходимо учитывать, как минимум, пропускную способность сети, требования к скорости передачи данных для предполагаемого приложения и формата данных.

О б о с н о в а н и е . Защита сети охватывает множество технологий, правил и конфигураций, предназначенных для защиты целостности, конфиденциальности и доступности сетей. Постоянно меняются угрозы, злоумышленники постоянно пытаются найти и использовать уязвимости.

При решении проблемы защиты сети необходимо учитывать множество уровней. Атаки могут происходить на любом уровне сети, поэтому сетевое оборудование, ПО и политики должны учитывать все уровни.

Физические и технические средства контроля безопасности предназначены для предотвращения получения неавторизованными лицами физического доступа к компонентам сети и защиты данных, хранящихся или обрабатываемых сетью. Процедурные средства контроля безопасности состоят из политик безопасности и процессов, которые контролируют поведение пользователей.

2.2.2.2.3 Подтверждение соответствия.

2.2.2.2.3.1 Этап проектирования.

На этапе проектирования подтверждение соответствия не требуется.

2.2.2.2.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.2.2.3.3 Этап ввода в эксплуатацию:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и провести:

испытания атаками типа «отказ в обслуживании» (DoS), направленных на оборудование защиты границ зон безопасности, если применимо;

испытания типа «отказ в обслуживании» (DoS) для обеспечения защиты от чрезмерного потока данных, исходящего из каждого сегмента сети. Испытания на отказ обслуживания должны включать в себя испытания на «широковещательный шторм» (т.е. попытку использовать всю пропускную способность сегмента сети) и атаку прикладного уровня (т.е. попытку использовать всю вычислительную мощность выбранных узлов сети)[1];

проверку того, что неиспользуемые функции, порты, протоколы и службы КС удалены или запрещены в соответствии с рекомендациями поставщиков по усилению защиты (см. 3.4.7 и 3.5.3.4.7)[1].

2.2.2.2.3.4 Этап эксплуатации:

.1 очередное освидетельствование.

В случае внесения изменений в КС, судовладелец должен продемонстрировать Регистру выполнение требований 2.2.2.2.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.2.3 Антивирусные, антивредоносные, антиспам программы и другие средства защиты от вредоносного кода.

2.2.2.3.1 Требование.

КС, входящие в область применения настоящей части, должны быть защищены от вредоносного кода, такого как вирусы, «черви», «троянские кони», шпионские программы и т.д.

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

2.2.2.3.2 Детализация требования:

.1 в КС, входящих в область применения настоящей части, должна быть предусмотрена защита от вредоносного ПО. На КС, работающих под операционной системой, для которой доступно и поддерживается в актуальном состоянии стандартное антивирусное и антивредоносное ПО, такое ПО должно быть установлено, обслуживаться и регулярно обновляться, если только установка такого ПО не снижает способность КС выполнять необходимые функции и обеспечивать уровень обслуживания (например, для КС категорий II и III, выполняющих задачи в режиме реального времени);

.2 если на КС невозможно установить ПО для защиты от вредоносного ПО, такая защита должна быть реализована в виде эксплуатационных процедур, физических средств защиты или в соответствии с рекомендациями изготовителя.

О б о с н о в а н и е . Вирус или любая нежелательная программа, попавшая в систему без ведома пользователя, может самостоятельно копироваться и распространяться, выполнять нежелательные и вредоносные действия, которые, в конечном итоге, вредят производительности системы, данным/файлам пользователя, и/или обходят меры безопасности данных.

Антивирусное, антивредоносное, антиспам ПО будет действовать как барьер, не пропускающий вредоносное ПО. Оно обнаруживает потенциальный вирус и затем удаляет его, как правило, до того как вирус успеет нанести вред системе.

Распространенными способами проникновения вредоносного кода в КС являются электронная почта, вложения электронной почты, веб-сайты, съемные носители (например, устройства универсальной последовательной шины (universal serial bus (USB), дискеты или компакт-диски), документы в формате PDF, веб-сервисы, сетевые подключения и зараженные ноутбуки.

2.2.2.3.3 Подтверждение соответствия.

2.2.2.3.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

описание одобренных механизмов защиты от вредоносного кода и несанкционированного ПО, предоставленное для каждой КС соответствующими поставщиками;

инструкции по обновлению антивирусных баз КС, на которых установлено антивредоносное ПО;

любые эксплуатационные ограничения и физические средства защиты, которые судовладелец должен внедрить в систему управления киберрисками.

2.2.2.3.3.2 Этап постройки:

.1 системный интегратор должен обеспечить обновление установленного антивредоносного ПО.

2.2.2.3.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать эффективность одобренного антивредоносного ПО и/или компенсирующих мер (например, с помощью безопасного файла тестирования антивредоносного ПО).

2.2.2.3.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладелец должен описать процесс управления антивредоносной защитой, учитывающий как минимум следующие требования:

обслуживание/обновление (см. 2.2.2.3.2);

эксплуатационные процедуры, физические средства защиты (см. 2.2.2.3.2);

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

использование носимых, переносных, съемных носителей информации (см. 2.2.2.4.2.4 и 2.2.2.7.2);

управление доступом (см. 2.2.2.4);

.2 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, а именно то, что:

обслуживается и обновляется антивредоносное ПО;

соблюдаются инструкции по использованию носимых, переносных, съемных носителей информации;

соблюдается политика и процедуры по управлению доступом;

поддерживаются физические средства защиты;

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.2.3.3.4.2;

.4 очередное освидетельствование.

Судовладелец должен продемонстрировать Регистру выполнение требований 2.2.2.3.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.2.4 Контроль доступа.

2.2.2.4.1 Требование.

В КС и сетях, входящих в область применения настоящей части, должны быть обеспечены физические и/или логические средства для выборочного ограничения функциональности и средств для связи или иного взаимодействия с самой системой, использования системных ресурсов для обработки информации, получения сведений об информации, которую содержит система, или управления компонентами и функциями системы. Эти средства должны быть такими, чтобы не препятствовать доступу уполномоченного персонала к КС с их уровнем доступа в соответствии с принципом наименьших привилегий.

2.2.2.4.2 Детализация требования.

Доступ к КС и сетям, входящим в область применения настоящей части, а также ко всей информации, хранящейся в этих системах, должен быть разрешен только уполномоченному персоналу исходя из их производственной потребности доступа к информации в рамках своих обязанностей.

2.2.2.4.2.1 Контроль физического доступа.

КС категорий II и III с целью предотвращения несанкционированного доступа должны располагаться в запираемых помещениях или контролируемом пространстве, или устанавливаться в запираемых шкафах или консолях. Эти места или запираемые шкафы/консоли должны быть легкодоступными для экипажа и различных заинтересованных сторон, которым необходим доступ к КС для установки, интеграции, работы, технического обслуживания, ремонта, замены, утилизации и т.д., чтобы не препятствовать эффективной и действенной эксплуатации судна.

2.2.2.4.2.2 Контроль физического доступа для посетителей.

Доступ к судовым КС посетителей, таких как представители власти, технические специалисты, агенты, должностные лица порта, а также представители судовладельца должен быть ограничен, например, посредством разрешения доступа только под наблюдением.

2.2.2.4.2.3 Контроль физического доступа к точкам подключения к сети:

.1 точки подключения к судовым сетям, соединяющим КС категории II и/или III, должны быть физически и/или логически заблокированы, за исключением случаев, когда подключение происходит под наблюдением или в соответствии с задокументированными процедурами, например, с целью технического обслуживания;

.2 в случае эпизодического подключения посетителя (например, для распечатки документов) должны использоваться независимые компьютеры, изолированные от всех судовых сетей, или другие сети, такие как выделенные гостевые сети или сети, предназначенные для досуга пассажиров.

2.2.2.4.2.4 Управление съемными носителями.

Должна быть внедрена политика использования съемных носителей, а также процедуры проверки съемных носителей на наличие вредоносного ПО и/или подтверждения подлинности ПО цифровыми подписями и водяными знаками, а также сканирования перед разрешением загрузки файлов в судовую систему или скачивания данных из судовой системы. с учетом требований 2.2.2.7.

2.2.2.4.2.5 Управление учетными данными:

.1 КС и соответствующая информация должны быть защищены при помощи списков контроля доступа (Access Control Lists (ACL)) для файловой системы, сети, приложения или базы данных. Учетные записи для экипажа и берегового персонала должны быть активными только в течение ограниченного периода времени в соответствии с ролью и обязанностями владельца учетной записи. Учетные записи должны удаляться, как только в них нет больше необходимости.

Примечание. В соответствии с п. 1 табл. 3.3.1 КС должны идентифицировать и аутентифицировать пользователей – физических лиц. Нет необходимости уникальным образом идентифицировать и аутентифицировать всех пользователей – физических лиц;

.2 контроль доступа к судовым КС должен обеспечиваться в соответствии с политикой зоны безопасности, при этом не должно оказываться негативного влияния на работу по назначению КС. КС, требующие строгого контроля доступа, могут быть защищены с помощью надежного ключа шифрования или многофакторной аутентификации;

.3 управление привилегиями администратора должно осуществляться в соответствии с политикой контроля доступа. Полный доступ к КС должен предоставляться только уполномоченным и соответствующим образом обученным лицам, которые в рамках своих должностных обязанностей в береговых подразделениях судовладельца или на борту судна должны входить в системы с использованием этих привилегий.

2.2.2.4.2.6 Политика наименьших привилегий:

.1 любому пользователю – физическому лицу, допущенному к КС и сетям, входящим в область применения настоящей части, должны предоставляться только минимальные привилегии, достаточные для выполнения его функций;

.2 по умолчанию должен быть установлен минимальный уровень привилегий для всех новых учетных записей. По возможности, повышенные привилегии должны быть ограничены только теми моментами, когда они необходимы, например, с использованием только временных привилегий и учетных записей однократного использования. Должно обеспечиваться предотвращение накопления привилегий с течением времени, например, путем регулярного аудита учетных записей пользователей.

О б о с н о в а н и е . Злоумышленники могут попытаться получить доступ к системам и данным судна как с борта судна, так и внутри инфраструктуры судовладельца, либо удаленно посредством подключения к интернету. В целях обеспечения безопасности судна и его груза должны быть предусмотрены средства контроля физического и логического доступа к КС, сетям и т.д.

Физические угрозы и соответствующие меры также рассматриваются в Международном кодексе по охране судов и портовых средств, принятом резолюцией 2 конференции ИМО 2002 года, с поправками[1]. Аналогичным образом Международный кодекс по управлению безопасностью, принятый резолюцией ИМО А.741(18), с поправками[2], содержит указания для обеспечения безопасной эксплуатации судна и защиты окружающей среды. Реализация Кодекса ОСПС и МКУБ может предполагать включение в План охраны судна (ПОС) и Систему управления безопасностью (СУБ) инструкций и процедур по контролю доступа к важным с точки зрения безопасности судовым КС.

2.2.2.4.3 Подтверждение соответствия.

2.2.2.4.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

расположение каждой КС и меры контроля доступа. Если оборудование, предоставляющее человеко-машинный интерфейс (HMI) для операторов, которым необходим немедленный доступ, установлено в помещении с контролируемым доступом, то оно может не обеспечивать идентификацию и аутентификацию пользователя. Такое оборудование должно быть перечислено отдельно.

2.2.2.4.3.2 Этап постройки.

На этапе постройки судна системный интегратор должен обеспечить предотвращение несанкционированного доступа к КС.

2.2.2.4.3.3 Этап ввода в эксплуатацию:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна и продемонстрировать, что:

блоки КС расположены в помещениях или местах, в которых физический доступ может контролироваться уполномоченным экипажем;

учетные записи пользователей настроены в соответствии с принципами разделения обязанностей и наименьших привилегий, временные учетные записи удалены[3].

2.2.2.4.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должен быть описан процесс управления логическим и физическим доступом, учитывающий, как минимум, следующие требования:

контроль физического доступа (см. 2.2.2.4.2.1);

контроль физического доступа посетителей (см. 2.2.2.4.2.2);

контроль физического доступа к точкам подключения к сети (см. 2.2.2.4.2.3);

управление учетными данными (см. 2.2.2.4.2.5);

политика наименьших привилегий (см. 2.2.2.4.2.6);

.2 в Программе кибербезопасности и киберустойчивости судна судовладельцем должен быть описан процесс управления конфиденциальной информацией, учитывающий как минимум следующие требования:

конфиденциальная информация (см. 2.2.1.1.2);

информация доступная уполномоченному персоналу (см. 2.2.2.4.2);

информация, передаваемая по беспроводной сети (см. 2.2.2.5.2);

---

[1] В дальнейшем — Кодекс ОСПС.

[2] В дальнейшем — МКУБ.

[3] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

.3 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, т.е. того, что:

персонал имеет доступ к КС в соответствии со своими обязанностями;

только разрешенные устройства подключаются к КС;

посетителям предоставляется доступ к КС согласно соответствующим политикам и процедурам;

поддерживается и применяется контроль физического доступа;

учетные данные, ключи, секретная информация, сертификаты, соответствующая документация КС и иная закрытая информация содержатся конфиденциально согласно соответствующим политикам и процедурам;

.4 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.2.4.3.4.3.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.2.5 Беспроводная связь.

2.2.2.5.1 Требование.

Беспроводные сети, входящие в область применения настоящей части, должны быть спроектированы, построены и обслуживаться таким образом, чтобы:

.1 киберинциденты не распространялись на другие КС;

.2 доступ к беспроводной сети предоставлялся только уполномоченным пользователям;

.3 связь предоставлялась только разрешенным процессам и устройствам;

.4 обеспечивалась невозможность подделки или раскрытия информации, передаваемой по беспроводной сети.

2.2.2.5.2 Детализация требования:

.1 для обеспечения целостности и конфиденциальности информации, передаваемой по беспроводной сети, должны применяться механизмы криптографии, такие как алгоритмы шифрования и длины ключей в соответствии с отраслевыми стандартами и передовой практикой;

.2 устройства в беспроводной сети должны обмениваться данными только в беспроводной сети (т.е. они не должны иметь двойного соединения);

.3 беспроводные сети должны быть спроектированы как отдельные сегменты в соответствии с 2.2.2.1 и защищены в соответствии с 2.2.2.2;

.4 беспроводные точки доступа и другие устройства в сети должны быть установлены и настроены таким образом, чтобы можно было контролировать доступ к сети;

.5 сетевые устройства или системы, использующие беспроводное соединение, должны обеспечивать возможность идентификации и аутентификации всех пользователей (людей, программных процессов или устройств), участвующих в этом соединении.

О б о с н о в а н и е . Беспроводные сети создают дополнительные киберриски по сравнению с проводными сетями. Главным образом это связано с меньшей физической защитой устройств и использованием радиосвязи.

Из-за недостаточного контроля физического доступа неуполномоченные лица могут получить доступ к физическим устройствам, что, в свою очередь, может привести к обходу ограничений логического доступа или подключению к сети неразрешенных устройств.

Передача сигнала по радиоканалу создает риски глушения и подслушивания, что, в свою очередь, может привести к таким атакам, как «Piggybacking» (использование беспроводного соединения для несанкционированного доступа) и «злой двойник» (подмена оригинальной точки доступа двойником, к которому подключается пользователь, предоставляя злоумышленнику возможность доступа к конфиденциальной информации).

2.2.2.5.3 Подтверждение соответствия.

2.2.2.5.3.1 Этап проектирования.

В Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

описание беспроводных сетей, входящих в область применения настоящей части. Описание должно включать оборудование, ограничивающее зону безопасности, и разрешенный трафик (например, правила межсетевого экрана).

2.2.2.5.3.2 Этап постройки.

На этапе постройки судна системный интегратор должен обеспечить предотвращение несанкционированного доступа к беспроводным сетям.

2.2.2.5.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать, что:

только разрешенные устройства могут получить доступ к беспроводной сети;

используется безопасный протокол беспроводной связи, указанный в одобренной документации соответствующего поставщика (например, при помощи анализатора сетевых протоколов).

2.2.2.5.3.4 Этап эксплуатации:

.1 очередное освидетельствование.

В случае изменений беспроводных сетей, входящих в область применения настоящей части, судовладелец должен продемонстрировать Регистру выполнение требований 2.2.2.5.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.2.6 Управление удаленным доступом и связь с ненадежными сетями.

2.2.2.6.1 Требование.

КС, входящие в область применения настоящей части, должны быть защищены от несанкционированного доступа и других киберугроз, исходящих из ненадежных сетей.

2.2.2.6.2 Детализация требования:

для управления удаленным доступом к судовым IT- и OT-системам на борту судна должно находиться руководство пользователя, в котором четко определены роли, разрешения и функции;

ни один IP-адрес КС, входящей в область применения настоящей части, не должен быть доступен из ненадежных сетей;

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

при связи с ненадежными сетями или через них должно применяться защищенное соединение (например, туннели) с аутентификацией конечных точек, защитой целостности, аутентификацией и шифрованием на сетевом или транспортном уровне. Должна обеспечиваться конфиденциальность информации, на которую распространяется разрешение на чтение.

2.2.2.6.2.1 Проектирование.

КС, входящие в область применения данного раздела, должны:

обеспечивать возможность прерывания соединения с конечной точки на борту судна. Любой удаленный доступ должен предоставляться только после прямого подтверждения ответственным лицом на борту судна;

обеспечивать управление прерываниями удаленных сеансов, чтобы не ставить под угрозу безопасность ОТ-систем или целостность и доступность данных, используемых ОТ-системами;

обеспечивать регистрацию всех событий удаленного доступа и их хранение в течение периода времени, достаточного для автономного просмотра удаленных соединений, например, после обнаружения киберинцидента.

2.2.2.6.2.2 Дополнительные требования к удаленному обслуживанию.

Если удаленный доступ используется для обслуживания, то в дополнение к требованиям 2.2.2.6.2.1 должны быть выполнены следующие требования:

.1 должна представляться документация, описывающая как происходят соединение и интеграция с береговым участком;

.2 перед установкой патчи безопасности и обновления должны тестироваться и оцениваться, чтобы убедиться в их эффективности и отсутствии недопустимых побочных эффектов или появления киберсобытий. Перед проведением удаленного обновления должен быть получен соответствующий отчет от поставщика ПО;

.3 поставщики должны уведомлять судовладельца об обновлениях и предоставлять к ним доступ (см. 3.4.2, 3.4.3, 3.4.4);

.4 при проведении удаленного технического обслуживания уполномоченный персонал на борту судна в любое время должен иметь возможность прервать сеанс, отменить работу и вернуться к предыдущей безопасной конфигурации КС и затрагиваемых систем;

.5 любой доступ к КС пользователей из ненадежных сетей должен предоставляться с использованием многофакторной аутентификации;

.6 после настраиваемого количества неудачных попыток получения удаленного доступа следующая попытка должна блокироваться на заранее определенный период времени;

.7 если по какой-либо причине при удаленном обслуживании происходит прерывание соединения, доступ к системе должен быть прекращен функцией автоматического выхода из системы.

О б о с н о в а н и е . Судовые КС все больше используют подключение к интернету для выполнения широкого спектра разрешенных функций. Использование цифровых систем для мониторинга и управления судовыми КС делает их уязвимыми для киберинцидентов. Злоумышленники могут попытаться получить доступ к судовым КС через соединение с интернетом и внести изменения, влияющие на работу КС, или даже получить полный контроль над КС, или попытаться выгрузить информацию из судовой КС. Кроме того, поскольку использование устаревших IT- и ОТ-систем, которые больше не поддерживаются и/или работают под управлением устаревших операционных систем, в значительной степени влияет на киберустойчивость, особое внимание должно быть уделено установке на борту соответствующего оборудования и ПО, способствующего поддержанию достаточного уровня киберустойчивости, при осуществлении удаленного доступа к этим системам, также учитывая, что не все киберинциденты являются результатом преднамеренной атаки.

2.2.2.6.3 Подтверждение соответствия.

2.2.2.6.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

перечень КС, входящих в область применения настоящей части, которые взаимодействуют через границу зоны безопасности с ненадежными сетями, в том числе для предоставления удаленного доступа;

описание соответствия требованиям 2.2.2.6.2 каждой КС, для которой эти требования применимы.

2.2.2.6.3.2 Этап постройки.

Системным интегратором должно быть обеспечено, что любые взаимодействия с ненадежными сетями имеют временный характер и используются в соответствии с требованиями 2.2.2.6.

2.2.2.6.3.3 Этап ввода в эксплуатацию:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать, что:

связи с ненадежными сетями защищены в соответствии с 3.3.2, и что не могут быть согласованы менее защищенные версии протоколов связи (например, при помощи анализатора сетевых протоколов);

для удаленного доступа необходима многофакторная аутентификация удаленного пользователя;

установлено ограничение количества неудачных попыток входа в систему, и перед установлением сеанса связи удаленному пользователю предоставляется соответствующее уведомление;

удаленное соединение осуществляется только после прямого подтверждения ответственным лицом на борту судна;

сеанс удаленного доступа может быть прерван вручную с борта судна и в случае бездействия сеанс будет автоматически завершен;

сеансы удаленного доступа регистрируются (п. 13 табл. 3.3.1);

поставщиками предоставлены соответствующие инструкции и процедуры (см. 3.2.1.3).

2.2.2.6.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должен быть описан процесс управления удаленным доступом и взаимодействия с ненадежными сетями, учитывающий как минимум следующие требования:

руководство пользователя (см. 2.2.2.6.2);

роли и разрешения (см. 2.2.2.6.2);

патчи и обновления (см. 2.2.2.6.2.2);

подтверждение перед удаленным обновлением ПО (см. 2.2.2.6.2.2);

прерывание, отмена и возврат (см. 2.2.2.6.2.2);

.2 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, т.е. того, что:

сессии удаленного доступа регистрируются и проводятся согласно соответствующим политикам и руководству пользователя, обеспечивается регистрация или запись сессий удаленного доступа;

установка патчей безопасности и других обновлений проводится в соответствии с процедурами управления изменениями и при поддержке поставщика;

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.2.6.3.4.2;

.4 очередное освидетельствование.

Судовладелец должен продемонстрировать Регистру выполнение требований 2.2.2.6.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.2.7 Использование носимых и переносных устройств.

2.2.2.7.1 Требование.

Использование носимых и переносных устройств в КС, входящих в область применения настоящей части, должно ограничиваться только необходимыми действиями и контролироваться в соответствии с п. 10 табл. 3.3.1. Порты ввода/вывода КС, не удовлетворяющих полностью вышеуказанным требованиям, должны быть физически заблокированы.

2.2.2.7.2 Детализация требования:

.1 носимые и переносные устройства должны использоваться только уполномоченным персоналом. Допускается подключение к КС только разрешенных устройств. Использование таких устройств должно происходить в четком соответствии с политикой судовладельца по использованию носимых и переносных устройств.

Обоснование. КС могут быть повреждены вследствие заражения вредоносным ПО через мобильное или портативное устройство. В связи с этим должно быть уделено внимание подключению носимых и переносных устройств. В дополнение к этому, носимое оборудование, которое необходимо использовать для эксплуатации и технического обслуживания судна, должно находиться под контролем судовладельца.

2.2.2.7.3 Подтверждение соответствия.

2.2.2.7.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

определение всех КС, входящих в область применения настоящей части, но не отвечающих требованиям п. 10 табл. 3.3.1, т.е. тех КС, для которых необходима физическая блокировка портов.

2.2.2.7.3.2 Этап постройки.

.1 системный интегратор должен убедиться, что использование физических портов ввода/вывода КС контролируется в соответствии с п. 10 табл. 3.3.1 и что при подключении таких устройств к КС соблюдаются процедуры по предотвращению от попадания вредоносного ПО в КС.

2.2.2.7.3.3 Этап ввода в эксплуатацию:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна и продемонстрировать, что контроль за использованием носимых и переносных устройств реализован правильно, включая демонстрацию следующих мер (если применимо):

использование носимых и переносных устройств разрешено только уполномоченному персоналу;

порты ввода/вывода могут использоваться только определенными типами устройств;

невозможна передача файлов в систему с носимых и переносных устройств;

невозможен автоматический запуск файлов с носимых и переносных устройств (запрещен автозапуск);

сетевой доступ разрешен только определенным MAC или IP адресам;

неиспользуемые порты ввода/вывода отключены и/или физически заблокированы.

2.2.2.7.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должен быть описан процесс управления носимыми и переносными устройствами, учитывающий, как минимум, следующие требования:

внедрение политики и процедур (см. 2.2.2.4.2.4);

физическая блокировка портов ввода/вывода (см. 2.2.2.7.1);

использование только уполномоченным персоналом (см. 2.2.2.7.3.3);

подключение только разрешенных устройств (см. 2.2.2.7.3.3);

учет рисков внедрения вредоносного ПО (см. 2.2.2.7.3.3);

.2 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, т.е. того, что:

использование носимых, переносных устройств или съемных носителей разрешено только уполномоченному персоналу и проводится согласно соответствующим политикам и процедурам;

к КС подключаются только разрешенные устройства;

применяются устройства ограничения доступа в соответствии с одобренной документацией проекта судна;

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.2.7.3.4.2;

.4 очередное освидетельствование.

Судовладелец должен продемонстрировать Регистру выполнение требований 2.2.2.7.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.3 Обнаружение.

Требования направлены на разработку и внедрение надлежащих мер, обеспечивающих способность выявлять и распознавать аномальную активность в судовых КС и сетях, а также идентифицировать киберинциденты.

2.2.3.1 Мониторинг работы сети.

2.2.3.1.1 Требование.

Сети, входящие в область применения настоящей части, должны постоянно контролироваться, и в случае возникновения неисправностей или снижения/ухудшения пропускной способности должны срабатывать сигналы тревоги.

2.2.3.1.2 Детализация требования:

.1 средства мониторинга сетей, входящих в область применения настоящей части, должны обеспечивать:

мониторинг и защиту от чрезмерного трафика;

мониторинг сетевых соединений;

мониторинг и регистрацию действий по управлению устройством;

защиту от подключения неразрешенных устройств;

срабатывание сигнала тревоги при превышении значения порога использования полосы пропускания, установленного поставщиком (см. 7.9.8.2.1.5 части XV «Автоматизация»);

.2 при соблюдении нижеследующих условий допускается использование системы обнаружения вторжений (IDS):

использование системы обнаружения вторжений (IDS) должно быть одобрено поставщиком соответствующей КС;

система обнаружения вторжений (IDS) должна быть пассивной и не активировать функции защиты, которые могут повлиять на работу КС;

соответствующий персонал должен быть обучен и иметь квалификацию для использования системы обнаружения вторжений (IDS).

О б о с н о в а н и е . Кибератаки становятся все более изощренными, и атаки, направленные на уязвимые места, которые были неизвестны на момент постройки судна, могут привести к инцидентам, при которых судно окажется плохо подготовленным к угрозе. Для раннего реагирования на атаки, направленные на эти типы неизвестных уязвимостей, необходима технология, способная обнаруживать нестандартные события. Система мониторинга, способная обнаруживать аномалии в сетях и проводить анализ после инцидента, обеспечивает возможность надлежащего реагирования и дальнейшего восстановления после киберсобытия.

2.2.3.1.3 Подтверждение соответствия.

2.2.3.1.3.1 Этап проектирования.

На этапе проектирования подтверждение соответствия не требуется.

2.2.3.1.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.3.1.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен включить проверку средств мониторинга и защиты сети в Программу испытаний киберустойчивости судна, а также продемонстрировать Регистру, что:

при отключении сетевого соединения происходит срабатывание сигнала тревоги и регистрация события;

при обнаружении аномально высокого сетевого трафика происходит срабатывание сигнала тревоги и регистрация события. Это испытание может проводиться совместно с испытанием, указанным в 2.2.4.4.3.3;

КС будет безопасно реагировать на сценарии сетевого шторма, включая как одноадресную, так и многоадресную передачу (см. также 2.2.2.2.3.3);

ведется журнал аудита (регистрация событий безопасности);

система обнаружения вторжений (IDS) пассивная и не активирует защитные функции, которые могут повлиять на работу КС по прямому назначению (если используется система обнаружения вторжений (IDS)).

.2 любая система обнаружения вторжений (IDS) в КС, входящих в область применения настоящей части, подлежит техническому наблюдению Регистра. Соответствующая документация должна быть представлена на одобрение Регистру с последующим освидетельствованием на борту судна.

2.2.3.1.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должны быть описаны мероприятия по определению аномалий в КС и сетях, учитывающие как минимум следующие требования:

выявление и распознавание аномальной активности (см. 2.2.3);

проверка записей контроля безопасности (см. 2.2.3.1.2);

инструкции или процедуры по обнаружению инцидента (см. 2.2.4.1.1);

.2 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, т.е. того, что:

КС регулярно проверяются на наличие аномалий при помощи просмотра журнала аудита и расследования причин сигналов тревоги КС;

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать Регистру выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.3.1.3.4.2;

.4 очередное освидетельствование.

В случае внесения изменений в КС, судовладелец должен продемонстрировать Регистру выполнение требований 2.2.3.1.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.3.2 Функции проверки и диагностики КС и сетей.

2.2.3.2.1 Требование.

КС и сети, входящие в область применения настоящей части, должны обеспечивать контроль работоспособности и исправности функций безопасности, требуемых настоящим разделом. Функции диагностики должны обеспечивать пользователю достаточную информацию о состоянии и целостности КС, а также средства поддержания собственной работоспособности для обеспечения безопасной эксплуатации судна.

2.2.3.2.2 Детализация требования:

.1 должны быть обеспечены функции диагностики КС и сетей, способные проверить работоспособность всех требуемых функций безопасности на этапах проведения испытаний и эксплуатации судна.

О б о с н о в а н и е . Для обеспечения управления киберустойчивостью в течение всего срока службы судна важную роль играет возможность проверки работы функций безопасности. Диагностические инструменты могут включать в себя автоматические или ручные средства, такие как средства самодиагностики каждого устройства, или инструменты для мониторинга сети (например, ping, traceroute, ipconfig, netstat, nslookup, Wireshark, nmap и т.д.).

Однако следует отметить, что выполнение диагностических функций может иногда влиять на эксплуатационные характеристики КС.

2.2.3.2.3 Подтверждение соответствия.

2.2.3.2.3.1 Этап проектирования.

На этапе проектирования подтверждение соответствия не требуется.

2.2.3.2.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.3.2.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать в работе методики проверки функций безопасности, предоставленные поставщиками.

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

2.2.3.2.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должны быть описаны мероприятия по проверке правильности работы функций безопасности КС и сетей, учитывающие, как минимум, следующие требования:

тестирование и техническое обслуживание (см. 2.2.3.2.2);

периодическое обслуживание (см. 2.3.3.3);

.2 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, т.е. того, что:

функции безопасности КС периодически тестируются или проверяются;

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.3.2.3.4.2.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.4 Реагирование.

Требования направлены на разработку и внедрение надлежащих мер, обеспечивающих способность минимизировать воздействие киберинцидентов, ограничивая распространение возможного повреждения судовых КС и сетей.

2.2.4.1 План действий в случае киберинцидента.

2.2.4.1.1 Требование.

Судовладельцем должен быть разработан план действий в случае киберинцидента, охватывающий соответствующие нештатные ситуации и определяющий порядок реагирования на киберинциденты. В Плане действий в случае киберинцидента должен быть задокументирован заранее определенный набор инструкций или процедур по обнаружению, реагированию и ограничению последствий инцидентов, направленных против КС, входящих в область применения данного раздела.

2.2.4.1.2 Детализация требования:

.1 для разработки Плана действий в случае киберинцидента, различные заинтересованные стороны, участвующие в этапах проектирования и постройки судна, должны предоставить судовладельцу необходимую информацию. Во время первого ежегодного освидетельствования План действий в случае киберинцидента должен быть на борту судна. План действий в случае киберинцидента должен постоянно поддерживаться в актуальном состоянии (например, после технического обслуживания) в течение всего срока эксплуатации судна;

.2 в Плане действий в случае киберинцидента должны быть описаны процедуры уведомления соответствующих должностных лиц о произошедших киберинцидентах, с сообщением принятых мер по реагированию на киберинцидент и ограничению распространения киберинцидента на другие сегменты сети;

.3 План действий в случае киберинцидента должен содержать, как минимум, следующую информацию:

точки отключения для изолирования скомпрометированных систем;

описание аварийных сигналов и индикаторов, сигнализирующих об обнаружении активных киберсобытий и/или аномалий, вызванных киберсобытиями;

описание ожидаемых последствий киберинцидентов;

варианты реагирования. При этом приоритет должен отдаваться вариантам реагирования, не предполагающим ни отключение, ни передачу под независимое или местное управление (при наличии);

информацию о способах независимого и местного управления для работы независимо от системы, вышедшей из строя в результате киберинцидента;

.4 План действий в случае киберинцидента должен храниться в твердой копии и быть доступным в случае полной потери электронных устройств.

О б о с н о в а н и е . План действий в случае киберинцидента — это инструмент, призванный помочь ответственным лицам противодействовать киберинцидентам. Для того, чтобы План действий в случае киберинцидента был эффективен, он должен быть простым и тщательно проработанным. При разработке Плана действий в случае киберинцидента важно понимать значимость любого киберинцидента и соответствующим образом расставлять приоритеты вариантов реагирования.

В Плане действий в случае киберинцидента должны быть также указаны средства для поддержания максимально возможной функциональности и уровня обслуживания для безопасной эксплуатации судна, например, переход на резервное оборудование. В случае возникновения киберинцидента, назначенное(ые) лицо(а) судовладельца/компании (см. разд. 4 МКУБ) должно(ны) находиться на связи с судном.

2.2.4.1.3 Подтверждение соответствия.

2.2.4.1.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

ссылки на информацию, представленную поставщиками (см. 3.2.1.8, которая может быть использована судовладельцем при разработке плана действий в случае инцидента.

2.2.4.1.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.4.1.3.3 Этап ввода в эксплуатацию.

На этапе ввода в эксплуатацию подтверждение соответствия не требуется.

2.2.4.1.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должен быть описан План действий в случае киберинцидента, учитывающий, как минимум, следующие требования:

описание того, кто, когда и каким образом должен реагировать на киберинциденты в соответствии с требованиями 2.2.4.1;

инструкции по местному/ручному управлению в соответствии с требованиями 2.2.4.2;

инструкции по изолированию зон безопасности в соответствии с требованиями 2.2.4.3;

описание ожидаемого поведения КС в случае киберинцидента в соответствии с требованиями 2.2.4.4;

.2 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, т.е. того, что:

ответственные члены экипажа судна имеют доступ к Плану действий в случае киберинцидента;

ответственные члены экипажа судна имеют доступ к инструкциям по местному/ручному управлению в соответствии с требованиями;

ответственные члены экипажа судна имеют доступ к инструкциям по отключению/изоляции зон безопасности;

реагирование на произошедшие киберинциденты происходило в соответствии с планом действий в случае киберинцидента;

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.4.1.3.4.2.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.4.2 Местное, независимое и/или ручное управление.

2.2.4.2.1 Требование.

Любая КС, необходимая для местного управления, требуемого 2.3.4 части XV «Автоматизация», должна быть независимой от основной системы управления. Это также относится к человеко-машинному интерфейсу (HMI), необходимому для работы местного управления.

2.2.4.2.2 Детализация требования:

.1 КС для местного управления и контроля должны быть автономными и работать по прямому назначению независимо от связей с другими КС;

.2 если связь с системой дистанционного управления или другими КС осуществляется по сетям, должны быть реализованы меры по сегментации и защите, описанные в 2.2.2.1 и 2.2.2.2. Это означает, что система местного управления и контроля должна рассматриваться как отдельная зона безопасности;

.3 несмотря на вышесказанное, в каждом конкретном случае могут учитываться различные особенности построения КС;

.4 КС для местного управления и контроля должны также соответствовать другим требованиям настоящей части.

О б о с н о в а н и е . Независимое местное управление механизмами и оборудованием, необходимое для поддержания безопасной эксплуатации, является важным элементом для судов с экипажем. Целью этого требования является обеспечение возможности экипажа осуществлять управление вручную в непосредственной близости от механизмов при отказе дистанционного управления в результате отказа или киберинцидента.

2.2.4.2.3 Подтверждение соответствия.

2.2.4.2.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

описание каким образом местное управление, указанное в 2.3.4 части XV «Автоматизация», защищено от киберинцидентов в любых подключенных системах автоматического или дистанционного управления.

2.2.4.2.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.4.2.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать, что обязательное местное управление, входящее в область применения настоящей части и необходимое для безопасной эксплуатации судна, может работать независимо от любых систем дистанционного или автоматического управления.

2.2.4.2.3.4 Этап эксплуатации:

.1 очередное освидетельствование.

В случае внесения изменений в КС, судовладелец должен продемонстрировать Регистру выполнение требований 2.2.4.2.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

2.2.4.3 Изоляция сети.

2.2.4.3.1 Требование.

Должна быть обеспечена возможность прерывания сетевого соединения с зоной безопасности.

2.2.4.3.2 Детализация требования:

.1 если План действий в случае киберинцидента предписывает выполнить изоляцию сети, должна обеспечиваться возможность изоляции зон безопасности по соответствующей процедуре, например, с помощью физического переключателя «ВКЛ/ВЫКЛ» на сетевом устройстве, отсоединением кабеля от маршрутизатора/брандмауэра или других аналогичных действий. Должны быть доступны инструкции и четкая маркировка на оборудовании, позволяющая экипажу эффективно изолировать сеть;

.2 необходимо определить зависимости отдельных систем от данных, которые могут повлиять на функциональность и штатную работу, включая безопасность, с четким указанием, где необходимо предусмотреть меры резервирования данных или функциональных входов, в случае изоляции сегмента сети во время непредвиденной ситуации.

О б о с н о в а н и е . План действий в случае киберинцидента должен включать в себя меры по противодействию дальнейшему распространению киберинцидента и его последствий. В качестве таких мер может выступать изолирование сегментов сети и систем управления, выполняющих ключевые функции.

2.2.4.3.3 Подтверждение соответствия.

2.2.4.3.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

инструкция по изоляции каждой зоны безопасности от других зон и сетей. Описание последствий изоляции, иллюстрирующее, что КС, расположенные в изолированной зоне безопасности, не зависят от данных, передаваемых IP-сетями из других зон и сетей.

2.2.4.3.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.4.3.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна и продемонстрировать путем отключения всех сетей, пересекающих границу зоны безопасности, что КС, входящие в область применения настоящей части, сохраняют достаточную функциональность без сетевых подключений с другими зонами безопасности и сетями.

2.2.4.3.3.4 Этап эксплуатации:

.1 очередное освидетельствование.

В случае внесения изменений в КС судовладелец должен продемонстрировать выполнение требований 2.2.4.3.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

2.2.4.4 Возврат к состоянию минимального риска.

2.2.4.4.1 Требование.

В случае киберинцидента, затрагивающего способность КС или сети, входящих в область применения настоящей части, выполнять требуемые функции по назначению, система или сеть должна обеспечивать возможность перехода в состояние минимального риска, т.е. привести себя в стабильное, безопасное состояние.

2.2.4.4.2 Детализация требования:

.1 при обнаружении киберинцидента, затрагивающего КС или сеть и ставящего под угрозу способность системы выполнять требуемые функции по назначению, система незамедлительно должна быть переведена в приемлемое безопасное состояние. Действия по возврату в безопасное состояние могут включать:

полную остановку системы;

отсоединение системы;

передачу управления другой системе или экипажу;

иные компенсирующие действия;

.2 возврат к состоянию минимального риска должен происходить в течение времени, достаточного для поддержания судна в безопасном состоянии;

.3 способность системы возвращаться в состояние минимального риска должна быть учтена на этапе проектирования поставщиком и системным интегратором.

О б о с н о в а н и е . Способность КС и интегрированных систем возвращаться к одному или нескольким состояниям минимального риска в случае непредвиденных или неконтролируемых отказов или событий является мерой безопасности, направленной на поддержание системы в постоянном, известном и безопасном состоянии.

Возврат к состоянию минимального риска обычно означает способность системы прервать текущую операцию и подать соответствующий сигнал экипажу. Состояние минимального риска может различаться в зависимости от условий окружающей среды, фазы рейса судна (например, выход из порта/прибытие в порт или же переход в открытое море) и произошедших событий.

2.2.4.4.3 Подтверждение соответствия.

2.2.4.4.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

описание безопасного состояния функций управления КС, входящих в область применения настоящей части.

2.2.4.4.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.4.4.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна и продемонстрировать, что КС, входящие в область применения настоящей части, безопасным образом реагируют на киберинциденты (см. 2.2.4.4.3.1), например, поддерживая внешние подключения к службам ответственного назначения и предоставляя оператору функции управления и мониторинга альтернативными средствами. Испытания, как минимум, должны включать в себя DoS атаки и могут быть совмещены с испытаниями 2.2.3.1.3.3.

2.2.4.4.3.4 Этап эксплуатации.

.1 очередное освидетельствование.

В случае внесения изменений в КС, судовладелец должен продемонстрировать Регистру выполнение требований 2.2.4.4.3.3 в соответствии с Программой испытаний киберустойчивости судна.

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.5 Восстановление.

Требования направлены на разработку и внедрение соответствующих мер, обеспечивающих возможность восстановления судовых КС и сетей, подвергнутых киберинциденту.

2.2.5.1 План восстановления.

2.2.5.1.1 Требование.

Судовладелец должен разработать План восстановления для возвращения рабочего состояния КС, входящих в область применения настоящей части, после сбоя, вызванного киберинцидентом. План восстановления должен включать в себя подробную информацию о том, где и кем может быть оказана поддержка.

2.2.5.1.2 Детализация требования:

.1 различные заинтересованные стороны, участвующие в проектировании и постройке судна, должны представить судовладельцу информацию для разработки Плана восстановления, который должен быть на борту во время первого ежегодного освидетельствования. План восстановления должен поддерживаться в актуальном состоянии (например, после технического обслуживания) в течение всего срока эксплуатации судна;

.2 План восстановления должен быть понятным для экипажа и берегового персонала и должен включать в себя основные инструкции и процедуры для обеспечения восстановления отказавшей системы, а также, в случае необходимости, способы получения внешней поддержки с берега. Кроме того, на борту должны быть доступны средства или инструменты для восстановления;

.3 при разработке Плана восстановления должны быть указаны различные задействованные системы и подсистемы. Также должны быть определены следующие цели восстановления:

восстановление системы: методы и процедуры по восстановлению коммуникационных возможностей должны определяться в контексте целевого времени восстановления (recovery time objective (RTO)). Оно определяется как время, необходимое для восстановления требуемых каналов связи и возможностей обработки данных;

восстановление данных: методы и процедуры восстановления данных, необходимых для восстановления безопасного состояния ОТ-систем и безопасной эксплуатации судна, должны определяться в контексте целевой точки восстановления (recovery point objective (RPO)). Она определяется как самый длительный период времени, в течение которого допускается отсутствие данных;

.4 после определения целей восстановления должен быть составлен список потенциальных киберинцидентов, а также разработана и описана процедура восстановления;

.5 План восстановления должен включать следующую информацию или же ссылки на нее:

инструкции и процедуры по восстановлению отказавшей системы без нарушения работы резервированной или независимой системы, или местного управления;

процессы и процедуры резервного копирования и безопасного хранения информации;

полную и актуальную логическую схему сети;

список персонала, ответственного за восстановление отказавшей системы;

процедуру связи и список сотрудников для обращения за внешней технической поддержкой, включая поставщиков системы, сетевых администраторов и т.д.

информацию о текущей конфигурации для всех компонентов;

.6 КС, необходимые для управления судном и навигации, должны иметь приоритет в Плане восстановления для обеспечения безопасности экипажа судна;

.7 План восстановления в твердой копии должен быть доступен экипажу и береговому персоналу, ответственному за кибербезопасность и отвечающему за оказание помощи при киберинцидентах.

Обоснование. Процедуры реагирования на инциденты являются важной частью восстановления системы. Ответственный персонал должен знать, выполнять, а также осознавать последствия действий по восстановлению (таких как стирание информации с дисков).

Также следует отметить, что некоторые действия по восстановлению могут привести к уничтожению доказательств, которые могли бы предоставить ценную информацию о причинах инцидента.

В случае необходимости, для оказания помощи в сохранении доказательств при одновременном восстановлении работоспособности может потребоваться получение профессиональной поддержки в реагировании на киберинциденты.

2.2.5.1.3 Подтверждение соответствия.

2.2.5.1.3.1 Этап проектирования:

.1 в Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

ссылки на информацию, предоставленную поставщиками (см. 3.2.1.8), которая может быть полезна судовладельцу для разработки Плана восстановления в случае киберинцидента.

2.2.5.1.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.5.1.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать эффективность процедур и инструкций по восстановлению в случае киберинцидента, предоставленных поставщиками.

2.2.5.1.3.4 Этап эксплуатации:

.1 в Программе кибербезопасности и киберустойчивости судна судовладельцем должны быть описаны планы восстановления всех КС, входящих в область применения настоящей части, учитывающие, как минимум, следующие требования:

описание кто, когда и каким образом восстанавливает КС в случае киберинцидента в соответствии с требованиями 2.2.5.1;

политику резервного копирования с указанием периодичности, обслуживания и проверки резервных копий. Политика должна учитывать допустимое время простоя, доступность альтернативных средств управления, возможность поддержки изготовителя, критичность КС в соответствии с требованиями 2.2.5.2;

ссылки на руководства пользователя или процедуры по резервному копированию, отключению, сбросу, восстановлению и повторному запуску КС в соответствии с требованиями 2.2.5.2 и 2.2.5.3;

.2 первое ежегодное освидетельствование.

Судовладелец должен представить Регистру записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна, а именно то, что:

ответственные члены экипажа на борту судна имеют доступ к инструкциям и/или процедурам по восстановлению в случае киберинцидента;

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

ответственные члены экипажа на борту судна имеют доступ к оборудованию, инструментам, документации и/или к ПО и данным, необходимым для восстановления;

резервные копии КС создаются в соответствии с политиками и процедурами;

ответственные члены экипажа на борту судна имеют доступ к руководствам пользователя и процедурам по отключению, сбросу, восстановлению и повторному запуску;

.3 последующие ежегодные освидетельствования.

По требованию Регистра судовладелец должен продемонстрировать выполнение Программы кибербезопасности и киберустойчивости судна, представив записи или иные задокументированные свидетельства, как указано в 2.2.5.1.3.4.2.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.5.2 Резервное копирование и восстановление.

2.2.5.2.1 Требование.

КС и сети, входящие в область применения настоящей части, должны поддерживать возможность резервного копирования и восстановления своевременным, полным и безопасным образом. Резервные копии должны регулярно обновляться и проверяться.

О б о с н о в а н и е . Целью стратегии резервного копирования и восстановления является защита данных и восстановление данных в случае потери. Как правило, задачи администрирования резервного копирования включают:

планирование и тестирование ответных действий при возникновении различных неисправностей;

настройку среды базы данных для резервного копирования и восстановления;

настройку расписания резервного копирования;

мониторинг среды резервного копирования и восстановления;

создание копии базы данных для долгосрочного хранения;

перемещение данных из одной базы данных (или с одного узла) на другой и т.д.

2.2.5.2.2 Детализация требования.

2.2.5.2.2.1 Способность к восстановлению:

.1 КС, входящие в область применения настоящей части, должны поддерживать возможность резервного копирования и восстановления, позволяющие судну после киберинцидента безопасно восстановить свое рабочее состояние;

.2 должна обеспечиваться возможность восстановления данных из защищенной копии или образа;

.3 информация и средства резервного копирования должны быть достаточными для восстановления после киберинцидента.

2.2.5.2.2.2 Резервное копирование:

.1 КС и сети, входящие в область применения настоящей части, должны обеспечивать резервное копирование данных. Для повышения устойчивости к вредоносному ПО, поражающему онлайн-устройства резервного копирования, должно быть предусмотрено использование автономных резервных копий;

.2 должны быть разработаны планы резервного копирования, с указанием состава резервируемой информации, способа и периодичности создания резервных копий, носителя, а также срока хранения резервных копий.

2.2.5.2.3 Подтверждение соответствия.

2.2.5.2.3.1 Этап проектирования.

На этапе проектирования подтверждение соответствия не требуется.

2.2.5.2.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.5.2.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать процедуры и инструкции по восстановлению КС, входящих в область применения настоящей части, предоставленных поставщиками.

2.2.5.2.3.4 Этап эксплуатации:

.1 очередное освидетельствование.

В случае внесения изменений в КС, судовладелец должен продемонстрировать Регистру выполнение требований 2.2.5.2.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

2.2.5.3 Контролируемое отключение, сброс, откат и повторный запуск.

2.2.5.3.1 Требование.

КС и сети, входящие в область применения настоящей части, для обеспечения быстрого и безопасного восстановления после возникновения неисправности, вызванной киберинцидентом, должны быть способны осуществлять контролируемое отключение, сброс в первоначальное состояние, возврат в безопасное состояние, а также запуск в безопасном режиме из выключенного состояния.

Документация, описывающая выполнение вышеупомянутых операций, должна храниться на борту судна.

2.2.5.3.2 Детализация требования:

.1 КС и сети, входящие в область применения настоящей части, должны обеспечивать:

контролируемое отключение, позволяющее другим подключенным системам завершить/откатить незавершенные транзакции, завершить процессы, закрыть соединения и т.д., оставляя всю интегрированную систему в безопасном, устойчивом и известном состоянии;

сброс, предписывающий системе пройти через процесс выключения, очищения памяти и возвращения компонентов в первоначальное состояние;

откат к предыдущей конфигурации и/или состоянию для восстановления целостности и устойчивости системы;

перезапуск и загрузку актуального образа всего ПО и данных (например, после операции отката) из источника, доступного только для чтения. Время перезапуска должно быть приемлемым, чтобы не препятствовать работе системы по прямому назначению, и не должно приводить другие подключенные системы или интегрированную систему, частью которой она является, в неустойчивое или небезопасное состояние;

.2 экипажу судна должна быть доступна документация, описывающая порядок осуществления вышеупомянутых операций в случае, если система повреждена в результате киберинцидента.

О б о с н о в а н и е . Контролируемое отключение заключается в выключении КС или сети с помощью программной функции, позволяющей другим подключенным системам завершить/откатить ожидающие транзакции, завершить процессы, закрыть соединения и т.д., оставляя всю интегрированную систему в безопасном и известном состоянии. Контролируемое отключение противоположно неконтролируемому отключению, которое происходит, например, когда компьютер принудительно выключается из-за прерывания питания.

---

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

Несмотря на то что в случае некоторых киберинцидентов неконтролируемое отключение может расцениваться как мера предосторожности, в случае интегрированных систем контролируемое отключение предпочтительнее для поддержания их в устойчивом и известном состоянии с предсказуемым поведением. Если стандартные процедуры отключения не выполняются, может произойти повреждение данных или файлов программ и операционной системы. В случае ОТ-систем результатом повреждения могут быть нестабильность, неправильная работа или невозможность работы по назначению.

Операция сброса обычно запускает программно-управляемую загрузку, предписывая системе пройти процесс выключения, очистки памяти и возврата устройств в их первоначальное состояние. В зависимости от рассматриваемой системы операция сброса может иметь различные последствия.

Откат — это операция, которая возвращает систему в некое предыдущее состояние. Откаты важны для целостности данных и системы, поскольку они означают, что данные и программы системы могут быть восстановлены до чистой копии даже после выполнения ошибочных операций. Откаты имеют решающее значение для восстановления после аварий и киберинцидентов, возвращая систему в устойчивое состояние.

Перезапуск системы и повторная загрузка нового образа всего ПО и данных (например, после операции отката) из источника, доступного только для чтения, является эффективным подходом для восстановления после неожиданных сбоев или киберинцидентов. Однако операции перезапуска должны контролироваться, особенно для интегрированных систем, где неожиданный перезапуск отдельного компонента может привести к неустойчивому состоянию системы или ее непредсказуемому поведению.

2.2.5.3.3 Подтверждение соответствия.

2.2.5.3.3.1 Этап проектирования.

В Описание мер обеспечения кибербезопасности системным интегратором должна быть включена следующая информация:

ссылки на руководства пользователя или процедуры, в которых содержится описание безопасного выполнения отключения, сброса, восстановления и повторного запуска КС, входящих в область применения настоящей части.

2.2.5.3.3.2 Этап постройки.

На этапе постройки подтверждение соответствия не требуется.

2.2.5.3.3.3 Этап ввода в эксплуатацию[1]:

.1 системный интегратор должен представить Регистру Программу испытаний киберустойчивости судна (см. 2.3.2.1) и продемонстрировать наличие руководств пользователя или процедур по выполнению отключения, сброса, восстановления и повторного запуска КС, входящих в область применения настоящей части. Эти руководства/процедуры должны быть переданы судовладельцу.

2.2.5.3.3.4 Этап эксплуатации:

.1 очередное освидетельствование.

В случае изменений КС, входящих в область применения настоящей части, судовладелец должен продемонстрировать Регистру выполнение требований 2.2.5.3.3.3 в соответствии с Программой испытаний киберустойчивости судна.

Общие требования к освидетельствованиям во время эксплуатации судна содержатся в 2.3.3.

[1] Допускается не проводить испытания на этапе ввода судна в эксплуатацию, если они проводились на этапе сертификации КС в соответствии с 2.3.2.1.

2.3 ПОДТВЕРЖДЕНИЕ СООТВЕТСТВИЯ

Для оценки соответствия требованиям настоящей части Регистром производится рассмотрение документации и выполняются освидетельствования на соответствующих этапах как указано ниже.

Документация, представляемая поставщиками на одобрение Регистру, указана в разд. 3. Поставщик должен представлять одобренную документацию системному интегратору в соответствии с требованиями 3.5.2.

Документация, представляемая системным интегратором, указана в 2.3.1 и 2.3.2.

Документация, представляемая судовладельцем, указана в 2.2.3.

При сдаче судна, системный интегратор передает судовладельцу:

документацию от поставщиков КС (см. 3.5.2);

документацию, разработанную системным интегратором (см. 2.3.1 и 2.3.2).

(См. также приложения 1 и 2).

2.3.1 Этапы проектирования и постройки.

Поставщик должен подтвердить соответствие требованиям путем сертификации КС согласно 3.5.

Системный интегратор должен подтвердить соответствие требованиям, представив Регистру документацию, указанную ниже.

На этапах проектирования и постройки все изменения проекта должны осуществляться в соответствии с требованиями по управлению изменениями (см. 7.9.6.2.1 части XV «Автоматизация»).

2.3.1.1 Схема зон безопасности и каналов связи.

Содержание этого документа указано в 2.2.2.1.3.1.

2.3.1.2 Описание мер обеспечения кибербезопасности.

Содержание этого документа указано в пунктах «этап проектирования» для каждого требования 2.2.

2.3.1.3 Ведомость судовых КС.

Содержание этого документа указано в 2.2.1.1.

2.3.1.4 Оценка риска для исключения КС от применения требований.

Содержание этого документа указано в 2.4.

2.3.1.5 Описание компенсирующих мер.

Если какая-либо КС, входящая в область применения настоящей части, была одобрена с компенсирующими мерами вместо соответствия требованиям разд. 3, то в этом документе она должна быть обозначена с указанием отсутствующих функциональных возможностей обеспечения безопасности и детальным описанием компенсирующих мер (см. также 3.2.1.3), в документации поставщика должны описываться компенсирующие меры.

2.3.2 Этап ввода в эксплуатацию.

Перед передачей судна в эксплуатацию системный интегратор должен:

представить Регистру актуализированную документацию проекта судна, указанную в 2.3.1;

представить Регистру Программу испытаний киберустойчивости судна, описывающую методы подтверждения соответствия требованиям настоящей части;

провести испытания по Программе испытаний киберустойчивости судна в присутствии инспектора РС.

2.3.2.1 Программа испытаний киберустойчивости судна:

.1 содержание документа указано в пунктах «этап ввода в эксплуатацию» для каждого требования 2.2;

.2 требуемые функциональные возможности обеспечения безопасности и их конфигурация проверяются и испытываются в процессе сертификации каждой КС (см. разд. 3). В случае успешного проведения испытаний в ходе сертификации КС в

соответствии с разд. 3 допускается не проводить отдельные испытания на этапе ввода в эксплуатацию, если это явным образом указано в пунктах «этап ввода в эксплуатацию». Тем не менее Программа испытаний киберустойчивости судна должна включать в себя все испытания, а решение о возможности непроведения испытания принимается Регистром. Испытания должны проводиться, если по результатам сертификации имеются открытые замечания, перенесенные на этап ввода в эксплуатацию, или если выполнение требований обеспечивается при помощи компенсирующих мер, или по иным причинам, таким как внесение изменений в КС после завершения сертификации;

.3 Программа испытаний киберустойчивости судна также должна включать в себя испытания компенсирующих мер, описанных в 2.3.1.2;

.4 Программа испытаний киберустойчивости судна должна обеспечивать возможность регистрации и обновления результатов испытаний, а также содержать следующую информацию:

необходимую тестовую конфигурацию (для обеспечения возможности повторения испытаний с тем же результатом);

испытательное оборудование;

описание начального состояния;

пошаговую методику испытаний;

ожидаемые результаты и критерии успешного прохождения испытаний;

.5 перед тем как направить в Регистр Программу испытаний киберустойчивости судна, системный интегратор должен удостовериться в том, что:

вся информация актуализирована и все изменения вносятся в соответствии с принятыми процедурами управления изменениями (см. 7.9.7.2 части XV «Автоматизация»);

Программа испытаний киберустойчивости судна приведена в соответствие с последними конфигурациями КС и сетей, соединяющими КС как между собой на борту судна, так и с другими КС, не находящимися на борту (например, на берегу);

испытания задокументированы таким образом, чтобы обеспечивалась проверка мер и средств, принятых для выполнения соответствующих требований настоящего раздела, в окончательной конфигурации судовых КС и сетей;

.6 системный интегратор должен задокументировать контрольные испытания или оценку мер и средств безопасности на полностью сопряженных КС, включая управление изменениями конфигураций и отмечая в задокументированных результатах испытаний те случаи, когда на безопасное состояние судна могут негативно повлиять конкретные обстоятельства или отказы, указанные в Программе испытаний киберустойчивости судна;

.7 испытания киберустойчивости судна проводятся только после завершения всех остальных пусконаладочных мероприятий КС;

.8 Регистр может потребовать проведение дополнительных испытаний.

2.3.3 Во время эксплуатации судна.

Судовладелец должен принять технические и организационные меры обеспечения безопасности, перечисленные в настоящем разделе.

Внесение изменений в КС, входящих в область применения настоящей части, должно выполняться в соответствии с требованиями к управлению изменениями (см. 7.9.7.12.1 части XV «Автоматизация»). Это включает в себя поддержание документации КС в актуальном состоянии.

Судовладелец при содействии поставщиков должен поддерживать в актуальном состоянии Программу испытаний киберустойчивости судна в соответствии с судовыми КС и сетями, соединяющими КС как между собой на борту судна, так и с другими КС, не находящимися на борту (например, на берегу). Судовладелец должен обновлять Программу испытаний киберустойчивости судна, учитывая изменения

в судовых КС и сетях, появление возможных рисков, вызванных этими изменениями, новых угроз и уязвимостей, а также других возможных изменений эксплуатационных условий судна.

Судовладелец должен разработать и внедрить организационные процедуры, обеспечить периодическую подготовку и проведение обучения для экипажа судна и соответствующего берегового персонала, с целью их ознакомления с судовыми КС и сетями, соединяющими КС как между собой на борту судна, так и с другими КС, не находящимися на борту (например, на берегу) и надлежащим управлением мерами и средствами, принятыми для выполнения требований настоящей части.

Судовладелец при содействии поставщиков должен поддерживать в актуальном состоянии меры и средства, принятые для выполнения требований настоящей части.

Судовладелец должен хранить на борту копию результатов испытаний и актуальную Программу испытаний киберустойчивости судна, а также представлять эти документы Регистру.

В случае смены судовладельца, требуется проверка Программы кибербезопасности и киберустойчивости судна в объеме первого ежегодного освидетельствования.

2.3.3.1 Первое ежегодное освидетельствование:

.1 до первого ежегодного освидетельствования судна судовладелец должен представить Регистру Программу кибербезопасности и киберустойчивости судна, в которой задокументировано управление кибербезопасностью и киберустойчивостью КС, входящих в область применения настоящей части;

.2 Программа кибербезопасности и киберустойчивости судна должна включать в себя политики, процедуры, планы и/или другую информацию, описывающую процессы и мероприятия, указанные в пунктах «подтверждение соответствия» 2.2;

.3 после того, как Программа кибербезопасности и киберустойчивости судна будет одобрена Регистром, на первом ежегодном освидетельствовании судовладелец должен подтвердить соответствие, представив записи или иные задокументированные свидетельства, подтверждающие внедрение процессов, описанных в одобренной Программе кибербезопасности и киберустойчивости судна.

2.3.3.2 Последующие ежегодные освидетельствования.

При последующих ежегодных освидетельствованиях по требованию Регистра судовладелец должен представить записи или иные задокументированные свидетельства, подтверждающие выполнение Программы кибербезопасности и киберустойчивости судна.

2.3.3.3 Очередное освидетельствование.

При возобновлении классификационного свидетельства судовладелец должен провести испытания по Программе испытаний киберустойчивости судна в присутствии инспектора РС. Определенные меры и средства безопасности должны быть продемонстрированы во время очередного освидетельствования, в то время как другие подлежат проверке в случае изменений в КС, как указано в пунктах «этап эксплуатации» 2.2.

2.4 ОЦЕНКА РИСКА ДЛЯ ИСКЛЮЧЕНИЯ КС ОТ ПРИМЕНЕНИЯ ТРЕБОВАНИЙ

2.4.1 Требование.

В случае если какая-либо КС, входящая в область применения настоящей части, исключается от применения соответствующих требований разд. 2, должна проводиться оценка рисков. Оценка рисков должна подтвердить приемлемый уровень риска, связанного с исключением КС от выполнения требований.

2.4.2 Детализация требования:

.1 на этапе проектирования и постройки судна оценка риска должна проводиться и обновляться системным интегратором с учетом возможных изменений первоначального проекта и вновь обнаруженных угроз и/или уязвимостей, о которых изначально не было известно;

.2 в процессе эксплуатации судна судовладелец должен обновлять оценку риска с учетом изменений киберрисков и обнаружения новых уязвимостей КС. В случае выявления новых рисков судовладелец должен обновить существующие или внедрить новые меры по их снижению;

.3 если в результате изменений уровень риска, связанного с оцениваемыми КС, превысит порог приемлемого, то судовладелец должен представить обновленную оценку риска Регистру на рассмотрение;

.4 для определения вероятности возникновения киберинцидентов и воздействий, которые они могут оказать на безопасность людей, безопасность судна и/или окружающую среду, в оценке риска с учетом категории КС должен проводится анализ предполагаемых условий эксплуатации оцениваемых КС. Должен быть проведен анализ поверхности атаки с учетом степени взаимодействия КС, интерфейсов для портативных устройств, логических ограничений доступа и т.д.;

.5 также должны быть выявлены возникающие риски, связанные с конкретной конфигурацией оцениваемой КС. При оценке риска должно учитываться следующее:

уязвимости объектов;

внутренние и внешние угрозы;

потенциальное воздействие киберинцидентов на безопасность людей, безопасность судна и/или возникновение угрозы для окружающей среды;

возможные негативные влияния на интегрированные системы и интерфейсы между системами, включая системы, не находящиеся на борту судна (например, в случае предоставления удаленного доступа к бортовым системам).

2.4.3 Критерии принятия:

.1 исключение КС, входящей в область применения настоящей части, от применения соответствующих требований может быть принято Регистром только в случае уверенности, что киберриски не влияют на безопасную эксплуатацию КС. Это исключение может быть принято Регистром и в отношении КС, которая не в полной мере соответствует всем нижеуказанным критериям, в случае представления рационального объяснения и доказательств, признанных Регистром удовлетворительными. Для принятия исключения Регистр также вправе потребовать представления дополнительных документов;

.2 при оценке приемлемости уровня риска должны быть соблюдены следующие критерии:

КС изолирована, т.е. не имеет IP-подключений к другим системам и сетям;

КС не имеет физически доступных портов ввода/вывода. Неиспользуемые порты логически отключены. Подключение неавторизованных устройств к КС невозможно;

КС расположена в помещениях с контролируемым доступом;

КС не является интегрированной системой управления, обеспечивающей несколько судовых функций, перечисленных в области применения настоящей части (см. 1.1);

.3 при оценке приемлемости уровня риска должны дополнительно учитываться следующие критерии:

КС не должна использоваться для обеспечения судовых функций категории III;

известные уязвимости, угрозы, потенциальные последствия, которые могут возникнуть в результате киберинцидента, затрагивающего КС, должным образом учтены при оценке рисков;

поверхность атаки для КС сведена к минимуму, учитывая ее сложность, возможность подключения, физические и логические точки доступа, включая беспроводные точки доступа.

О б о с н о в а н и е . Исключение КС, входящих в область применения настоящей части, от применения соответствующих требований должно быть надлежащим образом обосновано и задокументировано. Такое исключение может быть принято Регистром только в том случае, если будут представлены доказательства на основании специальной оценки риска того, что уровень риска, связанный с эксплуатацией КС, находится ниже приемлемого порога.

Оценка риска должна быть основана на имеющихся базах знаний и опыте эксплуатации аналогичных проектов, если таковые имеются, с учетом категории, внешних подключений, а также функциональных требований и характеристик судна и КС. Для лучшего понимания вероятностей и последствий событий, связанных с кибербезопасностью, может быть использована информация о киберугрозах из внутренних и внешних источников.

3 КИБЕРУСТОЙЧИВОСТЬ СУДОВЫХ СИСТЕМ И ОБОРУДОВАНИЯ

3.1 КОНЦЕПЦИЯ БЕЗОПАСНОСТИ

3.1.1 Системы и оборудование.

3.1.1.1 Система может состоять из группы аппаратных и программных средств, обеспечивающих безопасную, защищенную и надежную работу (например, система управления двигателем, система динамического позиционирования и т.д.).

3.1.1.2 Оборудование может относиться к одному или нескольким следующим видам:

сетевые устройства (например, маршрутизаторы, управляемые коммутаторы);

устройства безопасности (например, межсетевые экраны, система обнаружения вторжений);

компьютеры (например, рабочие станции, серверы);

устройства автоматизации (например, программируемые логические контроллеры);

виртуальные машины, размещенные в выделенных ресурсах удаленного компьютера-сервера.

3.1.2 Киберустойчивость.

Требования к киберустойчивости, изложенные в 3.3, относятся ко всем системам, входящим в область применения настоящей части. Дополнительные требования, связанные со взаимодействием с ненадежными сетями, применяются только к системам, в которых такое взаимодействие предусмотрено.

3.1.3 Доступность систем ответственного назначения.

3.1.3.1 Меры безопасности системы ответственного назначения не должны отрицательно влиять на ее работоспособность.

3.1.3.2 Внедрение мер безопасности не должно приводить к потере функциональной безопасности, функций управления и контроля, а также других функций, которые могут привести к отрицательным последствиям для человека, судна и/или окружающей среды.

3.1.3.3 Система должна быть спроектирована таким образом, чтобы при эксплуатации судна обеспечивались конфиденциальность, целостность и доступность данных, необходимых для безопасности судна, его систем, экипажа и груза.

3.1.4 Компенсирующие меры.

3.1.4.1 Компенсирующие меры могут применяться вместо или в дополнение к существующим мерам и средствам безопасности для удовлетворения одного или нескольких требований безопасности.

Компенсирующие меры должны соответствовать замыслу и строгости первоначально заявленного требования, с учетом стандартов, на которые даны ссылки, а также различий между каждым требованием и соответствующими пунктами стандартов, и следовать принципам, указанным в 3.2.1.3.

3.2 ДОКУМЕНТАЦИЯ

3.2.1 Документация КС.

В соответствии с требованиями настоящего раздела должны быть представлены для рассмотрения и одобрения следующие документы (см. также 3.5.2):

3.2.1.1 Ведомость КС.

Ведомость КС должна включать следующую информацию:

.1 перечень аппаратных компонентов (например, хост-устройства, встроенные устройства, сетевые устройства) с указанием следующего:

наименование;

марка/изготовитель;

модель/тип;

краткое описание функции/назначения;

физические интерфейсы (например, сетевые, последовательные);

наименование/тип системного ПО (например, операционная система, микропрограмма);

версия и уровень патча системного ПО;

поддерживаемые протоколы связи;

.2 перечень программных компонентов (например, прикладное ПО, служебное ПО) с указанием следующего:

аппаратный компонент, на котором он установлен;

марка/изготовитель;

модель/тип;

краткое описание функции/назначения;

версия ПО.

3.2.1.2 Топологические схемы:

.1 схема физической топологии должна отражать физическую архитектуру системы. На схеме физической тополоти должно быть возможно определить аппаратные компоненты, указанные в Ведомости КС. На схеме физической топологии должны быть отражены:

все конечные точки и сетевые устройства, включая идентификацию резервных блоков;

кабели связи (сети, последовательные соединения), включая связь с блоками ввода-вывода;

кабели связи с другими сетями или системами;

.2 схема логической топологии должна отражать потоки данных между компонентами системы. На схеме логической топологии должны быть отражены:

конечные точки связи (например, рабочие станции, контроллеры, серверы);

сетевые устройства (коммутаторы, маршрутизаторы, межсетевые экраны);

физические и виртуальные компьютеры;

физические и виртуальные пути связи;

протоколы связи;

.3 допускается представление единой комбинированной топологической схемы, если на ней четко отражена вся требуемая информация.

3.2.1.3 Описание функциональных возможностей обеспечения безопасности:

.1 в этом документе должно быть описано, каким образом в КС с ее аппаратными и программными компонентами реализуются требуемые функциональные возможности обеспечения безопасности, указанные в 3.3.1;

.2 должны быть описаны любые сетевые интерфейсы с другими КС, входящими в область применения настоящей части. Описание должно включать КС назначения, потоки данных и протоколы связи. В случае, если системный интегратор выделил КС назначения в другую зону безопасности, то должны быть подробно описаны компоненты, обеспечивающие защиту границы зоны безопасности (см. 2.2.2.1), если они поставляются в составе КС;

.3 также должны быть описаны любые сетевые интерфейсы к другим системам или сетям, не входящими в область применения настоящей части (ненадежные сети). В описании должно быть указано соответствие дополнительным функциональным возможностям обеспечения безопасности, перечисленным в 3.3.2, а также содержаться соответствующие процедуры или инструкции для экипажа. Компоненты, обеспечивающие защиту границы зоны безопасности (см. 2.2.2.1), должны быть подробно описаны, если они поставляются в составе КС;

.4 каждому требованию должна быть отведена отдельная глава. Описание должно включать в себя все аппаратные и программные компоненты системы, если необходимо;

.5 если какое-либо требование выполняется не полностью, то это указывается в описании и предлагаются компенсирующие меры. Компенсирующие меры должны:

защищать от тех же угроз, что и первоначальное требование;

обеспечивать такой же уровень защиты, что и первоначальное требование;

не быть мерой контроля безопасности, требуемой другими требованиями в настоящем разделе;

не создавать повышенные риски безопасности;

.6 в описании должны быть указаны ссылки на любые подтверждающие документы (например, информация об изготовителе), необходимые для проверки соответствия требованиям.

3.2.1.4 Программа испытаний функциональных возможностей обеспечения безопасности.

.1 в документе должны быть описаны методы испытаний, подтверждающие соответствие системы требованиям 3.3.1 и 3.3.2, включая любые компенсирующие меры. Допускается подтверждение соответствия при помощи аналитической оценки (где применимо);

.2 Программа испытаний функциональных возможностей обеспечения безопасности должна включать в себя отдельную главу для каждого применимого требования и содержать следующую информацию:

необходимую тестовую конфигурацию (для обеспечения возможности повторения испытаний с тем же результатом);

испытательное оборудование;

описание начального состояния;

пошаговую методику испытаний;

ожидаемые результаты и критерии успешного прохождения испытаний;

.3 Программа испытаний функциональных возможностей обеспечения безопасности также должна обеспечивать возможность регистрации и обновления результатов испытаний.

3.2.1.5 Руководство по конфигурации безопасности.

В документе должны быть описаны рекомендуемые параметры конфигурации функциональных возможностей обеспечения безопасности и указаны значения по умолчанию. Цель документа заключается в том, чтобы обеспечить реализацию функциональных возможностей обеспечения безопасности в соответствии с требованиями разд. 2 и любыми спецификациями системного интегратора (например, учетные записи пользователей, авторизация, политика паролей, безопасное состояние оборудования, правила брандмауэра и т.д.).

Документ должен служить основанием для проверки выполнения п. 29 табл. 3.3.1.

3.2.1.6 Документы по жизненному циклу безопасной разработки.

Документация представляется по требованию Регистра. В документации должны быть описаны процессы и процедуры поставщика в соответствии с требованиями к жизненному циклу безопасной разработки, изложенными в 3.4. Должен быть описан процесс обновления ПО и установки патчей. Документ представляется с целью подготовки к освидетельствованию в соответствии с 3.5.3.4.

3.2.1.7 Планы технического обслуживания и верификации КС.

Документы должны представляться по требованию Регистра, в документах должны содержаться процедуры технического обслуживания и испытаний системы, связанные с безопасностью. Документы должны содержать инструкции для пользователя по проверке работы функций безопасности системы в соответствии с требованиями п. 19 табл. 3.3.1.

3.2.1.8 Информация для поддержки разработки планов реагирования и восстановления в случае киберинцидента.

Документ представляется по требованию Регистра, в документе должны содержаться процедуры или инструкции, позволяющие пользователю выполнить следующее:

местное независимое управление (см. 2.2.4.2);

изоляцию сети (см. 2.2.4.3);

расследование киберинцидента с использованием записей аудита (см. п. 13 табл. 3.3.1);

детерминировать поток выходных сигналов (см. 2.2.4.4 и п. 20 табл. 3.3.1);

резервирование (см. п. 26 табл. 3.3.1);

восстановление (см. п. 27 табл. 3.3.1)**;**

контролируемое отключение, сброс, откат и повторный запуск (см. 2.2.5.3).

3.2.1.9 Управление изменениями.

Документ представляется по требованию Регистра. Документ не является специфичным для кибербезопасности и требуется также в соответствии с 7.9 части XV «Автоматизация».

3.2.1.10 Протоколы испытаний.

КС, имеющие Свидетельство о типовом одобрении (СТО) РС, подтверждающее соответствие функциональных возможностей обеспечения безопасности данного раздела, могут быть освобождены от освидетельствования. Однако Регистру должны быть представлены протоколы испытаний, заверенные поставщиком и подтверждающие, что поставщик завершил проектирование, изготовление, испытания, настройку и усиление защиты, которые в случае отсутствия СТО проверяются Регистром при освидетельствовании (см. 3.5.3).

3.3 ТРЕБОВАНИЯ К СИСТЕМЕ

Требования настоящей главы основаны на требованиях стандарта IEC 62443-3-3, которыми необходимо руководствоваться при проектировании и изготовлении КС.

3.3.1 Требуемые функциональные возможности обеспечения безопасности.

Требуемые функциональные возможности обеспечения безопасности представлены в табл. 3.3.1.

Таблица 3.3.1

№	Задача	Требования
Защита от случайного или совпадающего доступа лиц, не прошедших проверку подлинности		
1	Идентификация и аутентификация пользователя – физического лица	КС должна обеспечивать возможность идентификации и аутентификации всех пользователей – физических лиц, которые могут получить доступ к системе напрямую или через интерфейсы. (См. IEC 62443-3-3:2013/SR 1.1)
2	Управление учетными записями	КС должна обеспечивать возможность управления всеми учетными записями авторизованных пользователей, включая добавление, активацию, изменение, деактивацию и удаление учетных записей. (См. IEC 62443-3-3:2013/SR 1.3)
3	Управление идентификаторами	КС должна обеспечивать возможность управления идентификаторами по пользователям, группам и ролям. (См. IEC 62443-3-3:2013/SR 1.4)
4	Управление аутентификаторами	КС должна обеспечивать возможность: инициализации содержания аутентификатора; изменения всех аутентификаторов, заданных по умолчанию, после инсталляции системы управления; изменения/обновления всех аутентификаторов; и защиты всех аутентификаторов от неавторизованного раскрытия и изменения в ходе их ввода и передачи. (См. IEC 62443-3-3:2013/SR 1.5)
5	Управление беспроводным доступом	КС должна обеспечивать возможность идентификации и аутентификации всех пользователей (физических лиц, программных процессов или устройств), участвующих в беспроводной коммуникации. (См. IEC 62443-3-3:2013/SR 1.6)
6	Надежность аутентификации по паролю	КС должна обеспечивать настраиваемую надежность конфигурируемых паролей на основе минимальной длины и разнотипности символов. (См. IEC 62443-3-3:2013/SR 1.7)
7	Обратная связь при аутентификации	КС должна обеспечивать скрытность в ходе процесса аутентификации. (См. IEC 62443-3-3:2013/SR 1.10)
Защита от непреднамеренного или случайного неправильного использования		
8	Контроль выполнения авторизаций	Пользователям – физическим лицам должна быть назначена авторизация на всех интерфейсах в соответствии с принципами разделения полномочий и минимальных привилегий. (См. IEC 62443-3-3:2013/SR 2.1)

№	Задача	Требования
9	Контроль беспроводного использования	КС должна обеспечивать возможность авторизации, отслеживания и установления ограничений на беспроводное подключение к системе в соответствии с общепринятыми практиками индустрии безопасности. (См. IEC 62443-3-3:2013/SR 2.2)
10	Контроль использования носимых и переносных устройств	Если КС поддерживает использование носимых и переносных устройств, система должна обеспечивать возможность: ограничения использования носимых и переносных устройств только теми, которые разрешены конструктивно; ограничение на передачу кодов и данных от/на носимые и переносные устройства. П р и м е ч а н и е . Для отдельных систем могут быть допущены ограничители/блокираторы (в том числе силикон) портов. (См. IEC 62443-3-3:2013/SR 2.3)
11	Мобильный код	КС должна контролировать использование мобильного кода, такого как java-скрипты, ActiveX и PDF. (См. IEC 62443-3-3:2013/SR 2.4)
12	Блокировка сеанса	КС должна блокировать дальнейший доступ по истечении заданного времени в случае отсутствия активности или после ручной активации блокировки сеанса. (См. IEC 62443-3-3:2013/SR 2.5)
13	События, подлежащие аудиту	КС должна регистрировать, по крайней мере, следующие события, относящиеся к безопасности: управление доступом, события операционной системы, события резервного копирования и восстановления, изменения конфигурации, потеря связи. (См. IEC 62443-3-3:2013/SR 2.8)
14	Емкость систем хранения данных аудита	КС должна выделять достаточную емкость для системы хранения записей аудита в соответствии с общепризнанными рекомендациями по управлению файлами регистрации и конфигурированию систем. Система управления должна предусматривать такие механизмы аудита, которые снижают вероятность переполнения хранилища. (См. IEC 62443-3-3:2013/SR 2.9)
15	Ответные действия в случае сбоев обработки данных аудита	В случае сбоя при проведении аудита, КС должна предотвратить потерю ответственных сервисов и функций. (См. IEC 62443-3-3:2013/SR 2.10)
16	Временные метки	КС должна проставлять временные метки в записях аудита. (См. IEC 62443-3-3:2013/SR 2.11)
Защита целостности КС от непреднамеренных действий		
17	Целостность коммуникации	КС должна защищать целостность передаваемой информации. П р и м е ч а н и е . В беспроводных сетях должны использоваться криптографические механизмы. (См. IEC 62443-3-3:2013/SR 3.1)

№	Задача	Требования
18	Защита от вредоносного кода	КС должна обеспечивать возможность применения защитных мер для предотвращения, обнаружения и уменьшения воздействий вредоносного кода или неавторизованного ПО. КС должна обеспечивать возможность обновления защитных мер. (См. IEC 62443-3-3:2013/SR 3.2)
19	Верификация функций безопасности	КС должна обеспечивать возможность проверки предполагаемой работы функций безопасности и сообщать о возникновении аномалий во время технического обслуживания. (См. IEC 62443-3-3:2013/SR 3.3)
20	Детерминированный поток выходных сигналов	КС должна обеспечивать возможность приведения выходов в заранее определенное состояние, если в результате атаки не может поддерживаться штатная работа. Заранее определенное состояние может быть следующим: состояние без питания; последнее известное значение; фиксированное значение. (См. IEC 62443-3-3:2013/SR 3.6)
Предотвращение несанкционированного раскрытия информации путем перехвата или случайного воздействия		
21	Конфиденциальность информации	КС должна обеспечивать возможность защиты конфиденциальности информации, чтение которой подлежит авторизации, будь то хранящаяся или передаваемая информация. Примечание. Для беспроводной сети должны использоваться криптографические механизмы для защиты конфиденциальности всей передаваемой информации. (См. IEC 62443-3-3:2013/SR 4.1)
22	Использование криптографии	В случае использования криптографии КС должна использовать криптографические алгоритмы, размеры ключей и механизмы в соответствии с общепринятой в индустрии безопасности практикой и рекомендациями. (См. IEC 62443-3-3:2013/SR 4.3)
Контроль за работой КС и реагирование на инциденты		
23	Доступность журнала аудита	КС должна обеспечить доступность журнала аудита в режиме «только чтение» авторизованным физическим лицам и/или инструментам. (См. IEC 62443-3-3:2013/SR 6.1)

№	Задача	Требования
Обеспечение надежной работы КС в нормальных производственных условиях		
24	Защита от отказа в обслуживании	КС должна обеспечивать минимальные возможности для поддержки основных функций во время событий типа «отказ в обслуживании» (DoS). Примечание. Допускается, что КС может работать в ухудшенном режиме при возникновении событий DoS, но она не должна выходить из строя таким образом, который может привести к опасным ситуациям. Следует учитывать события DoS, основанные на перегрузке, т.е. когда предпринимается попытка переполнения пропускной способности сети и когда предпринимается попытка использования ресурсов компьютера. (См. IEC 62443-3-3:2013/SR 7.1)
25	Управление ресурсами	Функции безопасности КС должны обеспечивать возможность ограничения использования ресурсов для предотвращения их истощения. (См. IEC 62443-3-3:2013/SR 7.2)
26	Резервирование системы	Идентификация и расположение критически важных файлов, а также возможность создания резервных копий информации на уровне пользователя и системы (включая информацию о состоянии системы) должны поддерживаться КС, не влияя на нормальную работу. (См. IEC 62443-3-3:2013/SR 7.3)
27	Восстановление системы	После сбоя или отказа КС должна обеспечивать возможность своего восстановления до известного безопасного состояния. (См. IEC 62443-3-3:2013/SR 7.4)
28	Альтернативный источник питания	КС должна обеспечивать возможность переключения на альтернативный источник питания и обратно без влияния на существующий уровень безопасности или наличие предусмотренного и задокументированного режима ограниченной функциональности. (См. IEC 62443-3-3:2013/SR 7.5)
29	Параметры конфигурации сети и безопасности	КС должна обеспечивать возможность своего конфигурирования в соответствии с рекомендованными конфигурациями сети и безопасности, как описано в документации изготовителя. КС должна обеспечивать интерфейс для текущих параметров конфигурации сети и безопасности. (См. IEC 62443-3-3:2013/SR 7.6)
30	Минимальная функциональность	Установка, доступность и права доступа к следующим элементам должны быть строго ограничены потребностями функций, выполняемых КС: программные компоненты операционных систем, процессы и сервисы; сетевые сервисы, порты, протоколы, маршруты и доступ к узлам, а также любое ПО. (См. IEC 62443-3-3:2013/SR 7.7)

3.3.2 Дополнительные функциональные возможности обеспечения безопасности.

Для КС с сетевым подключением к ненадежным сетям (т.е. интерфейсом к любым сетям, не входящим в область применения настоящей части) предъявляются дополнительные требования согласно табл. 3.3.2.

КС, которые взаимодействуют через границу зоны безопасности, должны также соответствовать требованиям к сегментации сети и защите границ зон, указанным в 2.2.2.1 и 2.2.2.2.

Таблица 3.3.2

№	Задача	Требования
31	Многофакторная аутентификация для пользователей – физических лиц	В случае предоставления доступа к КС пользователям – физическим лицам из ненадежной сети или через нее, требуется многофакторная аутентификация. (См. IEC 62443-3-3:2013/SR 1.1, RE 2)
32	Идентификация и аутентификация программных процессов и устройств	КС должна идентифицировать и аутентифицировать программные процессы и устройства. (См. IEC 62443-3-3:2013/SR 1.2)
33	Неудачные попытки входа в систему	КС должна обеспечивать ограничение количества последовательных неудачных попыток входа в систему из ненадежных сетей в течение определенного периода времени. (См. IEC 62443-3-3:2013/SR 1.11)
34	Уведомление об использовании системы	КС должна обеспечивать возможность отображения сообщения об использовании системы перед аутентификацией. Должна быть предусмотрена возможность конфигурирования этого сообщения уполномоченным персоналом. (См. IEC 62443-3-3:2013/SR 1.12)
35	Доступ через ненадежные сети	Любой доступ к КС из ненадежных сетей или через них должен отслеживаться и контролироваться. (См. IEC 62443-3-3:2013/SR 1.13)
36	Принятие явного запроса на доступ	КС должна отклонить доступ из ненадежных сетей или через них, за исключением случаев, когда это явно одобрено уполномоченным экипажем на борту судна. (См. IEC 62443-3-3:2013/SR 1.13, RE1)
37	Завершение удаленного сеанса	КС должна обеспечивать возможность завершения удаленного сеанса либо автоматически после настраиваемого периода времени неактивности, либо вручную пользователем, инициировавшим сеанс. (См. IEC 62443-3-3:2013/SR 2.6)
38	Защита целостности средствами криптографии	КС должна использовать криптографические механизмы для выявления изменений информации во время связи с ненадежными сетями или через них. (См. IEC 62443-3-3:2013/SR 3.1, RE1)
39	Валидация входных данных	КС должна проверять синтаксис, длину и содержание любых входных данных из ненадежных сетей, которые служат входными данными для управления процессом или являются входными данными, непосредственно влияющими на работу КС. (См. IEC 62443-3-3:2013/SR 3.5)

№	Задача	Требования
40	Целостность сеанса	КС должна защищать целостность сеансов. Недействительные идентификаторы сеансов должны быть отклонены. (См. IEC 62443-3-3:2013/SR 3.8)
41	Аннулирование идентификаторов сеанса после завершения сеанса	Система должна аннулировать идентификаторы сеансов при выходе пользователя из системы или другом завершении сеанса (включая сеансы браузера). (См. IEC 62443-3-3:2013/SR 3.8, RE1)

3.4 ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ БЕЗОПАСНОЙ РАЗРАБОТКИ

При разработке систем или оборудования должен соблюдаться жизненный цикл безопасной разработки (secure development lifecycle (SDLC)), учитывающий аспекты безопасности на следующих этапах:

этап анализа требований;

этап проекта;

этап внедрения;

этап проверки;

этап выпуска;

этап технической поддержки;

этап окончания срока службы.

Должен быть подготовлен и представлен Регистру на рассмотрение и одобрение документ, описывающий, каким образом на вышеуказанных этапах учтены аспекты безопасности и, как минимум, содержащий описание управляемых процессов, указанных в 3.4.1 — 3.4.7.

3.4.1 Изготовитель должен иметь процедурные и технические средства контроля для защиты закрытых ключей, используемых для написания кода, от несанкционированного доступа или модификации, если применимо (см. IEC 62443-4-1:2018/SM-8).

3.4.2 Должен быть внедрен процесс, обеспечивающий доступ пользователей к документации об обновлениях безопасности изделия (что может быть осуществлено путем установления контактного лица по кибербезопасности или при помощи периодических публикаций, к которым пользователь может получить доступ), включающей в себя следующее, но не ограничиваясь этим (см. IEC 62443-4-1:2018/SUM-2):

.1 номер(а) версии ПО, к которому применяется патч безопасности;

.2 инструкции по установке утвержденных патчей вручную и с помощью автоматизированного процесса;

.3 описание любых последствий, включая перезагрузку, которые может повлечь за собой установка патча;

.4 инструкция по проверке, что утвержденный патч был установлен; и

.5 риски, связанные с неустановлением патча и с использованием неодобренных средств обновления.

3.4.3 Должен быть внедрен процесс, обеспечивающий предоставление пользователям документации об обновлениях безопасности зависимых компонентов или операционной системы, включающей в себя следующее, но не ограничиваясь этим (см. IEC 62443-4-1:2018/SUM-3):

.1 указание о том, совместим ли продукт с зависимым компонентом или обновлением безопасности операционной системы.

3.4.4 Должен быть внедрен процесс, обеспечивающий предоставление пользователям обновлений безопасности для всех поддерживаемых изделий и версий изделий таким образом, чтобы облегчить проверку подлинности патча безопасности (см. IEC 62443-4-1:2018/SUM-4).

Изготовитель должен иметь процедуру контроля качества для проверки обновления перед выпуском.

3.4.5 Должен быть внедрен процесс разработки документации на изделие, содержащей описание стратегии эшелонированной защиты изделия для поддержки установки, эксплуатации и технического обслуживания и включающей в себя следующее (см. IEC 62443-4-1:2018/SG-1):

.1 функциональные возможности обеспечения безопасности, реализуемые изделием, и их роль в стратегии эшелонированной защиты;

.2 угрозы, на которые направлена стратегия эшелонированной защиты; и

.3 стратегии пользователя изделия по снижению рисков безопасности, связанных с продуктом, включая риски, связанные с устаревшим кодом.

3.4.6 Должен быть внедрен процесс разработки пользовательской документации, описывающей меры обеспечения эшелонированной защиты в ожидаемых условиях внешней среды работы изделия (см. IEC 62443-4-1:2018/SG-2).

3.4.7 Должен быть внедрен процесс разработки документации пользователя изделия, которая включает в себя руководство по усилению защиты изделия при его установке и обслуживании (см. IEC 62443-4-1:2018/SG-3). Руководство должно включать, помимо прочего, инструкции, обоснование и рекомендации в отношении следующего:

.1 интеграция изделия, включая компоненты сторонних производителей, в контексте безопасности изделия;

.2 интеграция интерфейсов/протоколов прикладного программирования продукта с пользовательскими приложениями;

.3 применение и поддержание изделием стратегии эшелонированной защиты;

.4 конфигурация и использование параметров безопасности для поддержки локальных политик безопасности, а также для каждого параметра безопасности:

их вклад в стратегию эшелонированной защиты;

описания конфигурируемых и стандартных значений, включающие информацию о влиянии каждого из них на безопасность, а также о потенциальном воздействии каждого из них на методы работы; и

установка/изменение/удаление их значения;

.5 инструкции и рекомендации по использованию всех инструментов и утилит, связанных с безопасностью, которые поддерживают администрирование, мониторинг, обработку инцидентов и оценку безопасности изделия;

.6 инструкции и рекомендации по проведению периодических мероприятий по поддержанию безопасности;

.7 инструкции по информированию поставщика изделия об инцидентах, связанных с безопасностью изделия;

.8 описание лучших практик безопасности для обслуживания и администрирования изделия.

3.5 ПОДТВЕРЖДЕНИЕ СООТВЕТСТВИЯ

3.5.1 Введение.

Поставщики совместно с системным интегратором должны определить, являются ли требования разд. 3 обязательными для КС (см. рис. 3.5.1-1).

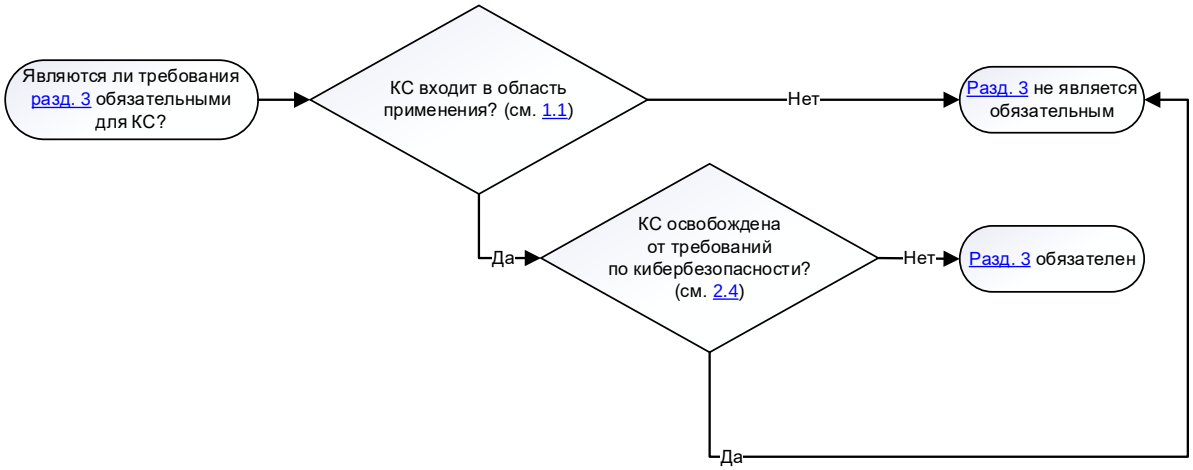

Рис. 3.5.1-1

Должно быть продемонстрировано соответствие требованиям безопасности, как указано на рис. 3.5.1-2. Этот процесс классификации относится к конкретному судну и завершается выдачей свидетельства РС на систему.

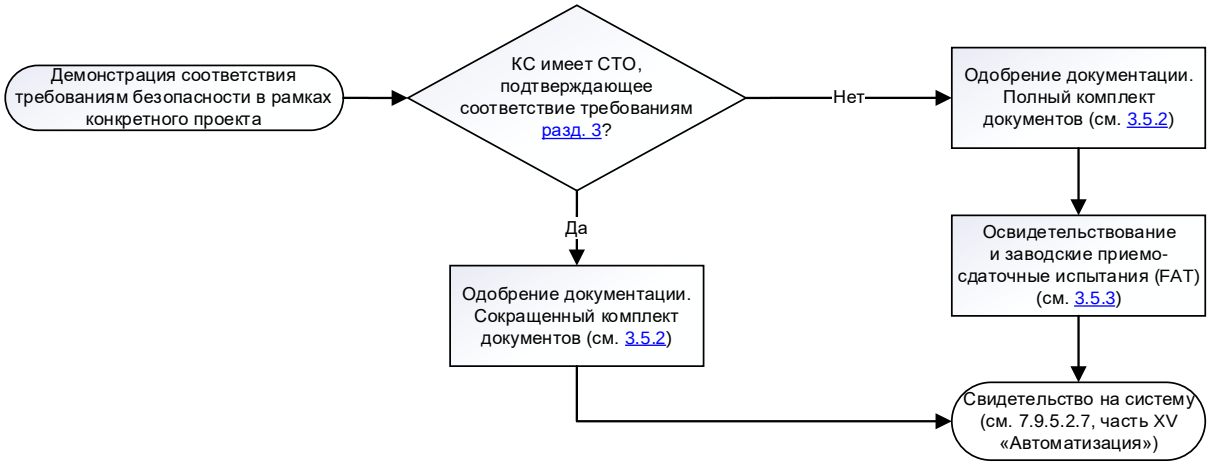

Рис. 3.5.1-2

Типовое одобрение является добровольным и применяется к КС, которые являются стандартными и изготавливаются в режиме установившегося производства. Требования к сертификации и типовому одобрению КС изложены в 7.9.5.2.4 части XV «Автоматизация».

Процессы, представленные на рис. 3.5.1-1 и 3.5.1-2, применяются также, если для навигационного оборудования и оборудования радиосвязи используются другие эквивалентные стандарты (см. 1.1.5). В таком случае:

процесс на рис. 3.5.1-1 иллюстрирует, является ли эквивалентный стандарт обязательным (вместо требований разд. 3).

процесс на рис. 3.5.1-2 иллюстрирует, что процесс сертификации может быть сокращен, если КС имеет СТО в соответствии с эквивалентным стандартом.

3.5.2 Одобрение документации.

Одобрение документации — это оценка документов КС, предназначенных для конкретного судна. Документы, указанные в 3.2, должны быть представлены поставщиком с целью подтверждения соответствия требованиям настоящего раздела.

Если КС имеет действующее СТО РС, подтверждающее соответствие требованиям настоящего раздела, поставщик может представить Регистру сокращенный комплект документов, относящихся к конкретному судну (см. приложение 3).

Одобренная версия документов должна быть включена в комплект поставки КС системному интегратору.

3.5.3 Освидетельствование и заводские приемо-сдаточные испытания.

Освидетельствование и заводские приемо-сдаточные испытания (factory acceptance test (FAT)) — это проверка КС, поставляющейся на конкретное судно и не имеющей действующего СТО РС, подтверждающего соответствие требованиям настоящего раздела.

Освидетельствование и FAT проводятся с целью подтверждения при помощи испытаний и/или аналитической оценки соответствия КС применимым требованиям настоящего раздела. Освидетельствование и FAT проводятся на предприятии поставщика или на других предприятиях, имеющих соответствующее оборудование для проведения испытаний и проверок.

После завершения одобрения документации и освидетельствования с положительным результатом Регистр выдаст свидетельство на систему, которое должно сопровождать КС при поставке системному интегратору.

3.5.3.1 Общие элементы освидетельствования.

Поставщик должен продемонстрировать, что проектирование, изготовление и внутренние испытания были завершены. Также должно быть продемонстрировано, что поставляемая система соответствует одобренной документации. Это должно быть сделано путем проверки системы и сравнения компонентов и расположения/архитектуры с Ведомостью КС (см. 3.2.1.1) и топологическими схемами (см. 3.2.1.2).

3.5.3.2 Испытания функциональных возможностей обеспечения безопасности.

Поставщик должен провести испытания требуемых функциональных возможностей обеспечения безопасности поставляемой системы. Испытания должны проводиться в соответствии с одобренной программой испытаний, указанной в 3.2.1.4, в присутствии инспектора РС.

Испытания должны продемонстрировать инспектору РС, что все требования выполнены. Испытание идентичных компонентов как правило не требуется.

3.5.3.3 Правильная конфигурации функциональных возможностей обеспечения безопасности.

Поставщик должен продемонстрировать инспектору РС, что параметры безопасности в компонентах системы сконфигурированы в соответствии с рекомендациями, приведенными в 3.2.1.5. Эта демонстрация может быть проведена совместно с проверкой функциональных возможностей обеспечения безопасности.

Параметры безопасности должны быть задокументированы в отчете, например, в руководстве по конфигурации для конкретного судна.

3.5.3.4 Жизненный цикл безопасной разработки.

Поставщик должен, согласно документации, указанной в 3.2.1.6, продемонстрировать соответствие требованиям к жизненному циклу безопасной разработки, изложенным в 3.4.

3.5.3.4.1 Средства управления закрытыми ключами (см. IEC 62443-4-1:2018/SM-8).

Это требование применяется, если система включает в себя ПО, имеющее цифровую подпись с целью предоставления пользователю возможности проверить его подлинность.

Поставщик должен представить документацию по системе менеджмента, подтверждающую наличие политик, процедур и технических средств контроля для защиты от несанкционированного доступа создания, хранения и использования закрытых ключей, используемых для написания кода.

Политики и процедуры должны определять роли, обязанности и рабочие процессы. Технический контроль должен включать, например, ограничение физического доступа и криптографическое оборудование (например, аппаратный модуль безопасности) для хранения закрытого ключа.

3.5.3.4.2 Документация по обновлениям безопасности (см. IEC 62443-4-1:2018/SUM-2).

Поставщик должен представить документацию по системе менеджмента, подтверждающую, что в организации внедрен процесс, обеспечивающий информирование пользователей об обновлениях системы безопасности. Информация для пользователей должна включать элементы, перечисленные в 3.4.2.

3.5.3.4.3 Документация по обновлениям безопасности зависимых компонентов (см. IEC 62443-4-1:2018/SUM-3).

Поставщик должен представить документацию по системе менеджмента в соответствии с требованиями 3.4.3, подтверждающую, что в организации внедрен процесс, гарантирующий информирование пользователей о том, совместима ли система с обновленными версиями приобретенного ПО в системе (новые версии/патчи операционной системы или микропрограммы). Информация должна касаться того, как управлять рисками, связанными с неприменением обновленного приобретенного ПО.

3.5.3.4.4 Поставка обновлений безопасности (см. IEC 62443-4-1:2018/SUM-4).

Поставщик должен представить документацию по системе менеджмента в соответствии с требованиями 3.4.4, подтверждающую, что в организации внедрен процесс, обеспечивающий доступность обновлений безопасности системы для пользователей и описывающий, как пользователь может проверить подлинность обновленного ПО.

3.5.3.4.5 Эшелонированная защита изделия (см. IEC 62443-4-1:2018/SG-1).

Поставщик должен представить документацию по системе менеджмента в соответствии с требованиями 3.4.5, подтверждающую, что в организации внедрен процесс по документированию стратегии мер эшелонированной защиты с целью снижения угроз безопасности ПО в КС во время установки, технического обслуживания и эксплуатации.

Примерами угроз могут быть установка несанкционированного ПО, слабые места в процессе исправления, вмешательство в ПО на этапе эксплуатации судна.

3.5.3.4.6 Меры эшелонированной защиты, в ожидаемых условиях внешней среды работы (см. IEC 62443-4-1:2018/SG-2).

Поставщик должен представить документацию по системе менеджмента в соответствии с требованиями 3.4.6, подтверждающую, что в организации внедрен процесс документирования мер эшелонированной защиты, которые, как ожидается, будут обеспечены внешней средой, таких как физическое расположение, политика и процедуры.

3.5.3.4.7 Рекомендации по усилению безопасности (см. IEC 62443-4-1:2018/SG-3).

Поставщик должен представить документацию по системе менеджмента, в соответствии с требованиями 3.4.7, подтверждающую, что в организации внедрен процесс, гарантирующий разработку руководства по усилению безопасности системы. В руководстве должно быть указано, как уменьшить уязвимости в системе путем удаления/запрета/отключения ненужного ПО, учетных записей, служб и т.д.

ПРИЛОЖЕНИЕ 1

ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ И ДОКУМЕНТАЦИИ

Условные обозначения

Представление	Указанная заинтересованная сторона представляет в Регистр документацию для проверки на соответствие требованиям разд. 2 и одобрения.
Поддержание	Указанная заинтересованная сторона поддерживает документ в актуальном состоянии в соответствии с требованиями по управлению изменениями. Актуализированный документ и записи об управлении изменениями представляются в Регистр в соответствии с требованиями 7.9 части XV «Автоматизация».
Предъявление	Указанная заинтересованная сторона демонстрирует Регистру соответствие требованиям по одобренной документации.

Документ	**Системный интегратор**			**Судовладелец**			
	Проектирование	Постройка	Сдача в эксплуатацию	Эксплуатация	Первое ежегодное освидетельствование	Ежегодное освидетельствование	Очередное освидетельствование
Одобренная документация поставщика (см. 2.3)		Поддержание	Поддержание	Поддержание			
Схема зон безопасности и каналов связи (см. 2.3.1.1)	Представление	Поддержание	Поддержание	Поддержание			
Описание мер обеспечения кибербезопасности (см. 2.3.1.2)	Представление	Поддержание	Поддержание	Поддержание			
Ведомость судовых КС (см. 2.3.1.3)	Представление	Поддержание	Поддержание	Поддержание			
Оценка риска для исключения КС от применения требований (см. 2.3.1.4)[1]	Представление	Поддержание	Поддержание	Поддержание			
Описание компенсирующих мер (см. 2.3.1.5)[1]	Представление	Поддержание	Поддержание	Поддержание			
Программа испытаний киберустойчивости судна (см. 2.3.2.1)		Представление	Предъявление	Поддержание			Предъявление

Документ	Системный интегратор			Судовладелец			
	Проектирование	Постройка	Сдача в эксплуатацию	Эксплуатация	Первое ежегодное освидетельствование	Ежегодное освидетельствование	Очередное освидетельствование
Программа кибербезопасности и киберустойчивости судна (см. 2.3.3.1): управление изменениями (см. 2.2.1.1.3.4); управление обновлениями ПО (см. 2.2.1.1.3.4); управление межсетевыми экранами (см. 2.2.2.1.3.4); управление защитой от вредоносного ПО (см. 2.2.2.3.3.4); управление контролем доступа (см. 2.2.2.4.3.4); управление конфиденциальной информацией (см. 2.2.2.4.3.4); управление удаленным доступом (см. 2.2.2.6.3.4); управление носимыми и переносными устройствами (см. 2.2.2.7.3.4); обнаружение аномалий безопасности (см. 2.2.3.1.3.4); диагностика функций безопасности (см. 2.2.3.2.3.4); план действий в случае киберинцидента (см. 2.2.4.1.3.4); план восстановления (см. 2.2.5.1.3.4)				Поддержание	Представление	Предъявление	

[1] Если применимо.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ ТРЕБОВАНИЙ И ДОКУМЕНТАЦИИ

Ведомость судовых КС (см. 2.2.1.1)		
Функциональные возможности обеспечения безопасности КС	Документация по обновлениям безопасности	См. 3.4.2
	Документация по обновлениям безопасности зависимых компонентов	См. 3.4.3
	Поставка обновлений безопасности	См. 3.5.3.4.4
Документация КС	Ведомость КС	См. 3.2.1.1
	Управление планом изменений	См. 3.2.1.9
Документация проекта судна	Ведомость судовых КС	См. 2.2.1.1.3.1
Программа кибербезопасности и киберустойчивости судна	Управление изменениями	См. 2.2.1.1.3.4
	Управление обновлениями ПО	См. 2.2.1.1.3.4

Зоны безопасности и сегментация (см. 2.2.2.1)		
Функциональные возможности обеспечения безопасности КС		
Документация КС	Топологические схемы	См. 3.2.1.2
Документация проекта судна	Схема зон безопасности и каналов связи	См. 2.2.2.1.3.1
	Описание мер обеспечения кибербезопасности	См. 2.2.2.1.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.2.1.3.3
Программа кибербезопасности и киберустойчивости судна	Управление оборудованием, ограничивающим зоны безопасности (например, межсетевыми экранами)	См. 2.2.2.1.3.4

Меры обеспечения безопасности сети (см. 2.2.2.2)		
Функциональные возможности обеспечения безопасности КС	Защита от событий типа «отказ в обслуживании» (DoS)	См. п. 29 табл. 3.3.1
	Детерминированный поток выходных сигналов	См. п. 20 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
Документация проекта судна	Программа испытаний киберустойчивости судна	См. 2.2.2.2.3.3
Программа кибербезопасности и киберустойчивости судна		

Антивирусные, антивредоносные, антиспам программы и другие средства защиты от вредоносного кода (см. 2.2.2.3)		
Функциональные возможности обеспечения безопасности КС	Защита от вредоносного кода	См. п. 18 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.2.3.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.2.3.3.3
Программа кибербезопасности и киберустойчивости судна	Управление антивредоносной защитой	См. 2.2.2.3.3.4

Контроль доступа (см. 2.2.2.4)		
Функциональные возможности обеспечения безопасности КС	Идентификация и аутентификация пользователя – физического лица	См. п. 1 табл. 3.3.1
	Управление учетными записями	См. п. 2 табл. 3.3.1
	Управление идентификаторами	См. п. 3 табл. 3.3.1
	Управление аутентификаторами	См. п. 4 табл. 3.3.1
	Контроль выполнения авторизаций	См. п. 8 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.2.4.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.2.4.3.3
Программа кибербезопасности и киберустойчивости судна	Управление конфиденциальной информацией	См. 2.2.2.4.3.4
	управления логическим и физическим доступом	См. 2.2.2.4.3.4

Беспроводная связь (см. 2.2.2.5)		
Функциональные возможности обеспечения безопасности КС	Управление беспроводным доступом	См. п. 5 табл. 3.3.1
	Контроль беспроводного использования	См. п. 9 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.2.5.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.2.5.3.3
Программа кибербезопасности и киберустойчивости судна		

Управление удаленным доступом и связь с ненадежными сетями (см. 2.2.2.6)		
Функциональные возможности обеспечения безопасности КС	Многофакторная аутентификация	См. п. 31 табл. 3.3.2
	Идентификация и аутентификация процессов и устройств	См. п. 32 табл. 3.3.2
	Неудачные попытки входа в систему	См. п. 33 табл. 3.3.2
	Уведомление об использовании системы	См. п. 34 табл. 3.3.2
	Доступ через ненадежные сети	См. п. 35 табл. 3.3.2
	Принятие явного запроса на доступ	См. п. 36 табл. 3.3.2
	Завершение удаленного сеанса	См. п. 37 табл. 3.3.2
	Защита целостности средствами криптографии	См. п. 38 табл. 3.3.2
	Валидация входных данных	См. п. 39 табл. 3.3.2
	Целостность сеанса	См. п. 40 табл. 3.3.2
	Аннулирование идентификаторов сеанса после завершения сеанса	См. п. 41 табл. 3.3.2
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.2.6.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.2.6.3.3
Программа кибербезопасности и киберустойчивости судна	Управление удаленным доступом и связи с ненадежными сетями	См. 2.2.2.6.3.4

Использование носимых и переносных устройств (см. 2.2.2.7)		
Функциональные возможности обеспечения безопасности КС	Контроль использования носимых и переносных устройств	См. п. 10 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.2.7.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.2.7.3.3
Программа кибербезопасности и киберустойчивости судна	Управление носимыми и переносными устройствами	См. 2.2.2.7.3.4

Мониторинг работы сети (см. 2.2.3.1)		
Функциональные возможности обеспечения безопасности КС	Контроль использования носимых и переносных устройств	См. п. 10 табл. 3.3.1
	События, подлежащие аудиту	См. п. 13 табл. 3.3.1
	Защита от отказа в обслуживании	См. п. 24 табл. 3.3.1
	Срабатывание сигнала тревоги при достижении порога использования сети	См. 7.9.8.2.1.5 части XV «Автоматизация»
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
Документация проекта судна	Программа испытаний киберустойчивости судна	См. 2.2.3.1.3.3
Программа кибербезопасности и киберустойчивости судна	План действий в случае киберинцидента	См. 2.2.3.1.3.4

Функции проверки и диагностики КС и сетей (см. 2.2.3.2)		
Функциональные возможности обеспечения безопасности КС	Верификация функций безопасности	См. п. 19 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Планы технического обслуживания и верификации КС	См. 3.2.1.7
Документация проекта судна	Программа испытаний киберустойчивости судна	См. 2.2.3.2.3.3
Программа кибербезопасности и киберустойчивости судна	Проверка правильности работы функций безопасности	См. 2.2.3.2.3.4

План действий в случае киберинцидента (см. 2.2.4.1)		
Функциональные возможности обеспечения безопасности КС		
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Информация для поддержки планов реагирования и восстановления в случае киберинцидента	См. 3.2.1.8
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.4.1.3.1
Программа кибербезопасности и киберустойчивости судна	План действий в случае киберинцидента	См. 2.2.4.1.3.4

Местное, независимое и/или ручное управление (см. 2.2.4.2)		
Функциональные возможности обеспечения безопасности КС		
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Информация для поддержки планов реагирования и восстановления в случае киберинцидента	См. 3.2.1.8
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.4.2.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.4.2.3.3
Программа кибербезопасности и киберустойчивости судна	План действий в случае киберинцидента	См. 2.2.4.1.3.4

Изоляция сети (см. 2.2.4.3)		
Функциональные возможности обеспечения безопасности КС		
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Информация для поддержки планов реагирования и восстановления в случае киберинцидента	См. 3.2.1.8
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.4.3.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.4.3.3.3
Программа кибербезопасности и киберустойчивости судна	План действий в случае киберинцидента	См. 2.2.4.1.3.4

Возврат к состоянию минимального риска (см. 2.2.4.4)		
Функциональные возможности обеспечения безопасности КС	Детерминированный поток выходных сигналов	См. п. 20 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Информация для поддержки планов реагирования и восстановления в случае киберинцидента	См. 3.2.1.8
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.4.4.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.4.4.3.3
Программа кибербезопасности и киберустойчивости судна	План действий в случае киберинцидента	См. 2.2.4.1.3.4

План восстановления (см. 2.2.5.1)		
Функциональные возможности обеспечения безопасности КС		
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Информация для поддержки планов реагирования и восстановления в случае киберинцидента	См. 3.2.1.8
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.5.1.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.5.1.3.3
Программа кибербезопасности и киберустойчивости судна	Планы восстановления	См. 2.2.5.1.3.4

Резервное копирование и восстановление (см. 2.2.5.2)		
Функциональные возможности обеспечения безопасности КС	Резервирование системы	См. п. 26 табл. 3.3.1
	Восстановление системы	См. п. 27 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Информация для поддержки планов реагирования и восстановления в случае киберинцидента	См. 3.2.1.8
Документация проекта судна	Программа испытаний киберустойчивости судна	См. 2.2.5.2.3.3
Программа кибербезопасности и киберустойчивости судна	Планы восстановления	См. 2.2.5.1.3.4

Контролируемое отключение, сброс, откат и повторный запуск (см. 2.2.5.3)		
Функциональные возможности обеспечения безопасности КС	Восстановление системы	См. п. 27 табл. 3.3.1
Документация КС	Описание функциональных возможностей обеспечения безопасности	См. 3.2.1.3
	Программа испытаний функциональных возможностей обеспечения безопасности	См. 3.2.1.4
	Информация для поддержки планов реагирования и восстановления в случае киберинцидента	См. 3.2.1.8
Документация проекта судна	Описание мер обеспечения кибербезопасности	См. 2.2.5.3.3.1
	Программа испытаний киберустойчивости судна	См. 2.2.5.3.3.3
Программа кибербезопасности и киберустойчивости судна	Планы восстановления	См. 2.2.5.1.3.4

Оценка риска для исключения КС от применения требований (см. 2.4)		
Функциональные возможности обеспечения безопасности КС		
Документация КС		
Документация проекта судна	Оценка риска для исключения КС от применения требований	См. 2.3.1.4
Программа кибербезопасности и киберустойчивости судна		

ПРИЛОЖЕНИЕ 3

КРАТКИЕ СВЕДЕНИЯ О ДОКУМЕНТАХ, КОТОРЫЕ ПОСТАВЩИК ДОЛЖЕН ПРЕДСТАВИТЬ РЕГИСТРУ

Документ	Требования	Регистр
Ведомость КС (см. 3.2.1.1)	Подлежит включению в Ведомость судовых КС (см. 2.2.1.1)	Одобрение[1, 2]
Топологические схемы (см. 3.2.1.2)	Позволяет системному интегратору проектировать зоны безопасности и каналы связи (см. 2.2.2.1)	Одобрение[1, 2]
Описание функциональных возможностей обеспечения безопасности (см. 3.2.1.3)	Требуемые функциональные возможности обеспечения безопасности (см. 3.3.1)	Одобрение[1]
	Дополнительные функциональные возможности обеспечения безопасности, если применимо (см. 3.3.2)	
Программа испытаний функциональных возможностей обеспечения безопасности (см. 3.2.1.4)	Требуемые функциональные возможности обеспечения безопасности (см. 3.3.1)	Одобрение[1]
	Дополнительные функциональные возможности обеспечения безопасности, если применимо (см. 3.3.2)	
Руководство по конфигурации безопасности (см. 3.2.1.5)	Параметры конфигурации сети и безопасности (см. п. 29 табл. 3.3.1)	Для информации[1]
Описание жизненного цикла безопасной разработки (см. 3.2.1.6)	Требования к безопасному проектированию изделий и жизненному циклу разработки (см. 3.4)	Одобрение[1]
Планы технического обслуживания и верификации (см. 3.2.1.7)	Проверка функциональных возможностей обеспечения безопасности (см. п.19 табл. 3.3.1)	Для информации[1]
Информация, содержащая планы реагирования на инцидент и восстановление (см. 3.2.1.8)	События, подлежащие аудиту (см. п. 13 табл. 3.3.1)	Для информации[1]
	Детерминированный поток выходных сигналов (см. п. 20 табл. 3.3.1)	Для информации [1]
	Резервирование системы (см. п. 26 табл. 3.3.1)	Для информации[1]
	Восстановление системы (см. п. 27 табл. 3.3.1)	Для информации[1]
Управление планом изменений (см. 3.2.1.9)	Управление процессом изменений (см. 7.9.7 части XV «Автоматизация»)	Для информации[1]
Протоколы испытаний (см. 3.2.1.10)	Конфигурация функциональных возможностей обеспечения безопасности и усиление (см. 3.2.1.5 и 3.4.7)	Для информации[2]

[1] Требуется для КС, не имеющих СТО, подтверждающего соответствие функций безопасности требованиям разд. 3.

[2] Требуется для КС, имеющих СТО, подтверждающее соответствие функций безопасности требованиям разд. 3.

Российский морской регистр судоходства

Правила классификации и постройки морских судов
Часть XXI
Киберустойчивость

ФАУ «Российский морской регистр судоходства»
191181, г. Санкт-Петербург, ул. Миллионная, д. 7, литера А
www.rs-class.org/ru/