РОССИЙСКИЙ МОРСКОЙ РЕГИСТР СУДОХОДСТВА

РУКОВОДСТВО

ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

НД № 2-030101-040

Санкт-Петербург
2021

РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Руководство по обеспечению кибербезопасности Российского морского регистра судоходства утверждено в соответствии с действующим положением и вступает в силу 1 января 2021 года.

Настоящее издание Руководства разработано на основании Рекомендации МАКО № 166 (*Recommendation on Cyber Resilience*).

Руководство издается на русском и английском языках в электронном виде.

ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ

(изменения сугубо редакционного характера в Перечень не включаются)

Изменений нет

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 ОБЛАСТЬ РАСПРОСТРАНЕНИЯ

1.1.1 Руководство по обеспечению кибербезопасности[1] содержит рекомендации по проектированию, изготовлению, обслуживанию и проведению испытаний судовых компьютеризированных систем, а также рекомендации, применимые к системам управления безопасностью (СУБ).

1.1.2 Рекомендации Руководства направлены на реализацию положений резолюции ИМО MSC.428(98) «Управление киберрисками в морской отрасли в рамках систем управления безопасностью», в соответствии с которыми, не позднее чем во время первой ежегодной проверки Документа о соответствии компании (ДСК) после 1 января 2021 года необходимо учитывать киберриски в СУБ согласно положениям циркуляра ИМО MSC-FAL.1/Circ.3 «Руководство по управлению киберрисками в морской отрасли» (*Guidelines on maritime cyber risk management*).

1.1.3 Руководство применяется к судам, контракт на постройку которых заключен 01.01.2021 или после этой даты, если не указано иное в отдельных положениях Руководства.

1.1.4 Руководство является дополнением к другим требованиям Российского морского регистра судоходства (РС), применимым в соответствии с символом класса и назначением судна.

---

[1] В дальнейшем – Руководство.

1.2 ОПРЕДЕЛЕНИЯ И ПОЯСНЕНИЯ

1.2.1 Определения и пояснения, относящиеся к общей терминологии правил и руководств РС, приведены в 1.1 части I «Классификация» Правил классификации и постройки морских судов[1] и 1.1 части I «Общие положения по техническому наблюдению» Правил технического наблюдения за постройкой судов и изготовлением материалов и изделий для судов[2].

1.2.2 Основные термины, определения и сокращения.

Анализ видов и последствий отказов (*Failure Mode and Effects Analysis* (*FMEA*)) – методика определения возможных причин независимых отказов вместе с их влиянием на оборудование, программное обеспечение (ПО) или процесс на основе систематической разбивки на элементы. Методика может быть использована для демонстрации того, что предполагаемые риски определены и учтены.

Виртуальная защищенная сеть (*Virtual Private Network* (*VPN*) – безопасная, защищенная сеть, которая позволяет пользователям отправлять и получать данные через совместно используемые или общедоступные сети, как если бы их вычислительные устройства были напрямую подключены к защищенной сети, тем самым получая выгоду от функциональности, безопасности и политики управления защищенной сетью.

Виртуальная локальная вычислительная сеть (*Virtual Local Area Network* (*VLAN*)) – логическое объединение сетевых узлов. Виртуальная локальная вычислительная сеть позволяет территориально распределенным узлам сети обмениваться данными, как если бы они находились в одной сети.

Вирус (*Virus*) – скрытая, самовоспроизводящаяся часть ПО, которая злонамеренно заражает компьютерную программу или систему и управляет ее работой.

Восстановление (*Recovery*) – функция поддержки резервного копирования данных и восстановления судовых компьютеризированных систем для своевременного восстановления безопасного состояния судна.

Вредоносное программное обеспечение (*Malware*) – общий термин для обозначения различного вредоносного ПО, которое может неблагоприятно влиять на производительность компьютерных систем.

Встроенное программное обеспечение (*Firmware*) – ПО, встроенное в электронное устройство, обеспечивающее контроль, мониторинг и управление данными спроектированных изделий и систем. Обычно является энергонезависимым и недоступным для изменения пользователем.

Демилитаризованная зона (*Demilitarized zone* (*DMZ*)) – физический или логический сегмент сети, содержащий и предоставляющий общедоступные сервисы, а также отделяющий их от остальных элементов локальной вычислительной сети. Общая ограниченная сеть серверов, соединяющих две или более сетевые зоны с целью управления потоком данных между сетевыми зонами. Демилитаризованные зоны обычно используются, чтобы избежать прямых связей между различными сетевыми зонами.

Защита вглубь (*Defense in depth*) включает в себя три контролируемые части:

физическую, к которой относятся все меры по ограничению физического доступа к компьютеризированным системам неавторизованных лиц;

техническую, к которой относятся все аппаратные и программные средства защиты информации, предназначенные для контроля сетевого доступа к элементам

[1] В дальнейшем – Правила РС/К.

[2] В дальнейшем – Правила РС/ТН.

компьютеризированных систем, межсетевые экраны, средства антивирусной защиты, системы аутентификации и авторизации;

административную, к которой относятся политика и процедуры информационной безопасности, принятые в компании. Данные документы призваны регулировать управление защитой, распределение и обработку критичной информации, использование программных и технических средств в компании, а также взаимодействие экипажа с судовыми компьютеризированными системами и другими внешними объектами.

Защита вширь (*Defense in breadth*) – запланированный, систематический набор действий, направленных на выявление, управление и уменьшение уязвимостей в *IT*- и *OT*-системах, сетях и оборудовании на каждом этапе жизненного цикла системы, сети или элемента. На судах этот подход, как правило, сосредоточен на проектировании сети, системной интеграции, эксплуатации и обслуживании. Идея такого подхода заключается в защите системы от конкретного типа атаки с использованием нескольких независимых методов.

Изготовитель (*Producer*) – предприятие, которое производит судовое оборудование и соответствующее ПО.

Имитационное испытание (*Simulation test*) – испытание системы, при котором контролируемое оборудование частично или полностью заменяется инструментами моделирования или при котором части коммуникационной сети и линий заменяются инструментами моделирования.

Интегрированная система (*Integrated system*) – взаимосвязанная система, объединяющая несколько взаимодействующих судовых устройств, организованных для достижения одной или нескольких определенных целей.

Информационная технология (*Information technology* (*IT*)) – устройства, ПО и связанные с ними сети, ориентированные на использование данных в качестве информации, в отличие от эксплуатационной технологии (*Operational technology* (*OT*)).

Исправления (*Patches*) – ПО, предназначенное для обновления установленного ПО или поддержки данных для устранения уязвимостей в системе безопасности и других ошибок или улучшения компьютеризированных систем или приложений.

Категории обслуживания компьютеризированных систем (*Categories of maintenance*) – категории, присваиваемые операциям по обслуживанию компьютеризированных систем с учетом причин их выполнения, могут быть следующими:

исправление ошибок в ПО (*Bug fix*);

внесение дополнительных функций (*Feature release*);

поддержание ПО в соответствии с требованиями (*Compliance update*);

защита против киберугроз (*Security update*);

обновление устаревшего (неподдерживаемого) ПО и/или аппаратных средств (*Obsolescence update*);

различные комбинации указанных выше категорий.

Категории систем (I, II, III) (*System categories* (*I*, *II*, *III*)) – категории на основе влияния систем на возникновение опасных ситуаций для безопасности людей и судна, и/или угрозы для окружающей среды:

категория I – системы, отказ которых не приведет к возникновению опасных ситуаций для безопасности людей и судна, и/или угрозы для окружающей среды. К системам категории I относятся системы, обеспечивающие выполнение административных задач (учет расхода топлива, организация технического обслуживания и т.д.);

категория II – системы, отказ которых может, в конечном итоге, привести к возникновению опасных ситуаций для безопасности людей и судна, и/или угрозы для окружающей среды.

К системам категории II относятся:

системы аварийно-предупредительной сигнализации (согласно 1.2.1 части XV «Автоматизация» Правил РС/К),

системы индикации (согласно 1.2.1 части XV «Автоматизация» Правил РС/К;

системы внутренней связи;

системы управления грузовыми и балластными операциями;

система управления системой инертных газов;

система управления бункеровочными операциями;

категория III – системы, отказ которых может незамедлительно привести к возникновению опасных ситуаций для безопасности людей и судна, и/или угрозы для окружающей среды.

К системам категории III относятся:

системы главных и вспомогательных механизмов (согласно 1.2.1 части VII «Механические установки» Правил РС/К);

системы защиты (согласно 1.2.1 части XV «Автоматизация» Правил РС/К);

системы динамического позиционирования.

Качество данных (*Data quality*) – характеристика, показывающая степень пригодности к использованию данных, сгенерированных, обработанных, переданных и сохраненных при работе судовых компьютеризированных систем. Качество данных характеризуется следующими параметрами:

конфиденциальность (*Confidentiality*) – защита от потери конфиденциальности из-за неожиданного или несанкционированного раскрытия информации;

целостность (*Integrity*) – защита от потери целостности из-за неожиданного или несанкционированного изменения информации;

доступность (*Availability*) – защита от потери доступности из-за неожиданного или несанкционированного уничтожения информации или нарушения доступа, или использования *IT*-системы.

Качество обслуживания (*Quality of service* (*QoS*)) – измеримые сквозные характеристики производительности сетевого сервиса:

полоса пропускания (*Bandwidth*), которая описывает номинальную пропускную способность среды передачи информации (определяет ширину канала);

задержка при передаче пакета (*Delay*);

колебание задержки при передаче пакетов (*Jitter*);

потеря пакетов (*Packet loss*), которая определяет количество пакетов, теряемых сетью во время передачи.

Кибератака (*Cyber attack*) – любой вид вмешательства в *IT*- и *OT*-системы, компьютерные сети и/или персональные компьютеры с попыткой взломать, уничтожить или получить доступ к системам компании, судовым системам и данным.

Кибербезопасность (*Cyber safety*) – меры безопасности, применяемые для защиты от уязвимостей, возникающих в результате ненадлежащей эксплуатации, интеграции, обслуживания и проектирования компьютеризированных систем, и от преднамеренных и непреднамеренных киберугроз.

Киберинцидент (*Cyber incident*) – событие, которое фактически или потенциально приводит к неблагоприятным последствиям для судовой системы, сети и устройств или информации, которую они обрабатывают, хранят или передают, и которое может потребовать ответных действий для уменьшения последствий.

Киберустойчивость (*Cyber resilience*) – способность сокращать случаи возникновения и уменьшать последствия инцидентов, возникающих в результате нарушения или ухудшения эксплуатационной технологии, используемой для безопасной эксплуатации судна, которые потенциально могут привести

к возникновению опасных ситуаций для безопасности людей и судна, и/или угрозы для окружающей среды.

Компания – собственник судна или любая другая организация или лицо, например, управляющий или фрахтователь по бербоут-чартеру, который принял на себя ответственность за эксплуатацию судна от собственника судна и который при этом согласился принять на себя все обязанности и всю ответственность, возложенные Международным кодексом по управлению безопасной эксплуатацией судов и предотвращением загрязнения (МКУБ).

Компьютеризированная система (*Computer based system*) – сочетание взаимодействующих программируемых устройств и/или *IT*-систем, организованных для достижения одной или нескольких определенных целей. Компьютеризированная система может быть сочетанием подсистем, соединенных сетью. Судовая компьютеризированная система может быть подключена напрямую или через общедоступные средства связи (например, сеть Интернет) к береговым компьютеризированным системам, к компьютеризированным системам других судов и/или других объектов.

Критическая система (*Critical system*) – техническая система, внезапный отказ которой может привести к опасной ситуации.

Локальная вычислительная сеть (*Local Area Network* (*LAN*)) – компьютерная сеть, которая объединяет компьютеры и/или программируемые устройства в пределах ограниченной области, такой как здание, судно или офис, с применением сетевых устройств.

Локальное управление (*Local control*) – управление с места, расположенного в непосредственной близости от объекта управления.

Межсетевой экран (*Firewall*) – вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности.

Неуправляемая сеть (*Unmanaged Network*) – сеть, которая использует неуправляемые коммутаторы, что позволяет устройствам, подключенным к сети, обмениваться данными друг с другом. Это коммутаторы типа "*plug-and-play*", которые не требуют настройки или конфигурации и не допускают какого-либо вмешательства пользователя.

Оценка рисков (*Risk assessment*) – процесс сбора информации и присвоения значений рискам в качестве основания для принятия решения о приоритетах и разработки или сравнения планов действий.

Ошибка в программном обеспечении (*Bug*) – непреднамеренная функциональность в ПО.

План действий в непредвиденных обстоятельствах (*Contingency Plan*) – план, содержащий информацию и устанавливающий порядок действий для обеспечения эффективного реагирования и восстановления в случае киберинцидента, затрагивающего компьютеризированную систему, выполняющую ответственные функции.

Поверхность атаки (*Attack surface*) – компьютеризированные системы, к которым можно получить доступ извне либо через сеть, либо локально. Термин обозначает общее количество возможных уязвимых мест. Чем больше элементов компьютеризированных систем, тем больше число потенциально уязвимых мест и, соответственно, поверхность атаки.

Поставщик данных (*Data provider*) – лицо или компания, предоставляющее данные, необходимые для функционирования судовой компьютеризированной системы.

Поставщик услуг (*Service provider*) – компания или лицо, которое предоставляет ПО и выполняет его техническое обслуживание.

Программируемое устройство (*Programmable device*) – физическое устройство с установленным ПО.

Протоколы (*Protocols*) – общий набор правил и сигналов, которые компьютеры и программируемые устройства используют для связи.

Сетевой коммутатор (коммутатор) (*Network switch* (*Switch*)) – устройство, которое соединяет элементы в компьютерной сети, используя пакетную коммутацию для приема, обработки и пересылки данных на устройство назначения.

Сетевой концентратор (*Network hub*) – общая точка подключения для устройств в сети.

Сетевой маршрутизатор (*Network router*) – сетевое устройство, отвечающее за маршрутизацию трафика из одной сети в другую.

Сеть (*Network*) – группа из двух и более компьютерных систем, связанных друг с другом.

Система обнаружения вторжения (*Intrusion Detection System* (*IDS*)) – устройство или ПО, которое отслеживает сетевую или системную активность для обнаружения вредоносных действий или нарушений политики и выдает отчеты на станцию управления.

Система предотвращения вторжения (*Intrusion Prevention System* (*IPS*)) – устройство или ПО, которое отслеживает сетевую или системную активность для предотвращения вредоносных действий или нарушений политики.

Системный интегратор (*System integrator*) – сторона, осуществляющая интеграцию компьютеризированных систем, подсистем и ПО, предоставленных поставщиками, в систему, а также создание интегрированной системы. На системного интегратора также могут быть возложены обязанности по установке и интеграции системы на судне.

Функции системного интегратора выполняются строителем/судостроительной верфью. Обязанности системного интегратора могут быть возложены на другую организацию, при условии наличия соответствующего контракта.

При интеграции систем с привлечением нескольких сторон на любом этапе лишь одна сторона может являться системным интегратором и осуществлять координацию всех необходимых работ. При многоэтапной интеграции различные системные интеграторы могут нести ответственность за конкретные этапы, однако только одна сторона осуществляет определение этапов и общую координацию.

Системы ответственного назначения (*Essential systems*) – системы, обеспечивающие безопасную эксплуатацию судна.

Сценарий тестирования (*Test case*) – набор условий, методов и ожидаемых результатов, при которых лицо, проводящее испытания, будет определять, работает ли ПО в соответствии с проектными спецификациями или нет.

Съемные носители информации (*Removable media*) – общий термин для различных способов хранения и передачи данных между компьютерами без помощи сети. К съемным носителям информации относятся ноутбуки, *USB*-накопители, *CD*, *DVD*, дискеты и т.д.

Технология *QoS* – технология приоритизации трафика, т.е. предоставление различным классам трафика различных приоритетов в обслуживании и передаче по сети.

Управление доступом (*Access control*) – выборочное ограничение возможностей связей или иного взаимодействия с системой для использования системных ресурсов обработки информации, получения информации, содержащейся в системе, или для управления элементами и функциями системы.

Управление информацией о безопасности и событиях (*Security Information Event Monitoring* (*SIEM*)) – ПО, которое выполняет сбор и анализ данных о безопасности от различных элементов *IT*- и *OT*-систем и представляет эти данные в виде соответствующей информации через единый интерфейс.

Управление киберрисками (*Cyber risk management*) – процесс выявления, анализа, оценки и сообщения о киберриске, а также принятия, предотвращения, передачи или снижения его до приемлемого уровня с учетом затрат и выгод от любых предпринятых действий.

Управление рисками (*Risk management*) – процесс выявления, анализа, оценки и сообщения о риске, а также принятия, предотвращения, передачи или контроля риска до приемлемого уровня с учетом связанных с ними затрат и выгод от любых предпринятых действий.

Управляемая сеть (*Managed Network*) – сеть, в которой используются управляемые коммутаторы и которая позволяет подключенным сетевым устройствам взаимодействовать друг с другом, а также дает администратору сети больший контроль над управлением и установлением приоритетов сетевого трафика. Сетевой трафик можно контролировать и приоритизировать посредством изменений конфигурации.

Эксплуатационная технология (*Operational technology* (*OT*)) – устройства, датчики, ПО и связанные с ними сети, которые контролируют и управляют судовыми системами.

DLP (*Data loss prevention*) – предотвращение потери или кражи данных.

HMI (*Human machine interface*) – человеко-машинный интерфейс.

IT-система (*IT system*) – компьютеризированная система категории I, которая обеспечивает функции контроля для информационных/административных задач.

MAC-адрес (от англ. *Media access control* (*MAC*) – Контроль доступа к среде) – уникальный аппаратный адрес, который отличает одно устройство в сети от другого.

M2M (*Machine to machine interface*) – межмашинный интерфейс.

OT-система (*OT system*) – компьютеризированная система категории II или III, которая обеспечивает функции управления, сигнализации, контроля, безопасности или внутренней связи.

RAID (*Redundant array of independent disks*) – массив независимых дисков с избыточностью.

Wi-Fi – технология беспроводной передачи данных ближнего радиуса действия, которая использует какой-либо тип электромагнитного спектра для отправки и/или получения информации.

2 ТЕХНИЧЕСКАЯ ДОКУМЕНТАЦИЯ

2.1 ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

2.1.1 Техническая документация для систем категорий I (при наличии связей с системами категорий II или III), II и III, которая должна быть разработана на этапе проектирования и строительства судна и представлена в Регистр для рассмотрения, указана в табл. 2.1.1.

Таблица 2.1.1

№ п/п	Наименование	Описание	Примечание
1	Концепция компьютеризированной системы	Документ должен содержать следующую информацию: .1 назначение компьютеризированной системы с кратким описанием функций; .2 структурную схему (план), четко идентифицирующую(ий) судовые системы, управляемые/контролируемые компьютеризированной системой. На схеме (плане) также должна быть отражена следующая информация: связи с внешней сетью для контроля, управления и выполнения административных функций; связи с другими компьютеризированными системами	Представляется в Регистр для информации
2	Описание сетей передачи данных	Документ должен отражать следующую информацию: .1 физическое расположение элементов систем и подсистем (например, наименования помещения, палубы расположения и т.д.); .2 связи системы категории I с системами категорий II или III; .3 сетевую топологию систем и подсистем (звезда, кольцо и т.д.); .4 применяемые сетевые технологии (например, *Gigabit Ethernet*, *Fast Ethernet*); .5 применяемые кабели передачи данных (витая пара, оптический кабель и т.д.); .6 связи контроллеров и полевых устройств (*MODBUS*, *Fieldbus* и т.д.); .7 сетевые схемы с указанием устройств, узлов, данных о применяемых кабелях и общего расположения оборудования; .8 перечень *IT*- и *OT*-систем с указанием их категорий; .9 потоки данных и сетевые устройства или ресурсы, потенциально их ограничивающие; .10 внешние подключения для удаленного доступа; .11 точки доступа и интерфейсы, включая межмашинные (*M2M*) интерфейсы; .12 логические схемы судовых сетей	Представляется в Регистр для информации

2.2 ДОКУМЕНТАЦИЯ НА БОРТУ СУДНА

2.2.1 Документация, которая должна находиться на борту судна, представлена в табл. 2.2.1.

Таблица 2.2.1

№ п/п	Наименование	Описание	Примечание
1	Описание сетей передачи данных	Документ должен содержать следующую информацию: .1 физическое расположение элементов систем и подсистем (например, наименования помещения, палубы расположения и т.д.); .2 связи системы категории I с системами категорий II или III; .3 сетевую топологию систем и подсистем (звезда, кольцо и т.д.); .4 применяемые сетевые технологии (например, *Gigabit Ethernet*, *Fast Ethernet*); .5 применяемые кабели передачи данных (витая пара, оптический кабель и т.д.); .6 связи контроллеров и полевых устройств (*MODBUS*, *Fieldbus* и т.д.); .7 сетевые схемы с указанием устройств, узлов, данных о применяемых кабелях и общего расположения оборудования; .8 перечень *IT*- и *OT*-систем с указанием их категорий; .9 потоки данных и сетевые устройства или ресурсы, потенциально их ограничивающие; .10 внешние подключения для удаленного доступа; .11 точки доступа и интерфейсы, включая межмашинные (*M2M*) интерфейсы; .12 логические схемы бортовых сетей	
2	Опись элементов компьютеризированных систем категорий II и III	Для устройств, имеющих интерфейсные связи с компьютеризированными системами (например, для программируемых логических контроллеров, удаленных модулей ввода/вывода, станций человеко-машинного (*HMI*) интерфейса, датчиков, частотных преобразователей, автоматических выключателей,	Применяется к судам, контракт на постройку которых заключен 01.01.2021 или после этой даты, и существующим судам после 01.01.2022. Для существующих судов опись составляется компанией. Для судов, контракт

№ п/п	Наименование	Описание	Примечание
		физических серверов, компьютеров, рабочих станций, устройств хранения данных и т.д.), и сетевых коммуникационных устройств (например, для коммутаторов, маршрутизаторов, межсетевых экранов, преобразователей интерфейсов и т.д.) должны быть указано следующее (для каждого устройства): .1 наименование; .2 марка/производитель (поставщик); .3 модель; .4 версия операционной системы или встроенной программы (*Firmware*) и версия установленного ПО; .5 описание настроек, если применимо; .6 информация о расположении оборудования (например, жилое помещение/машинное отделение)	на постройку которых заключен 01.01.2021 или после этой даты, опись должна быть составлена системным интегратором до момента передачи судна. В период эксплуатации судна, непосредственно после внесения изменений в компьютеризированные системы (обновление ПО, замена оборудования, за исключением случаев замены на аналогичное оборудование без изменения ПО), ответственным персоналом на судне должны быть внесены соответствующие изменения в опись с указанием даты и причины внесения изменений, а также информация об исполнителе работ по внесению изменений
3	Опись компьютеризированных систем категорий II и III (логический уровень)	Документ должен содержать следующую информацию: .1 диапазон используемых *IP*-адресов с указанием: перечня сетевых устройств (с указанием *IP*-адреса), использующих *IP*-адреса в данном диапазоне; функционального описания диапазона *IP*-адресов; взаимосвязи с другими диапазонами; .2 для устройств без *IP*-адресов: перечень устройств с указанием *MAC*-адресов или адресов, специфичных для промышленных протоколов в сети; функционального описания сети; .3 точки подключения к сети с указанием: перечня портов доступа; адресации, если есть специальный протокол;	Применяется к судам, контракт на постройку которых заключен 01.01.2021 или после этой даты. Опись должна быть составлена системным интегратором до момента передачи судна. В период эксплуатации судна, непосредственно после внесения изменений в компьютеризированные системы (обновление ПО, замена оборудования, за исключением случаев замены на аналогичное оборудование без изменения ПО), ответственным

№ п/п	Наименование	Описание	Примечание
		перечня подключенных устройств; .4 логические серверы и компьютеры с указанием, если применимо: *IP*-адресации (сети, маски подсети, шлюзов); версии операционной системы; основного физического сервера; приложений и их версий; .5 соединения полевых устройств (удаленные модули ввода/вывода, интеллектуальные датчики и т.д.) с указанием: *IP*-адресации (сети, маски подсети, шлюза), связанного *MAC*-адреса и сети или адреса, специфичных для промышленных протоколов в сети, если необходимо	персоналом на судне должны быть внесены соответствующие изменения в опись с указанием даты и причины внесения изменений, а также информация об исполнителе работ по внесению изменений
4	Опись ПО компьютеризированных систем категорий II и III	Документ должен содержать следующую информацию: .1 наименование ПО; .2 наименование разработчика ПО; .3 дату установки и номер версии ПО; .4 способ обслуживания ПО (локальный/ удаленный); .5 вид учетной записи (общий/специальный); .6 матрицу доступа с указанием прав на чтение, запись или управление; .7 номер лицензии, если применимо; .8 вид и дату проведенного обслуживания ПО; .9 информацию о компании с указанием данных исполнителя, выполнившей обслуживание ПО	Применяется к судам, контракт на постройку которых заключен 01.01.2021 или после этой даты. Опись должна быть составлена системным интегратором до момента передачи судна. В период эксплуатации судна, непосредственно после внесения изменений в компьютеризированные системы (обновление ПО, замена оборудования, за исключением случаев замены на аналогичное оборудование без изменения ПО), ответственным персоналом на судне должны быть внесены соответствующие изменения в опись с указанием даты и причины внесения изменений, а также информация об исполнителе работ по внесению изменений
5	Оценка рисков	Согласно разд. 3	

№ п/п	Наименование	Описание	Примечание
6	Инструкция по обеспечению кибербезопасности на судне	Документ должен содержать следующую информацию: описание мер по предотвращению возникновения киберинцидентов; План действий в непредвиденных обстоятельствах (*Contingency Plan*); процедуры организации процесса обслуживания ПО	Применяется к судам, контракт на постройку которых заключен 01.01.2021 или после этой даты, и существующим судам после 01.01.2022. Документ разрабатывается компанией на основании оценки рисков и рекомендаций производителей оборудования
7	Перечень поставщиков услуг	Документ должен содержать следующую информацию: перечень оборудования с указанием наименования ПО, обслуживаемого поставщиком услуг; наименование организации, имеющей разрешение на обслуживание конкретного оборудования	Требования к поставщикам услуг указаны в 4.3.2.3. Применяется к существующим судам и судам, контракт на постройку которых заключен 01.01.2021 или после этой даты. Документ разрабатывается и обновляется, при необходимости, компанией в течение всего периода эксплуатации судна
8	Описание периметра безопасности	Документ должен содержать следующую информацию: перечень помещений с указанием перечня оборудования (коммуникационного оборудования, компьютеров, контроллеров), размещенного внутри каждого помещения; описание принятых мер по ограничению доступа	Применяется к судам, контракт на постройку которых заключен 01.01.2021 или после этой даты, и существующим судам после 01.01.2022. Для существующих судов описание составляется компанией. Для судов, контракт на постройку которых заключен 01.01.2021 или после этой даты, описание должно быть составлено системным интегратором до момента передачи судна. Описание должно обновляться, при необходимости, компанией в течение всего периода эксплуатации судна

3 ОЦЕНКА РИСКОВ

3.1 ОБЩИЕ ТРЕБОВАНИЯ ПО ВЫПОЛНЕНИЮ ОЦЕНКИ РИСКОВ

3.1.1 Оценка рисков возникновения кибератак и киберинцидентов должна быть выполнена для компьютеризированных систем категорий I (при наличии связей с системами категорий II или III), II и III.

3.1.2 Для судов, контракт на постройку которых заключен 01.01.2021 или после этой даты, оценка рисков должна быть выполнена системным интегратором, для существующих судов оценка рисков должна быть выполнена компанией. Повторная оценка рисков должна быть выполнена при внесении изменений (изменение структуры системы, замена элементов на новые отличные от ранее применяемых, добавление новых функций и т.д.) в компьютеризированные системы категорий I (при наличии связей с системами категорий II или III), II и III.

3.1.3 Для судов, контракт на постройку которых заключен 01.01.2021 или после этой даты, допускается выполнять оценку рисков для головного судна при условии отсутствия существенных различий между компьютеризированными системами судов одной серии. К существенным относятся следующие различия:

по количеству взаимосвязанных компьютеризированных систем;

по выполняемым функциям компьютеризированными системами;

по составу сетевых коммуникационных устройств;

по способам обслуживания (локальное, дистанционное) компьютеризированных систем;

по наличию подключений судовых компьютеризированных систем к внешним системам, находящимся за пределами судна.

3.1.4 При выполнении оценки рисков для существующих судов допускается выполнение общей оценки рисков для судов одного проекта при отсутствии различий между компьютеризированными системами различных судов, указанных в 3.1.3.

3.1.5 При выполнении оценки рисков должны учитываться тип судна, наличие связей между различными системами и связей между судном и берегом или между судном и другим объектом.

3.1.6 Анализ рисков должен выявить непосредственное влияние на оборудование, безопасность эксплуатации судна, безопасность людей и окружающую среду. Анализ рисков должен учитывать влияние на связанные системы.

3.1.7 При наличии удаленного доступа к судовым системам оценка рисков должна учитывать угрозы, связанные с удаленным доступом.

3.1.8 Результаты оценки рисков должны быть документированы. Документ должен содержать качественную и/или количественную оценку рисков, критерии принятия риска, а также информацию о степени серьезности последствий возникновения рисков.

3.1.9 На основании проведенной оценки рисков с учетом рекомендаций изготовителей должна быть разработана Инструкция по обеспечению кибербезопасности на судне.

3.2 ТИПОВЫЕ РИСКИ

3.2.1 При проведении оценки должны учитываться риски, связанные с особенностями и условиям эксплуатации различных типов судов. Должны быть учтены, как минимум, следующие риски:

.1 получение несанкционированного доступа;

.2 отказ работоспособности систем категорий II и III в результате физического повреждения элементов системы, повреждения ПО, нарушения целостности данных, потери электропитания и т.д.;

.3 непреднамеренные действия персонала, эксплуатирующего систему;

.4 заражение программно-аппаратных средств систем категорий I (при наличии связей с системами категорий II или III), II и III.

3.3 СТАНДАРТЫ ПО ОЦЕНКЕ РИСКОВ

3.3.1 Оценка рисков, связанных с эксплуатацией судовых компьютеризированных систем, должна выполняться с применением стандартизированных методов.

3.3.2 При проведении оценки рисков должны использоваться национальные и/или международные стандарты по управлению рисками и оценке рисков, например, стандарты ИСО/МЭК 27005 и ИСО/МЭК 31010 или другие эквивалентные стандарты.

4 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

Технические требования, изложенные в настоящем разделе, направлены на обеспечение выполнения целевых и функциональных требований по обеспечению кибербезопасности на судах.

Целью Руководства с точки зрения проектирования и строительства является обеспечение киберустойчивости судна, которая должна поддерживаться на протяжении всего периода эксплуатации. Для обеспечения выполнения данной цели должны выполняться следующие целевые и функциональные требования.

Идентификация (*I*) – наличие полной информации о всех устройствах, системах, сетях и потоках данных между системами и элементами систем на борту судна для принятия мер по защите от киберинцидентов, обнаружению кибератак и киберинцидентов, принятию ответных мер при возникновении киберинцидентов и восстановлению систем, подверженных киберинцидентам.

Функциональные требования:

I1: должна быть определена информация, которой обмениваются между собой судовые *OT*-системы, а также судовые *OT*-системы с другими системами;

I2: должны быть определены взаимозависимости между критическими системами и риски, которые могут повлиять на безопасность эксплуатации судна, безопасность людей и окружающую среду, когда такие системы подвергаются риску.

Защита (*P*) – применение защитных систем и устройств для обеспечения различных способов защиты *OT*-систем и соответствующей информации.

Функциональные требования:

P1: *IT*- и *OT*-системы должны быть разработаны с обеспечением безопасных конфигурации, интеграции и обслуживания ПО;

P2: совместная работа *OT*-систем должна быть ограничена только определенными критическими функциями;

P3: сети *IT*- и *OT*-систем должны быть сегментированы и разделены на сетевые зоны;

P4: доступ (физический и логический) к *OT*-системам должен быть ограничен;

P5: должна быть сведена к минимуму возможность нарушения работы *OT*-системы, которая влияет на способность выполнения критических функций безопасности.

Обнаружение (*D*) – обеспечение своевременного и эффективного обнаружения киберинцидентов.

Функциональные требования:

D1: должны быть предусмотрены средства для мониторинга состояния работы *OT*-систем, обеспечивающие непрерывную и/или по запросу самодиагностику и диагностику качества соединения, и/или средства для контроля производительности. Указанные средства должны применяться, по крайней мере, в сетях, соединяющих *OT*-системы, и в сетях, соединяющих *IT*-системы с *OT*-системами.

Реагирование (*R*) – ограничение распространения и длительности воздействия возможного повреждения *OT*-систем и соответствующей информации.

R1: влияние киберинцидентов должно быть ограничено зоной, определенной при проведении оценки рисков.

R2: должно быть сведено к минимуму распространение возможного отказа работы *OT*-системы, которая влияет на способность выполнения критических функций безопасности.

Восстановление (*RC*) – своевременное восстановление функциональности *OT*-систем для поддержания судна в безопасном состоянии.

Функциональные требования:

RC1: оборудование должно быть спроектировано таким образом, чтобы обеспечить возможность резервного копирования и восстановление *OT*-систем с целью своевременного восстановления безопасного состояния судна.

Допускается применение технических решений, отличных от указанных в настоящем разделе, если они в полной мере обеспечивают выполнение вышеуказанных целевых и функциональных требований.

В табл. 4 представлена сводная информация с указанием конкретных пунктов Руководства, обеспечивающих выполнение функциональных требований.

Таблица 4

Обозначение функционального требования	Раздел/пункт Руководства
I1	4.1.1.1
I2	разд. 3, 4.1.1.1
P1	4.1.1
P2	4.1.5.4
P3	4.1.5.6, 4.1.5.9, 4.1.5.10
P4	4.1.5.5, 4.1.6, 4.1.7
P5	4.1.5.3, 4.1.5.4
D1	4.1.3
R1	п. 6 табл. 2.2.1
R2	п. 6 табл. 2.2.1
RC1	4.1.4, 4.3.1.6

4.1 ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ

4.1.1 Общие требования.

4.1.1.1 Системным интегратором должна быть разработана документация, указанная в табл. 2.1.1.

4.1.1.2 На этапе проектирования изготовитель компьютеризированной системы должен выполнить анализ видов и последствий отказов (*FMEA*) компьютеризированной системы. На основании выполненного анализа должны быть определены технические меры безопасности.

4.1.1.3 Должна быть обеспечена защита от несанкционированного доступа к элементам систем, функциям обмена данными и функциям, влияющим на безопасность эксплуатации судна, безопасность людей и окружающую среду.

4.1.1.4 При выборе оборудования должны учитываться условия эксплуатации, возможность механического повреждения или несанкционированного доступа в места установки элементов компьютеризированных систем. Элементы компьютеризированных систем должны располагаться в местах, соответствующих техническим характеристикам (степень защиты оболочки оборудования (IP), диапазон рабочих температур и др.) оборудования, с учетом указаний изготовителя оборудования и требований Руководства.

4.1.1.5 Компьютеризированная система должна быть спроектирована таким образом, чтобы обеспечить конфиденциальность, целостность и доступность данных, необходимых для обеспечения безопасной эксплуатации судна.

4.1.2 Защита от киберинцидентов.

4.1.2.1 На основании выполненного анализа видов и последствий отказов (*FMEA*) могут применяться следующие меры защиты сети:

.1 управление инфраструктурой открытых ключей (*PKI*) и управление учетными данными пользователей сети, включая *M2M*-сети;

.2 аутентификация (проверка подлинности) или ограничение полномочий для удаленного доступа;

.3 контроль физического доступа к точкам подключения к сети;

.4 предоставление пользователю или системе доступа к информации и ресурсам, которые минимально необходимы для успешного выполнения поставленной задачи (принцип наименьших привилегий (*Least Privilege Policy*));

.5 шифрование данных при организации удаленного доступа;

.6 контроль целостности данных;

.7 разделение *IT*- и *OT*-систем. При необходимости организации связи между *IT*- и *OT*-системами должны быть выполнены требования 4.1.5.7 и 4.1.5.9;

.8 технология *QoS*.

4.1.2.2 Где это возможно, а также с учетом требований изготовителей, антивирусное ПО должно быть установлено на компьютерах или других программируемых устройствах, использующих стандартные операционные системы. Применение антивирусного ПО не должно оказывать влияние на производительность систем категорий II и III. Для программируемых логических контроллеров или других устройств, не использующих стандартные операционные системы, должны быть приняты меры по защите от вирусов на основании рекомендаций изготовителей.

4.1.2.3 При наличии демилитаризованной зоны (*DMZ*) допускается установка антивирусного ПО только на сервере приложений (*application server*) при условии, что обслуживание ПО элементов компьютеризированных систем осуществляется через сервер приложений. При обеспечении обслуживания ПО элементов компьютеризированных систем через специально выделенный для указанных целей сервер управления исправлениями (*patch management server*), антивирусное ПО допускается устанавливать только на данном сервере.

4.1.2.4 Обновление антивирусного ПО должно осуществляться в автоматическом режиме. В случае невозможности обеспечения автоматического обновления антивирусного ПО допускается выполнять обновление в ручном режиме не реже одного раза в неделю при условии наличия доступа к сети Интернет.

4.1.3 Обнаружение киберинцидентов.

4.1.3.1 На основании проведенного анализа видов и последствий отказов (*FMEA*), а также с учетом рекомендаций производителей оборудования, должны быть предусмотрены меры обнаружения киберинцидента, с целью ограничить влияние киберинцидента в зоне его обнаружения. Могут использоваться следующие средства для обнаружения киберинцидентов:

система обнаружения вторжения (*IDS*) и система предотвращения вторжения (*IPS*);

инструменты контроля качества соединения;

система контроля производительности сети;

инструменты обнаружения вредоносного ПО;

управление информацией о безопасности и событиях (*SIEM*).

4.1.3.2 В судовых компьютеризированных системах должны применяться системы контроля, регистрации и сигнализации, которые должны обеспечивать, как минимум:

.1 контроль и сигнализацию возникновения следующих кибератак:

сетевых атак (анализ сетевого трафика);

IP-спуфинга (использования чужого *IP*-адреса источника);

атак типа *Man-in-the-Middle* (кибератак, при которых злоумышленник способен читать и видоизменять данные, которыми обмениваются корреспонденты);

атак на уровне приложений;

сетевой разведки;

переадресации портов;

получения несанкционированного доступа в сеть;

атак, использующих приложения типа «троянский конь» или сетевых червей;

.2 контроль и сигнализацию следующих неисправностей:

отсутствия подключения к сети оборудования в течение заданного времени,

отказа элементов компьютеризированных систем;

.3 контроль и регистрацию возникновения событий, связанных со следующим:

аутентификацией (проверкой подлинности) пользователей,

созданием, изменением, удалением и блокированием учетных записей пользователей,

журналом событий (выгрузкой и удалением записей, превышением размера),

выполнением настроек системы,

обновлением ПО,

резервированием и восстановлением базы данных,

запуском или перезагрузкой системы и сервисов, а также системными журналами,

нарушением правил межсетевого экранирования или правил сетевой маршрутизации,

подключением неизвестного устройства, не принадлежащего сети,

подключением/отключением оборудования к/от сети.

4.1.3.3 Системы контроля сети должны предоставлять необходимую информацию, описывающую киберинцидент, для применения пользователем. Если на судне предусмотрена возможность удаленного доступа, должна быть обеспечена возможность идентифицировать киберинцидент, связанный с получением несанкционированного доступа из внешних сетей.

4.1.4 Восстановление.

4.1.4.1 Меры по восстановлению должны быть разработаны изготовителем и/или системным интегратором. Критические системы должны иметь возможность поддерживать своевременное безопасное резервное копирование и восстановление в полном объеме.

4.1.4.2 Должны быть обеспечены следующие меры по восстановлению компьютеризированных систем, затронутых киберинцидентом:

.1 резервирование или меры восстановления данных и элементов компьютеризированной системы;

.2 контролируемое отключение, сброс или перезагрузка систем, или элементов систем, подверженных влиянию киберинцидента.

4.1.5 Сеть.

4.1.5.1 При проектировании сетей передачи данных должны использоваться стандартные интерфейсы, а также должен учитываться объем передаваемых данных и требуемая скорость обмена данными между элементами сети с целью обеспечения требуемой производительности компьютеризированных систем. Должен быть обеспечен запас пропускной способности сетей передачи данных не менее 40 % с целью обеспечения требуемой производительности компьютеризированных систем при их изменении (добавлении новых функций, добавлении новых элементов системы и т.д.) в процессе эксплуатации судна.

4.1.5.2 Должно быть обеспечено резервирование каналов передачи данных для систем категорий II и III в соответствии с требованиями, изложенными в разд. 7 части XV «Автоматизация» Правил РС/К, или на основании выполненного анализа видов и последствий отказов (*FMEA*).

4.1.5.3 Отказ в одной части судовой сети из-за сбоя сетевых устройств или киберинцидента не должен влиять на остальные системы, подключенные к поврежденной сети.

4.1.5.4 С целью обеспечения устойчивости к отказам при проектировании компьютеризированных систем должны быть выполнены следующие требования:

.1 для систем категорий II и III должна быть обеспечена надежная передача данных между системами и элементами систем. При возникновении ошибок или отказов в передаче данных должны быть выполнены самокорректирующие действия (повторная передача/запрос данных, автоматическое переключение на резервный канал передачи данных и т.д.), обеспечивающие гарантированную передачу данных;

.2 для систем ответственного назначения должна быть обеспечена возможность местного управления системами и оборудованием при отказе компьютеризированной системы;

.3 для уменьшения поверхности атаки систем категорий II и III должно быть обеспечено разделение (физическое или логическое) критических и некритических данных и процессов;

.4 должны быть приняты меры, исключающие волновой эффект, при котором могут быть заражены другие системы и подсистемы в результате одного киберинцидента;

.5 для компьютеризированных систем категорий II или III в случае отказа какого-либо сетевого оборудования или нарушения его функционирования в результате киберинцидента судовое оборудование, которое управляется указанными компьютеризированными системами, должно перейти в состояние, обеспечивающее безопасную эксплуатацию судна.

4.1.5.5 Должен быть обеспечен контроль доступа к сети, исключающий возможность подключения к сети без идентификации (распознавание пользователя) и аутентификации (проверка подлинности пользователя или данных).

4.1.5.6 Должно быть выполнено разделение сетей на основании концепции компьютеризированной системы и результатов анализа видов и последствий отказов (*FMEA*). Разделение может быть выполнено либо с использованием разных физических сетей, либо с использованием разных логических сетей. Периметр каждой зоны сети должен быть четко определен и документирован.

4.1.5.7 В случае, если разрешен доступ между различными сетевыми зонами, он должен контролироваться по периметру с использованием соответствующих устройств защиты (например, прокси-серверов, маршрутизаторов, межсетевых экранов, сетевых шлюзов, однонаправленных сетевых шлюзов, защищенных и зашифрованных туннелей). Демилитаризованная зона (*DMZ*) должна быть организована между судовой сетью и внешней сетью (береговой сетью, сетью другого судна или объекта). Межсетевые экраны должны предусматриваться между сетями систем категорий I и II и между сетями систем категорий I и III.

4.1.5.8 Сети, обеспечивающие удаленный доступ, должны контролироваться для предотвращения любых угроз безопасности со стороны подключенных устройств с использованием межсетевых экранов, маршрутизаторов и коммутаторов, удовлетворяющих требованиям стандарта МЭК 61162-460. Внешний доступ таких соединений должен быть защищен для предотвращения несанкционированного доступа.

4.1.5.9 Разделение сетей должно выполняться с учетом следующих требований:

.1 не допускается установка постоянного сетевого шлюза между общественными сетями (сети, используемые пассажирами, сети, не относящиеся к сетям *IT*- и *OT*-систем, используемые экипажем) и сетями других зон;

.2 не допускается наличие незащищенного беспроводного доступа к сети для *OT*-систем;

.3 должен быть ограничен (физический или логический) доступ к портам подключения съемных носителей информации. При наличии критичной информации в сети, рекомендуется обеспечить физические блокировки портов, чтобы предотвратить несанкционированный доступ к этим портам;

.4 не допускается обмен данными между различными зонами, за исключением обмена данными через соответствующие устройства защиты согласно 4.1.5.7.

4.1.5.10 В пределах зоны (совокупности элементов компьютеризированных систем, соответствующих общим требованиям безопасности) должна быть выполнена сегментация сети (разбиение сети на сегменты с целью оптимизации сетевого трафика и/или повышения безопасности сети в целом) в соответствии с определенным уровнем риска. Критические системы должны быть сгруппированы (включая кабели связи) внутри зон на сегменты с общими уровнями безопасности с целью управления рисками и достижения желаемого уровня безопасности для каждой зоны.

При сегментировании сети должны выполняться следующие требования:

.1 для сетей системы категории II должна быть обеспечена физическая или логическая сегментация (виртуальная локальная вычислительная сеть (*VLAN*));

.2 для сетей системы категории III должна быть обеспечена физическая сегментация с применением независимых коммутаторов;

.3 должен быть исключен отказ критических систем при единичном отказе (например, отказе оборудования, повреждении кабеля, нарушении в работе ПО) для систем категории III;

.4 при взаимосвязи между сетями, которые включают в себя системы более низкой категории и системы более высокой категории, все взаимосвязанные системы рассматриваются как системы с высшей категорией, например, если сеть, которая включает системы категории I, подключена к сети, которая включает системы категории III, обе сети следует рассматривать как категорию III;

.5 должно быть предусмотрено два сетевых устройства между сегментами критических систем. В случае если потеря связи между сегментами может привести к аварийной ситуации, оба сетевых устройства должны работать в режиме реального времени. Они должны быть расположены таким образом, чтобы в случае выхода из строя одного из устройств или киберинцидента второе устройство могло обеспечить полное функционирование системы.

4.1.5.11 При применении беспроводных каналов связи должны выполняться следующие требования:

.1 должна быть обеспечена возможность идентификации и аутентификации всех пользователей (людей, программных средств или устройств), использующих беспроводные каналы связи;

.2 должна быть обеспечена возможность авторизации (предоставление прав на выполнение определенных действий), мониторинга и обеспечения соблюдения ограничений использования беспроводного подключения к системе управления;

.3 должны использоваться механизмы шифрования для предотвращения потери целостности и конфиденциальности информации во время передачи данных.

4.1.5.12 Радиочастоты и уровни мощности судовой беспроводной сети передачи данных должны соответствовать требованиям Международного союза электросвязи (*ITU*) и требованиям Администрации.

При использовании беспроводной сети передачи данных следует учитывать требования порта и местных норм, запрещающие использование беспроводной передачи данных из-за ограничений по частоте и уровню мощности.

4.1.6 Контроль доступа к компьютеризированным системам.

4.1.6.1 Элементы компьютеризированных систем должны быть установлены таким образом, чтобы обеспечить эффективную эксплуатацию судна экипажем и различными заинтересованными сторонами, которым необходим доступ к компьютеризированным системам для обновления, технического обслуживания, ремонта, замены и т.д.

Должен быть разработан документ с описанием периметра безопасности, в котором должна содержаться следующая информация:

перечень помещений (наименование помещения, палуба расположения и т.д.) с указанием оборудования (коммуникационного оборудования, компьютеров, контроллеров), размещенного внутри каждого помещения;

описание принятых мер по ограничению доступа.

Для существующих судов описание составляется компанией. Для судов, контракт на постройку которых заключен 01.01.2021 или после этой даты, описание должно быть составлено системным интегратором до момента передачи судна.

4.1.6.2 Для предотвращения несанкционированного доступа компьютерные системы категорий II и III должны располагаться в помещениях, которые могут быть закрыты или в помещениях ограниченного доступа (например, рулевой рубке, помещениях электрооборудования, машинных помещениях). Если это невозможно, то оборудование следует размещать в запираемых шкафах или в пультах.

4.1.6.3 Должны быть обеспечены меры для ограничения физического доступа к элементам компьютеризированных систем категорий II и III, расположенных в периметре безопасности, например, замок, камера видеонаблюдения и т.д.

4.1.6.4 Подключение к сети должно быть физически или логически заблокировано, за исключением случаев подключения внешнего устройства, предназначенного для обслуживания системы или оборудования.

4.1.7 Удаленный доступ.

4.1.7.1 Требования применяются к судовым *IT*- и *OT*-системам, к которым может быть осуществлен удаленный доступ (из мест, не находящихся на борту судна).

4.1.7.2 Передача данных в судовые компьютеризированные системы категорий II и III, которые являются критическими для обеспечения безопасности навигации, управления энергетической установкой, управления грузовыми операциями и др., должна быть защищена от несанкционированного доступа, и должны быть предусмотрены необходимые меры для снижения рисков, связанных с удаленным доступом. Должна быть обеспечена возможность принудительного завершения сеанса удаленного доступа к судовой сети и переход системы в безопасное состояние. Для принудительного завершения сеанса удаленного доступа может быть использовано сетевое оборудование, поддерживающее указанные функции.

В случае киберинцидента система должна обеспечивать возможность местного управления.

4.1.7.3 Системы и оборудование должны иметь способность предотвращать перерывы в сеансах удаленного доступа, влияющие на целостность и доступность *OT*-систем или целостность данных, используемых *OT*-системами.

4.1.7.4 На судах, оборудованных средствами удаленного доступа для технического обслуживания, должны быть обеспечены следующие меры защиты:

.1 должны быть предусмотрены аппаратные или программные механизмы для управления удаленным обслуживанием;

.2 со стороны судна должна быть обеспечена возможность отмены в любое время удаленного обслуживания;

.3 начало сеанса удаленного обслуживания должно быть подтверждено ответственным персоналом, находящимся на борту судна. Пароли не должны передаваться в незашифрованном виде. Должно быть обеспечено туннелирование трафика с использованием виртуальной защищенной сети (*VPN*);

.4 должна быть обеспечена возможность настройки максимального количества попыток неудачного получения доступа, после которых учетная запись пользователя должна быть временно заблокирована;

.5 должна быть обеспечена установка времени, через которое происходит принудительное отключение канала связи, используемого для удаленного обслуживания, при отсутствии активности;

.6 система должна иметь функцию блокировки доступа для удаленного обслуживания во время нормальной эксплуатации системы. Время проведения удаленного обслуживания должно быть ограничено и должно предоставляться только в течение точно определенного периода;

.7 если удаленное соединение по какой-либо причине нарушено во время проведения обслуживания, доступ к судовой компьютеризированной системе должен быть прекращен при помощи функции автоматического выхода из системы.

4.1.8 Ручное управление.

4.1.8.1 Должно быть обеспечено резервирование систем для обеспечения управления в ручном режиме. Если системы интегрированы или связаны другими способами, что может привести к одновременному влиянию киберинцидента на несколько систем, то для реализации ручного управления в данных обстоятельствах должно быть определено следующее:

.1 системы, подверженные одновременному влиянию киберинцидента, для планирования ручного управления;

.2 возможности каскадного отказа систем.

4.1.8.2 Должны быть выполнены следующие требования при проектировании и изготовлении локальных компьютеризированных систем механических установок:

.1 локальные системы управления должны включать необходимый человеко-машинный интерфейс (*HMI*) для эффективного местного управления;

.2 локальные системы управления должны иметь надежную конструкцию, устойчивую к воздействию окружающей среды и предполагаемым условиям эксплуатации;

.3 локальные системы управления должны быть автономными и независимыми от других систем или внешних каналов связи;

.4 отказ в системах дистанционного управления не должен препятствовать локальному управлению;

.5 неиспользуемые коммуникационные порты должны быть отключены либо должен быть ограничен доступ, исключающий несанкционированное подключение к портам;

.6 должны быть обеспечены средства выбора режима местного управления, расположенные вблизи объектов управления. При активном ручном режиме управления должны игнорироваться любые сигналы от системы дистанционного управления.

4.2 ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ

4.2.1 Оборудование, используемое в системах категорий II и III, должно обеспечивать снижение риска возникновения кибератак.

4.2.2 Сетевое коммуникационное оборудование, используемое в судовых компьютеризированных системах контроля, управления, регистрации и сигнализации, должно иметь подтверждение соответствия общепромышленным стандартам, применимым к сетевому коммуникационному оборудованию (например, стандарту МЭК 62443 или эквивалентным стандартам), а также должно быть испытано в соответствии с требованиями разд. 12 части IV «Техническое наблюдение за изготовлением изделий» Правил РС/ТН.

4.2.3 Сетевое коммуникационное оборудование, используемое в судовых навигационных системах и системах радиосвязи, должно соответствовать требованиям стандарта МЭК 61162-460.

4.2.4 Сетевое коммуникационное оборудование, используемое в системах категорий II и III, должно обеспечивать путем самодиагностики контроль следующих состояний:

.1 подключение к портам (для каждого порта) сетевого устройства;

.2 отключение от портов (для каждого порта) сетевого устройства;

.3 наличие питания или перезапуск оборудования;

.4 обнаружение широковещательного шторма;

.5 неисправность вентилятора охлаждения (для устройств, использующих вентилятор для охлаждения);

.6 контроль рабочей температуры (для устройств, обеспечивающих функцию контроля рабочей температуры).

Информация о состоянии сетевого коммуникационного оборудования должна быть доступна ответственному персоналу в местах несения постоянной вахты.

4.2.5 Сетевое коммуникационное оборудование, используемое в системах категорий II и III, должно обеспечивать сигнализацию при возникновении следующих состояний неисправности:

.1 отключении линии связи или потери питания сетевого устройства;

.2 неисправности/отказе сетевого устройства.

Сигнализация должна быть обеспечена в местах несения постоянной вахты. Допускается формирование общего сигнала неисправности с обеспечением расшифровки причины срабатывания сигнализации в местах расположения сетевого оборудования.

4.2.6 Должна быть обеспечена возможность физической или логической блокировки неиспользуемых портов сетевых устройств.

4.2.7 Сетевое коммуникационное оборудование должно иметь следующие параметры конфигурации:

.1 шифрование пароля;

.2 установку пароля на порты консоли;

.3 настраиваемое время ожидания сеанса;

.4 разрешение управления потока данных;

.5 блокировку неиспользуемых портов.

4.2.8 Электронные устройства, используемые для хранения данных для систем категорий II и III, должны соответствовать назначению и соответствовать морским условиям эксплуатации. Данные, хранящиеся на таких устройствах, должны быть надлежащим образом продублированы для минимизации потери данных в случае единичного отказа устройства.

4.3 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

4.3.1 Разработка ПО.

4.3.1.1 Требования настоящей главы применяются к ПО компьютеризированных систем категорий II и III.

4.3.1.2 Разработка ПО должна осуществляться в соответствии с принятыми в компании стандартами и процедурами в отношении процессов разработки программных средств.

4.3.1.3 Разработка ПО должна осуществляться на основании технического задания, содержащего информацию о цели разработки, решаемых задачах и функциях, выполняемых разрабатываемым программным модулем.

4.3.1.4 В процессе разработки разработчик ПО должен:

.1 документировать результаты разработки;

.2 обеспечить контроль и управление изменениями ПО (версионирование ПО);

.3 документировать результаты испытаний ПО, подтверждающие выполнение целей, задач и функций в соответствии с техническим заданием на программный модуль.

4.3.1.5 Для систем категорий I, II и III должны быть предусмотрены меры безопасности, такие как процедуры авторизации и аутентификации, чтобы предотвратить несанкционированное или непреднамеренное изменение (включая конфигурацию ПО) или удаление (локальное или удаленное) ПО.

4.3.1.6 При проектировании и разработке ПО должны быть обеспечены функции резервного копирования и восстановления ПО и данных. Изготовителем должны быть разработаны процедуры по восстановлению ПО и данных.

4.3.2 Обслуживание ПО.

4.3.2.1 Обслуживание ПО включает проверку, изменение конфигурации или обновление ПО компьютеризированной системы для предотвращения или исправления ошибок, соответствия нормативным требованиям и/или повышения производительности.

4.3.2.2 Процесс обслуживания компьютеризированных систем категорий II и III в обязательном порядке должен включать в себя следующие этапы:

.1 организацию (локального или удаленного) доступа для проведения обслуживания ПО в соответствии с процедурами технического обслуживания и ремонта оборудования, разработанными компанией;

.2 сохранение предыдущей версии ПО с целью восстановления работоспособности компьютеризированной системы в случае ошибок в новой версии ПО, выявленных в процессе эксплуатации или обслуживания;

.3 техническое обслуживание ПО;

.4 испытания компьютеризированной системы, в отношении которой было проведено обслуживание;

.5 учет информации о проведенном обслуживании (обновление описи элементов компьютеризированных систем категорий II и III и описи ПО компьютеризированных систем категорий II и III).

4.3.2.3 Обслуживание ПО компьютеризированных систем категорий II и III должно выполняться признанной РС компанией (код деятельности 22014002), являющейся изготовителем оборудования, ПО которого подлежит обновлению, или имеющей авторизацию от изготовителя данного оборудования.

4.3.2.4 При использовании съемных носителей информации для проведения обслуживания ПО данные носители должны быть проверена на наличие вирусов непосредственно перед подключением к оборудованию.

4.3.2.5 Обновление антивирусного ПО не является обслуживанием.

5 ТРЕБОВАНИЯ К СУБ

5.1 УПРАВЛЕНИЕ КИБЕРРИСКАМИ В РАМКАХ СИСТЕМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ (СУБ)

5.1.1 Положения настоящего раздела носят рекомендательный характер, несмотря на это они призваны поддержать реализацию инструментов ИМО в вопросах кибербезопасности в морской индустрии, в соответствии с которыми после 1 января 2021 года кибериски необходимо учитывать в системе управления безопасностью (СУБ), которую должна разработать, задействовать и поддерживать каждая компания в соответствии с требованиями Международного кодекса по управлению безопасной эксплуатацией судов и предотвращением загрязнения (МКУБ).

5.1.2 Несмотря на то, что МКУБ не регулирует кибербезопасность напрямую, вопросы управления кибербезопасностью могут быть связаны с требованиями МКУБ, так как они полностью соответствуют целям МКУБ, а именно обеспечению безопасности на море, предотвращению несчастных случаев или гибели людей и предотвращению нанесения вреда окружающей среде, в частности морской среде, и имуществу. Поэтому Международная морская организация (ИМО) резолюцией MSC.428(98) «Управление киберрисками в морской отрасли в рамках систем управления безопасностью» призывает Морские Администрации обеспечить, чтобы кибериски были должным образом учтены в СУБ, и чтобы при освидетельствовании СУБ в компаниях и на судах после 1 января 2021 года, наряду с оценкой эффективности выполнения элементов МКУБ, были оценены принятые каждой Компанией меры по оценке и управлению киберрисками, а также эффективность мер по организации защиты от выявленных киберинцидентов.

5.1.3 Следует помнить, что нет двух одинаковых судоходных компаний и подходы к управлению киберрисками будут всегда индивидуальны для каждой конкретной компании и ее судов. Эти подходы могут зависеть от многих факторов, но при этом должны основываться на соответствующих международных нормах, правилах Государства флага и учитывать применимые кодексы, руководства и стандарты, рекомендованные ИМО, Морскими Администрациями, классификационными обществами и организациями морской индустрии, как это определено в пункте 1.2.3.2 МКУБ.

5.1.4 В настоящем разделе нет прямых указаний компаниям как управлять кибербезопасностью и как эти вопросы должны быть интегрированы в СУБ. Это должна сделать компания. Такая интеграция должна соответствовать резолюции ИМО MSC.428(98) «Управление киберрисками в морской отрасли в рамках систем управления безопасностью», циркуляру ИМО MSC-FAL.1/Circ.3 «Руководство по управлению киберрисками в морской отрасли» и позволит компаниям избежать дополнительных административных и финансовых нагрузок. Специфические требования, связанные с управлением киберрисками, каждая компания может вносить в существующую СУБ.

5.1.5 При этом, доказательством того, что вопросы управления кибербезопасностью учтены в СУБ и находятся в управляемых условиях можно считать следующее:

.1 компанией проведена оценка рисков, связанных с кибератаками или киберинцидентами, для обеспечения бесперебойной работы своих береговых подразделений и судов в соответствии с процедурами оценки рисков установленными в СУБ;

.2 управление киберрисками начинается на уровне высшего руководства. В компании внедрена культура понимания киберрисков на всех уровнях организации для обеспечения гибкого режима устойчивости к кибератакам и киберинцидентам. Высшее руководство понимает важность оценки и управления киберрисками;

.3 компания разработала принципы защиты от кибератак и киберинцидентов, таких как отключение, взлом, внедрение вредоносных программ, блокировка компьютерных систем и т.д. на основе оценки рисков. Эти принципы могут быть представлены в виде функциональных элементов, которые должны применяться на практике, работать непрерывно и одновременно в рамках внедренной системы управления, а именно:

определены кадровые решения по управлению кибербезопасностью. Распределены функции и обязанности персонала по использованию и обслуживанию, установлена система доступа и правила использования;

определены данные и ресурсы, при сбое в работе которых возникают риски, связанные с выполнением судовых операций;

разработаны защитные меры, включая меры немедленного реагирования на случаи сбоев в работе компьютеризированных систем для обеспечения непрерывности выполнения морских операций;

разработаны и реализованы меры для своевременного обнаружения сбоев в работе компьютеризированных систем;

разработаны и внедрены мероприятия по восстановлению выполнения судовых операций альтернативными методами в случае сбоев в работе компьютеризированных систем;

определены меры по резервному копированию и восстановлению компьютеризированных систем в случае нарушения их работы.

5.1.6 Интеграция необходимых мер для управления кибербезопасностью в СУБ компании может быть реализована через следующие элементы СУБ:

.1 цели:

компания должна установить, что цели интеграции системы управления кибербезопасностью соответствуют целям МКУБ, а именно обеспечению безопасности на море, предотвращению несчастных случаев или гибели людей и предотвращению нанесения вреда окружающей среде, в частности морской среде, и имуществу;

.2 политика:

высшее руководство компании должно оценить и, в случае актуальности проблемы кибератак и киберинцидентов в рамках эксплуатации судов, признать необходимость изменения СУБ компании для внедрения процессов кибербезопасности. Политика в области управления безопасностью может быть пересмотрена с учетом проблем кибератак и киберинцидентов и необходимости принятия ответных мер. Кибербезопасность, наряду с другими вопросами управления безопасностью, должна стать предметом регулирования со стороны высшего руководства и обязательной для исполнения судовым и береговым персоналом;

.3 ответственность компании:

главная ответственность в области кибербезопасности остается за высшим руководством. Может быть рассмотрен вопрос о назначении в компании ответственного за управление кибербезопасностью, защиту от кибератак и киберинцидентов, а также ответственного за оказание помощи капитану в выполнении судовых задач и обязанностей, связанных с применением *IT* и *OT*;

.4 соответствие требованиям:

в отношении кибербезопасности компания должна соблюдать обязательные для выполнения международные и национальные требования, а также должны быть оценены и приняты во внимание применимые кодексы, рекомендации и руководства ИМО, Морских Администраций, классификационных обществ

и организаций морской индустрии. Это, в свою очередь, должно оказать помощь в формировании основы для оценки рисков и изменении СУБ компании;

.5 оценка риска:

с помощью установленных в СУБ процедур по оценке рисков должны быть определены основные риски, связанные с кибератаками и киберинцидентами, и способы защиты от негативных последствий. Если не существует эквивалентной системы, то для систематической оценки можно использовать подход, изложенный в разд. 3.

Результаты оценки рисков и меры по защите от кибератак и киберинцидентов должны быть учтены в СУБ компании. Это могут быть процедуры, инструкции, руководства и т.д. Все принятые изменения в СУБ должны быть проведены в соответствии с процедурами компании и доведены до сведения соответствующего берегового и судового персонала;

.6 капитан:

в СУБ должны быть определены требования к квалификации капитана в области *IT* и *OT*, чтобы он был способен выполнять возложенные на него обязанности связанные с его должностью;

.7 поддержка со стороны берегового подразделения компании:

должна быть определена береговая структура поддержки капитана и судна в случаях необходимости:

реагирования на кибератаки;

реагирования на последствия киберинцидентов;

восстановления работоспособности компьютеризированных систем;

.8 ресурсы и персонал; квалификация; доступ к компьютеризированным системам:

при приеме на работу новый судовой персонал и сотрудники береговых подразделений должны ознакомиться с правилами компании в области кибербезопасности. Должны быть распределены обязанности и разработаны инструкции для всех лиц, имеющих задачи по кибербезопасности, а также для персонала, использующего судовые компьютеризированные системы каким-либо способом.

Компания должна разработать и внедрить меры по ограничению как физического, так и логического доступа к информационным ресурсам и компьютеризированным системам, а также меры по использованию съемных носителей информации и подключению других компьютеризированных систем.

В случае необходимости должны быть предусмотрены мероприятия по ознакомлению, обучению и совершенствованию навыков судового и берегового персонала на регулярной основе. СУБ может содержать план обучения и повышения квалификации, а также требования к квалификации для занятия той или иной позиции;

.9 готовность к аварийным ситуациям:

для судов и береговых подразделений компании в СУБ должны быть предусмотрены планы действий в чрезвычайных ситуациях при возникновении кибератак и киберинцидентов. Также должны быть предусмотрены проведения учений и тренировок по вопросам действий в чрезвычайных ситуациях при возникновении кибератак и киберинцидентов;

.10 обслуживание и ремонт:

в систему технического обслуживания и ремонта судовых механизмов и устройств должны быть добавлены меры безопасности, которые должны соблюдаться при обслуживании и ремонте компьютеризированных систем. Эти меры должны быть определены на основании оценки рисков.

В СУБ должны быть установлены критерии по выбору поставщиков услуг;

.11 отчеты:

с целью совершенствования системы сообщения о кибератаках и киберинцидентах должны направляться в ответственные подразделения компании для оценки, анализа и разработки корректирующих действий в соответствии с процедурами, установленными в СУБ;

.12 проверка, анализ и оценка, осуществляемая компанией; документация:

как правило, СУБ устанавливает применимые требования к ведению и доступности документации. При составлении документации в области кибербезопасности, возможно, необходимо будет предусмотреть ограничения в области публичного доступа к информации доступной только ограниченной группе лиц на борту и/или на берегу, например, представление прав администратора, управление паролями, резервное копирование и восстановление и т.д.

5.1.7 Интегрированная в СУБ компании система управления кибербезопасностью, ее функционирование и эффективность должны периодически проверяться и оцениваться компанией в соответствии с требованиями, установленными МКУБ.

5.1.8 Управление кибербезопасностью является постоянно изменяющимся процессом, который может претерпевать изменения в зависимости от внешних обстоятельств, поэтому одноразовая установка процедур управления кибербезопасностью и внедрение защитных средств не могут рассматриваться как достаточные. Компания должна учитывать постоянные изменения и выявленные недостатки в собственной системе и обеспечивать обновление оценки рисков и СУБ, инициируя тем самым непрерывный процесс улучшения.

6 ИСПЫТАНИЯ И ПРОВЕРКИ

Проверки и испытания должны проводиться на этапах рассмотрения технической документации, изготовления оборудования и строительства судна.

При строительстве судна испытания на борту должны проводится после окончания работ по монтажу и подключению всех кабелей и оборудования компьютеризированных систем.

Объем испытаний и проверок компьютеризированных систем должен включать в себя, как минимум, следующее:

рассмотрение технической документации на компьютеризированные системы;

освидетельствование кабелей и оборудования, используемого в компьютеризированных системах;

испытания компьютеризированных систем на борту судна;

испытания после обслуживания ПО;

проверка удаленного доступа;

проверка ручного управления.

6.1 РАССМОТРЕНИЕ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

6.1.1 Рассмотрение технической документации проводится в соответствии с частью II «Техническая документация» Правил РС/ТН.

6.1.2 На рассмотрение в Регистр должна быть представлена документация, указанная в табл. 2.1.1.

6.1.3 По результатам рассмотрения технической документации составляется письмо-заключение с указанием всех рассмотренных документов и замечаний, при их наличии.

6.2 ОСВИДЕТЕЛЬСТВОВАНИЕ КАБЕЛЕЙ И ОБОРУДОВАНИЯ

6.2.1 Кабели, используемые в компьютеризированных системах, должны быть испытаны в соответствии с разд. 10 части IV «Техническое наблюдение за изготовлением изделий» Правил РС/ТН.

6.2.2 Проверка соответствия сетевого коммуникационного оборудования, используемого в судовых компьютеризированных системах контроля, управления, регистрации и сигнализации, требованиям общепромышленных стандартов (например, стандарту МЭК 62443 или эквивалентным стандартам) должно подтверждаться наличием сертификата соответствия, выданного компетентной организацией.

6.2.3 В дополнение к указанному в 6.2.2, сетевое оборудование должно быть испытано в соответствии с разд. 12 части IV «Техническое наблюдение за изготовлением изделий» Правил РС/ТН, а также испытано на соответствие требованиям Руководства согласно программе и методике испытаний, разработанным изготовителем оборудования.

6.2.4 Программа и методика испытаний электронных устройств, используемых для хранения данных для систем категорий II и III, должна быть разработана изготовителем с учетом вида устройств хранения данных и представлена в Регистр для согласования.

6.2.5 Сетевое коммуникационное оборудование, используемое в судовых навигационных системах и системах радиосвязи, должно быть испытано в соответствии с требованиями стандарта МЭК 61162-460.

6.2.6 При положительных результатах испытаний оформляется свидетельство соответствующей формы согласно части I «Общие положения по техническому наблюдению» Правил РС/ТН.

6.3 ИСПЫТАНИЯ КОМПЬЮТЕРИЗИРОВАННЫХ СИСТЕМ НА БОРТУ СУДНА

6.3.1 Общие требования.

6.3.1.1 Общие требования по освидетельствованию оборудования и систем на борту судна изложены в части I «Общие положения по техническому наблюдению» Правил РС/ТН и разд. 1 Руководства по техническому наблюдению за постройкой судов.

6.3.1.2 Предварительный перечень объектов технического наблюдения разрабатывается системным интегратором.

6.3.1.3 Перечень объектов технического наблюдения, содержащий детальный объем и порядок технического наблюдения, виды проверок, испытаний и контроля, разрабатывается верфью в соответствии с 13.3 части I «Общие положения по техническому наблюдению» Правил РС/ТН на основании предварительного перечня, указанного в 6.3.1.2, рассматривается и согласовывается подразделением РС, осуществляющим техническое наблюдение за постройкой судов.

6.3.1.4 Программы швартовных и ходовых испытаний рассматриваются Регистром в соответствии с положениями части II «Техническая документация» Правил РС/ТН и разд. 18 Руководства по техническому наблюдению за постройкой судов.

6.3.1.5 После завершения швартовных и ходовых испытаний должны быть подготовлены и представлены Регистру протоколы испытаний компьютеризированных систем.

6.3.1.6 Должны быть предусмотрены программные (например, *WireShark*, *TCPdump*, *NMAP*, *XSpider*, *RedCheck*, *Efros Config Inspector* и др.) и аппаратные средства для проведения испытаний технических средств защиты от киберинцидентов, средств обнаружения киберинцидентов и кибератак, систем контроля, сигнализации и регистрации.

6.3.2 Испытания сети передачи данных.

6.3.2.1 Испытания сети передачи данных должны проводиться в период швартовных испытаний в соответствии с методикой и программой, разработанными системным интегратором. Для проверки функционирования и производительности сети должны быть проведены, как минимум, следующие испытания:

.1 проверка максимальной пропускной способности сети;

.2 проверка реагирования сети при широковещательном шторме;

.3 испытания на избыточность, для систем, использующих резервированные каналы связи и сетевые устройства.

6.3.2.2 Должно быть проверено соответствие фактического расположения сетевых устройств указанному в описании сетей передачи данных.

6.3.3 Испытания систем контроля, сигнализации и регистрации.

6.3.3.1 Испытания должны выполняться в соответствии с методикой и программой, разработанными системным интегратором. Программа и методика испытаний должны содержать перечень объектов испытаний, перечень программных и аппаратных средств, необходимых для проведения испытаний, описание методик испытаний либо обоснование отсутствия необходимости проведения соответствующих испытаний.

6.3.3.2 Целью испытаний является подтверждение обеспечения надежности и качества сетей передачи данных, а также обеспечение сигнализации, контроля и регистрации обнаружения киберинцидентов. При испытаниях должны быть проверены контроль, сигнализация и регистрация событий, кибератак и сигналов неисправностей, указанных в 4.1.3.2, 4.2.4 и 4.2.5.

6.3.3.3 В период швартовных и ходовых испытаний для оборудования беспроводной передачи данных должны проводиться проверки, чтобы продемонстрировать, что радиочастотная передача не оказывает влияние на судовое оборудование в результате воздействия электромагнитных помех в условиях эксплуатации.

6.3.4 Испытания средств защиты от кибератак и киберинцидентов.

6.3.4.1 Испытания должны проводиться в соответствии с методикой и программой, разработанными системным интегратором. Программа и методика испытаний должны содержать перечень объектов испытаний, перечень программных и аппаратных средств, необходимых для проведения испытаний, описание методик испытаний либо обоснование отсутствия необходимости проведения соответствующих испытаний.

6.3.4.2 Целью испытаний является подтверждение эффективности используемых в компьютеризированных системах средств защиты от кибератак и киберинцидентов. Должны быть проведены испытания средств защиты, указанных в 4.1.2.

6.3.5 Испытания средств обнаружения кибератак и киберинцидентов.

6.3.5.1 Испытания должны проводиться в соответствии с методикой и программой, разработанными системным интегратором. Программа и методика испытаний должны содержать перечень объектов испытаний, перечень программных и аппаратных средств, необходимых для проведения испытаний, описание методик испытаний либо обоснование отсутствия необходимости проведения соответствующих испытаний.

6.3.5.2 Целью испытаний является подтверждение эффективности используемых в компьютеризированных системах средств обнаружения кибератак и киберинцидентов. Должны быть проведены испытания средств обнаружения, указанных в 4.1.3.1.

6.3.6 Испытания средств восстановления компьютеризированных систем.

6.3.6.1 Испытания должны проводиться в соответствии с методикой и программой, разработанными системным интегратором. Программа и методика испытаний должны содержать перечень объектов испытаний, перечень программных и аппаратных средств, необходимых для проведения испытаний, описание методик испытаний либо обоснование отсутствия необходимости проведения соответствующих испытаний.

6.3.6.2 Целью испытаний является подтверждение эффективности используемых в компьютеризированных системах средств восстановления. Должны быть проведены испытания средств восстановления, указанных в 4.1.4.1.

6.3.7 Проверки средств контроля доступа к компьютеризированным системам.

6.3.7.1 Проверки должны проводиться в соответствии с методикой и программой, разработанными системным интегратором.

6.3.7.2 Целью проверки является подтверждение обеспечения периметра безопасности средствами контроля доступа к компьютеризированным системам, указанными в 4.1.6.3 и 4.1.6.4.

6.4 ИСПЫТАНИЯ ПОСЛЕ ОБСЛУЖИВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.4.1.1 После завершения обслуживания ПО должны быть проведены следующие проверки и тестирование:

.1 регрессионное тестирование (тестирование с целью обнаружения ошибок в уже протестированных участках исходного кода);

.2 проверки новых функциональных возможностей и/или улучшений ПО;

.3 нагрузочное тестирование (тестирование с целью определения производительности и времени отклика программных и аппаратных средств в ответ на внешний запрос с целью установления соответствия требованиям, предъявляемым к данным средствам).

6.4.1.2 Регистру должны быть представлены протоколы, содержащие информацию о результатах проведенных проверок и тестирования.

6.4.1.3 Целью проверок и тестирования ПО после обслуживания является подтверждение того, что оборудование, интегрированное в соответствующую систему или подсистему, ПО которого подлежит обслуживанию, работает в соответствии с техническим заданием и применимыми требованиями.

6.4.1.4 При планировании обслуживания ПО изготовитель или поставщик услуг должен разработать программу тестирования, которая содержит информацию о проводимых проверках и тестах. Программа тестирования должна содержать сценарии тестирования (*test cases*), охватывающие как нормальную работу, так и условия отказа.

6.4.1.5 Целью регрессионных тестов является подтверждение того, что функциональность, которая, как ожидается, все еще будет присутствовать после технического обслуживания, не будет нарушена.

6.4.1.6 Целью проверок новых функциональных возможностей и/или улучшений является подтверждение того, что достигнут желаемый эффект в результате обслуживания ПО.

6.4.1.7 Нагрузочное тестирование должно проводиться для оценки соответствия производительности программно-аппаратных средств требованиям, сформулированным в техническом задании.

6.4.1.8 Тестирование должно проводиться для каждого оборудования, подлежащего обслуживанию, и состоит из следующих действий:

.1 разработки плана проверок и тестирования, определяющего объем и риски, связанные с обслуживанием ПО, а также определяющего цели и методы тестирования, ожидаемое время и ресурсы, необходимые для проведения тестирования. План должен содержать четкую информацию о порядке проведения проверок и тестов и критерии оценки результатов тестирования;

.2 выбора сценариев тестирования (*test cases*) на основе требований, технического задания, анализа рисков и интерфейсов оборудования, ПО которого подлежит обслуживанию;

.3 документирования результатов проведенных проверок и тестов, включая версии ПО, которое подлежит обслуживанию;

.4 проверки процедур восстановления предыдущей версии и конфигурации ПО в случае выявления ошибок в новой версии ПО;

.5 анализа результатов проведенных проверок с целью подтверждения того, что обновления ПО могут быть установлены, и что во время тестирования не было обнаружено никаких сбоев. В случае выявления некорректной работы ПО, должны быть запланированы корректирующие действия и разработан обновленный план тестирования;

.6 должны учитываться последствия и любые связанные риски, которые могут возникнуть в результате восстановления предыдущей версии и конфигурации ПО,

и определены соответствующие проверки, которые должны быть проведены после восстановления, чтобы убедиться в работоспособности системы, удовлетворяющей применимым требованиям.

6.4.1.9 Процедуры восстановления предыдущей версии и конфигурации ПО должны быть предоставлены по запросу Регистра.

6.4.1.10 Документы (например, отчет поставщика услуг), подтверждающие выполнение и содержащие результаты проведенных проверок и тестов ПО, должны быть предоставлены по запросу Регистра.

6.5 ПРОВЕРКА УДАЛЕННОГО ДОСТУПА

6.5.1 Испытания должны проводиться в соответствии с методикой и программой, разработанными системным интегратором.

6.5.2 Целью испытаний является подтверждение выполнения требований, указанных в 4.1.7.

6.6 ПРОВЕРКА РУЧНОГО УПРАВЛЕНИЯ

6.6.1 Испытания должны проводиться в соответствии с методикой и программой, разработанными системным интегратором.

6.6.2 Целью испытаний является подтверждение выполнения требований, указанных в 4.1.8.

ПРИЛОЖЕНИЕ

КАЧЕСТВО ДАННЫХ

1 Защита данных.

1.1 Общая цель защиты данных заключается в обеспечении конфиденциальности, целостности и доступности данных. В зависимости от предполагаемого использования данных, они могут иметь различный порядок приоритета. Например, *OT*-системы, передающие критические для безопасности данные, будут определять приоритетность доступности, а затем целостность.

1.2 Сфера применения обеспечения достоверности данных (*data assurance*) охватывает данные, жизненный цикл которых ограничен судовой компьютеризированной системой, а также обмен данными с береговыми системами, подключенными к судовым сетям. Несмотря на то, что последствия несанкционированного изменения, повреждения или потери данных могут различаться для данных *IT*-систем (как правило, операционных данных, влияющих на административные процессы) и данных *OT*-систем (могут включать в себя уставки контролируемых параметров для управления оборудованием и безопасностью с точки зрения безопасности или воздействия на окружающую среду) там, где передача и обновление данных осуществляются с использованием сети, цели защиты данных имеют общие функции и должны рассматриваться для системы в целом.

2 Категоризация данных.

2.1 Системный интегратор должен разработать документ, содержащий информацию о категориях данных и определяющий риски для различных категорий данных. Данные должны быть разбиты на категории с точки зрения возможностей последствий нарушения, влияющих на конфиденциальность, целостность и доступность данных.

2.2 Возможное влияние на потерю достоверности данных должно быть определено следующим образом:

.1 НИЗКОЕ: потеря конфиденциальности, целостности или доступности данных окажет незначительное неблагоприятное влияние на безопасность эксплуатации судна, безопасность людей и/или окружающую среду;

.2 УМЕРЕННОЕ: потеря конфиденциальности, целостности или доступности данных окажет серьезное неблагоприятное влияние на безопасность эксплуатации судна, безопасность людей и/или окружающую среду;

.3 ВЫСОКОЕ: потеря конфиденциальности, целостности или доступности данных окажет серьезное или катастрофическое неблагоприятное влияние на безопасность эксплуатации судна, безопасность людей и/или окружающую среду.

2.3 В табл. 2.3 указано как присвоить категорию системам с учетом их влияния на конфиденциальность, целостность и доступность данных.

Таблица 2.3

Категория	Влияние	Функции системы	Конфиденциальность	Целостность	Доступность
I	Системы, выход из строя которых не приведет к опасным ситуациям для безопасности эксплуатации судна, безопасности людей и/или окружающей среды	Функции мониторинга для информационных/ административных задач	Низкое	Умеренное	Низкое
II	Системы, выход из строя которых может в конечном итоге привести к опасным ситуациям для безопасности эксплуатации судна, безопасности людей и/или окружающей среды	Функции сигнализации, контроля и управления, необходимые для поддержания судна в рабочем и пригодном для эксплуатации состоянии	Умеренное	Высокое	Низкое
III	Системы, выход из строя которых может немедленно привести к опасным ситуациям для безопасности эксплуатации судна, безопасности людей и/или окружающей среды	Функции управления для поддержания движения судна и безопасности рулевого управления	Умеренное	Высокое	Высокое

2.4 Категоризация, указанная в табл. 2.3, является рекомендуемой и должна выполняться в каждом конкретном случае.

Примечания: 1. Расширение: для систем, осуществляющих обмен данными систем ответственного назначения, необходимыми для их функционирования, может быть присвоена повышенная категория влияния.

2. Уровень конфиденциальности: необходимо понимать, что уровень конфиденциальности информации может иметь непосредственный риск для коммерческой деятельности.

2.5 Свойства данных должны определять, какие аспекты данных (например, своевременность, точность) необходимо гарантировать, чтобы обеспечить безопасное функционирование системы.

3 Защищенные и зашифрованные данные.

3.1 Системный интегратор должен выполнить анализ с целью оценки стоимости обеспечения защиты данных и влияние данных на производительность системы.

3.2 Должны быть обеспечены надлежащие меры для контроля доступа и другие технические и/или процедурные защитные меры для компьютеризированных систем или средств связи, непосредственно взаимодействующих с системой.

3.3 Используемые протоколы обмена данных должны гарантировать целостность данных, связанных с функциями управления, сигнализации, контроля, связи и безопасности, и обеспечивать своевременное восстановление поврежденных или некорректных данных.

4 Хранение данных.

4.1 Должен быть разработан документ с указанием критических данных, определенных при анализе рисков, которые необходимо хранить на борту судна для обеспечения надлежащей работы систем.

4.2 Устройства, используемые для хранения данных для систем категорий II или III, должны соответствовать условиям эксплуатации и подходить для эксплуатации в морских условиях. Данные, хранящиеся на таких устройствах, должны быть надлежащим образом продублированы для минимизации вероятности потери данных в случае единичного отказа устройства.

Российский морской регистр судоходства

Руководство по обеспечению кибербезопасности

ФАУ «Российский морской регистр судоходства»
191186, Санкт-Петербург, Дворцовая набережная, 8
www.rs-class.org/ru/