РОССИЙСКИЙ МОРСКОЙ РЕГИСТР СУДОХОДСТВА

ЦИРКУЛЯРНОЕ ПИСЬМО **№ 315-12-1630ц** от 16.09.2021

Касательно:

изменений к Правилам технического наблюдения за постройкой судов и изготовлением материалов и изделий для судов, 2021, НД № 2-020101-139

Объект(ы) наблюдения:

оборудование обеспечения кибербезопасности

Дата вступления в силу:[1]
01.11.2021

~~Отменяет/изменяет/дополняет циркулярное письмо №~~ **-** ~~от~~ -

Количество страниц: 1 + 13

Приложения:

Приложение 1: информация об изменениях, внесенных циркулярным письмом

Приложение 2: текст изменений к части IV «Техническое наблюдение за изготовлением изделий»

Генеральный директор К.Г. Пальников

Текст ЦП:

Настоящим информируем, что в Правила технического наблюдения за постройкой судов и изготовлением материалов и изделий для судов вносятся изменения, приведенные в приложениях к настоящему циркулярному письму.

Необходимо выполнить следующее:

1. Довести содержание настоящего циркулярного письма до сведения инспекторского состава подразделений РС, заинтересованных организаций и лиц в регионе деятельности подразделений РС.
2. Применять положения настоящего циркулярного письма при осуществлении технического наблюдения за изготовлением оборудования/изделий, заявка на которое поступила 01.11.2021 или после этой даты.

Перечень измененных и/или дополненных пунктов/глав/разделов:

часть IV: раздел 18

Исполнитель: А.В. Кунавин 315 +7 (812) 380-19-92

Система «Тезис» № 21-200636

[1] Служебные отметки *(ненужное зачеркнуть)*: ~~содержит~~ / не содержит обязательные международные/национальные требования ~~/ требуется срочное внедрение~~.

Приложение 1 к циркулярному письму
№ 315-12-1630ц от 16.09.2021

Информация об изменениях, внесенных циркулярным письмом (для включения в Перечень изменений к соответствующему Изданию РС)

№	Изменяемые пункты/главы/разделы	Информация по изменениям	№ и дата циркулярного письма, которым внесены изменения	Дата вступления в силу
1	Часть IV	Добавлен раздел 18	315-12-1630ц от 16.09.2021	01.11.2021

Приложение 2 к циркулярному письму
№ 315-12-1630ц от 16.09.2021

ПРАВИЛА ТЕХНИЧЕСКОГО НАБЛЮДЕНИЯ ЗА ПОСТРОЙКОЙ СУДОВ И ИЗГОТОВЛЕНИЕМ МАТЕРИАЛОВ И ИЗДЕЛИЙ ДЛЯ СУДОВ, 2021,

НД № 2-020101-139

ЧАСТЬ IV. ТЕХНИЧЕСКОЕ НАБЛЮДЕНИЕ ЗА ИЗГОТОВЛЕНИЕМ ИЗДЕЛИЙ

Добавлен раздел 18 следующего содержания:

«18 ОБОРУДОВАНИЕ И СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

18.1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

18.1.1 В настоящем разделе приняты следующие определения.

Коммутатор сети 460 — устройство сетевой инфраструктуры, которое предназначено для объединения оконечных устройств в сеть 460 и которое удовлетворяет требованиям, изложенным в настоящем разделе.

Маршрутизатор сети 460 — устройство сетевой инфраструктуры, которое способно безопасно обмениваться потоками данных между сетью 460 и другими контролируемыми сетями (включая сети 460).

Сеть 460 — сеть, состоящая только из узлов сети 450, узлов сети 460, а также устройств сетевой инфраструктуры сети 460 (коммутаторов, маршрутизаторов, шлюзов).

Узел сети 450 — оконечное устройство, удовлетворяющее стандарту МЭК 61162- 450 и дополнительным требованиям в настоящем разделе.

Узел сети 460 — оконечное устройство, подключаемое к защищенной (контролируемой) сети и удовлетворяющее как требованиям к узлу сети 450, так и требованиям, изложенным в настоящем разделе.

Шлюз сети 460 — устройство сетевой инфраструктуры, которое соединяет защищенную (контролируемую) сеть 460 и неконтролируемые сети, а также удовлетворяет требованиям, изложенным в настоящем разделе.

18.2 ОБЩИЕ ПОЛОЖЕНИЯ

18.2.1 Положения настоящего раздела применяются при техническом наблюдении за оборудованием, перечисленным в разделах 15140000 и 05410000 Номенклатуры объектов технического наблюдения Регистра.

18.2.2 Раздел устанавливает порядок, объем и методы технического наблюдения за изготовлением вышеупомянутого оборудования на предприятии (изготовителе).

18.2.3 Общие положения по организации технического наблюдения приведены в части I «Общие положения по техническому наблюдению», по технической документации – в части II «Техническая документация» и в 1.4 настоящей части.

18.3 ТЕХНИЧЕСКАЯ ДОКУМЕНТАЦИЯ

18.3.1 Состав технической документации, подлежащей представлению в Регистр в зависимости от кода номенклатуры указан в приложении 1.

18.3.2 Кодификация технической документации, используемая в настоящем разделе, представлена в табл. 18.3.2-1.

Таблица 18.3.2-1

Код	Наименование	Описание
D1	чертеж общего вида	документ, определяющий конструкцию изделия, взаимодействие его составных частей и поясняющий принцип работы изделия
D2	схема структурная	документ, определяющий основные функциональные части изделия, их назначение и взаимосвязи
T1	техническое описание	документ, содержащий описание устройства и принципа действия разрабатываемого изделия, а также обоснование принятых при его разработке технических решений
T2	программа и методика испытаний	документ, содержащий технические данные, подлежащие проверке при испытании изделий, а также порядок и методы их контроля
T3	анализ последствий отказов (АПО) (FMEA)	анализ видов и последствий отказов, представляющий собой структурированный подход к выявлению потенциальных отказов, которые могут возникнуть в процессе эксплуатации изделия (установки)
T4	перечень MAC адресов	перечень должен содержать информацию о MAC адресах каждого оборудования обеспечения кибербезопасности систем навигации и систем радиосвязи
I1 [XXX][1]	сертификат соответствия	документ, удостоверяющий, что данный вид оборудования соответствует конкретному стандарту(ам)
I2	свидетельство о взрывозащите	документ, удостоверяющий, что данный вид оборудования соответствует конкретному стандарту на вид взрывозащиты и предназначено специально для использования во взрывоопасной среде
[1] в скобках вместо XXX указывается обозначение стандарта(ов), соответствие которым должно подтверждаться сертификатом		

18.3.3 При необходимости Регистр может потребовать представление дополнительной технической документации, включая данные о надежности.

18.3.4 При рассмотрении технической документации определяется соответствие конструкции и заявленных эксплуатационных характеристик изделий требованиям соответствующих нормативных документов Регистра, включая судовые условия эксплуатации.

18.4 ОБЪЕМ И ПОРЯДОК ОСВИДЕТЕЛЬСТВОВАНИЯ

18.4.1 Перед испытаниями оборудования на предприятии (изготовителе) должно быть проверено наличие:

.1 комплекта одобренной Регистром технической документации на испытуемое оборудование;

.2 одобренной Регистром программы и методики испытаний;

.3 документов (сертификатов, протоколов испытаний и т.д.) компетентных организаций, подтверждающих положительные результаты специальных видов испытаний, если они предусматриваются программой испытаний;

.4 предусмотренного программой и методикой испытаний испытательного оборудования с необходимыми документами, подтверждающими его характеристики, свидетельства испытательной лаборатории;

.5 документов компетентных организаций, подтверждающих соответствие измерительных приборов заявленной погрешности измерения.

18.4.2 При освидетельствовании инспектор должен удостовериться в том, что испытания проводятся в соответствии с одобренной Регистром программой и по методикам испытаний, изложенным в настоящем разделе или другим равноценным методикам, одобренным Регистром.

18.4.3 После проведения механических и климатических испытаний, при которых возможны повреждения отдельных деталей, а также при нарушении работоспособности изделия во время любого испытания, должен проводиться детальный осмотр

оборудования, и должна быть определена возможность проведения дальнейших испытаний.

18.4.4 Инспектор имеет право отказаться от проведения испытаний, если объект испытаний недостаточно подготовлен, а также при обнаружении дефектов, влияющих на безопасность проведения освидетельствования или испытаний.

18.4.5 Если изделие не выдержало какого-либо вида испытаний и в его конструкцию в связи с этим внесено изменение или усовершенствование, испытания должны быть проведены вновь в соответствии с программой и методикой испытаний. Объем повторных испытаний должен быть согласован с Регистром.

18.4.6 Объем и виды испытаний оборудования при его изготовлении представлены в приложении 1.

18.4.7 При положительных результатах испытаний оформляется свидетельство соответствующей формы согласно части I «Общие положения по техническому наблюдению».

18.4.8 По истечении срока действия СТО возобновляется по заявке изготовителя в соответствии с 6.8 части I «Общие положения по техническому наблюдению».

18.4.9 При внесении изменений в конструкцию оборудования автоматизации, которые приводят к изменению процесса работы, нагрузок на элементы изделия, ресурс или другие существенные параметры работы изделия, или внесения изменений в программное обеспечение и ранее заявленные технические характеристики материала или изделия, для подтверждения или возобновления СТО изделия должны быть подвергнуты испытаниям с учетом внесенных изменений по программе, одобренной Регистром.

18.5 УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ИСПЫТАНИЙ И ПРОВЕРОК

18.5.1 Испытания и проверки должны проводиться на одних и тех же образцах в последовательности, которая должна быть отражена в программе испытаний.

18.5.2 Для оборудования автоматизации вне зависимости от последовательности, указанной в программе испытаний, и не обязательно на образцах, подвергаемых другим видам испытаний, допускается проводить следующие испытания:

.1 на воздействие соляного тумана;

.2 на грибостойкость.

18.5.3 Испытания и проверки оборудования обеспечения кибербезопасности радио- и навигационного оборудования должны проводиться испытательной лабораторией.

18.5.4 Лаборатории, указанные в 18.5.3, должны иметь, как минимум, следующее оборудование:

.1 анализатор сетевых протоколов;

.2 симулятор способный обеспечить:

передачу и прием совместимого и не совместимого с МЭК 61162-450:2018 трафика;

генерацию неверных данных;

поддержку Ethernet интерфейса;

поддержку SNMP и данных системного журнала клиент-сервер;

мониторинг конфигурации и состояния сети с помощью SNMP;

мониторинг конфигурации и состояния сети с помощью системного журнала;

протокол межсетевых управляющих сообщений ICMP;

загрузку сети от 0 до 100 % трафиком, совместимым и не совместимым с МЭК 61162-450:2018 (например, TCP/IP, UDP/IP);

передачу с приоритетного трафика совместимого с МЭК 61162-450:2018;

многосетевую передачу данных, совместимых с МЭК 61162-450:2018, включая VLAN и подсети.

.3 симулятор для тестирования функций безопасности, который должен обеспечивать:

соединение клиент-сервер;

генерацию пакетов DoS-атак.

18.6 ОПИСАНИЕ ИСПЫТАНИЙ И ПРОВЕРОК

18.6.1 Испытания и проверки оборудования обеспечения кибербезопасности судовых систем управления и автоматизации.

18.6.1.1 Оборудование обеспечения кибербезопасности систем управления и автоматизации, должно соответствовать требованиям стандартов МЭК 62443-4-1:2018 и МЭК 62443-4-2:2019. Соответствие оборудования перечисленным стандартам должно подтверждаться сертификатом соответствия, выданным компетентной организацией, признанной национальным органом по аккредитации для выполнения оценки соответствия указанным стандартам.

18.6.1.2 В дополнение к 18.6.1.1 изделия должны быть подвергнуты испытаниям и проверкам, методики которых изложены в разд. 12 настоящей части. Перечень испытаний представлен в приложении 1. Обозначения проверок и испытаний соответствуют кодам, указанным в табл. 12.6 разд. 12 настоящей части.

18.6.2 Испытания и проверки оборудования обеспечения кибербезопасности радио- и навигационного оборудования.

18.6.2.1 Испытания и проверки узла сети 450.

.1 должно быть проверено, что при нормальной работе изделия не могут быть установлены никакие подключения к внешним сетям и съемным носителям информации;

.2 должно быть проверено, что в изделии реализована функция системного журнала в соответствии с требованиями п. 4.3.3.2 стандарта МЭК 61162-450:2018;

.3 должно быть проверено, что в документации изготовителя указана максимальная выходная рабочая полоса пропускания;

.4 если изделием предусмотрено выполнение сетевых функций иных чем описанных в стандарте МЭК 61162-450:2018, должно быть проверено, что в документации изготовителя указаны параметры протокола их выполнения (например, IP адреса, номера портов).

18.6.2.2 Испытания и проверки узла сети 460.

18.6.2.2.1 Проверка управления сетевым трафиком.

.1 должно быть проверено, что согласно документации предприятия (изготовителя) изделие не создает трафик, несовместимый с МЭК 61162-450:2018;

.2 должно быть проверено, что в документации предприятия (изготовителя) указана максимальная скорость передачи для всех поддерживаемых служб, при этом из документации должно следовать, что весь трафик совместимый с МЭК 61162-450:2018 передается на своей максимальной скорости;

.3 необходимо проверить, что изделие отвечает своим эксплуатационным требованиям при потере вплоть до 0,1 % пакетов в течение периода времени 10 мин;

.4 должно быть проверено, что в документации предприятия (изготовителя) содержится описание работы изделия при превышении максимальной скорости входных данных;

.5 необходимо проверить, что согласно документации предприятия (изготовителя) изделие отбрасывает все неподдерживаемые данные, поступающие на вход;

.6 если изделие поддерживает VLAN, то должно быть проверено, что в документации предприятия (изготовителя) указана максимальная скорость передачи для всех поддерживаемых VLAN служб. Предприятие (изготовитель) должно предоставить документальное подтверждение, что весь совместимый с МЭК 61162-450 трафик в каждой сети VLAN передается на своей максимальной скорости;

.7 если изделие поддерживает VLAN, то должно быть проверено, что согласно документации имеется поддержка протокола IEEE 802.1Q.

18.6.2.2.2 Общая проверка безопасности.

.1 должно быть проверено, что согласно документации в изделии не применяются функции беспроводной локальной сети или точки доступа;

.2 для изделий, поддерживающих VLAN, необходимо проверить, что не используется туннелирование.

18.6.2.2.3 Проверка отказа в обслуживании.

.1 должно быть проверено, что в документации предприятия (изготовителя) указана максимальная входная ширина полосы пропускания;

.2 необходимо проверить, что при подаче с симулятора трафика максимального (согласно документации) объема, изделие отвечает своим эксплуатационным требованиям;

.3 должна быть выполнена проверка по следующей методике: при помощи симулятора необходимо обеспечить подачу трафика объемом в 200 % от максимального (согласно документации) в течении не менее 10 мин, после этого уменьшить трафик до максимального (согласно документации). Необходимо проверить, что изделие работает так, как это заявлено в документации предприятия (изготовителя) как во время подачи повышенного трафика, так и после изменения;

.4 должно быть проверено, что в документации предприятия (изготовителя) указана максимальная выходная ширина полосы пропускания;

.5 необходимо проверить, что изделие не превышает заявленную максимальную выходную ширину полосы пропускания.

18.6.2.2.4 Проверка безопасности съемных носителей информации.

.1 необходимо проверить, что количество точек для подключения съемных носителей информации (USB- порты, приводы оптических дисков) сведено к абсолютному минимуму, необходимому для работы изделия и его обслуживания. Должно быть проверено, что легкий доступ к любым другим точкам подключения ограничен;

.2 должно быть проверено, что при подключении клавиатуры или мышки к USB-портам, предназначенным для подключения съемных носителей информации, изделие не распознает эти устройства и не выполняет их функции;

.3 должно быть проверено, что легкий доступ к USB-портам, предназначенным для иных целей, чем подключение съемных носителей информации, ограничен;

.4 в случае, если изделием предусмотрен ручной запуск любых файлов со съемного носителя информации, то должно быть проверено, что запуск возможен только для файлов, верифицированных цифровыми подписями или специальными ключами;

.5 в случае, если в соответствии с документацией на изделие, предусмотрено использование не запускаемых файлов, то должно быть проверено, что все не запускаемые файлы проверяются в соответствии с указаниями в документации изготовителя, перед использованием в изделии.

18.6.2.2.5 Проверка контроля доступа к настройке конфигурации.

.1 необходимо проверить, что согласно документации предприятия (изготовителя), доступ для внесения изменений в конфигурацию изделия предоставляется только авторизованному пользователю;

.2 должно быть проверено, что авторизация пользователя, необходимая для изменения настроек изделия, базируется по крайней мере на восьмизначном пароле или RSA ключах;

.3 должно быть проверено, что пароли, не имеющие хотя бы три из четырех типов символов (строчные, заглавные, цифры, специальные символы) не могут быть использованы при изменении пароля;

.4 необходимо проверить, что в руководстве пользователя даны указания по использованию надежных паролей (если применимо).

18.6.2.2.6 Проверка прямого доступа к неконтролируемой сети.

Проверки этого пункта применяются в случае, если в изделии предусмотрена функция прямого соединения с оборудованием, подключенным к неконтролируемой сети.

.1 должно быть проверено, что заводские настройки по умолчанию запрещают прямые соединения с неконтролируемыми сетями;

.2 должно быть проверено, что установление VPN соединения через шлюз сети 460 является обязательным условием для активации прямого соединения, при этом только оператор узла сети 460 может активировать прямое соединение. Эта проверка выполняется для каждого сконфигурированного прямого обмена данными;

.3 для каждого прямого обмена данными должно быть проверено следующее:

имеется постоянная индикация при активном прямом соединении;

при активации прямого соединения создается предостережение;

предостережение заменяется предупреждением по истечении заданного периода времени (если предусмотрено);

предостережение и предупреждение сбрасываются при закрытии прямого соединения.

.4 необходимо проверить, что документации изготовителя указан алгоритм шифрования, используемый для VPN. Алгоритм шифрования может быть как

ассиметричным, так и симметричным. Асимметричный алгоритм шифрования должен иметь длину ключа не менее 2048 бит и уровень защиты не ниже RSA. Симметричный алгоритм шифрования иметь длину ключа не менее 256 бит и уровень защиты не ниже AES.

18.6.2.2.7 Резервирование.

Для изделий, отнесенных согласно документации предприятия (изготовителя) к критически важным, должно быть проверено наличие резервирования интерфейсов или устройств.

18.6.2.2.8 Проверка функции мониторинга.

Должно быть проверено, что информация мониторинга записывается системный журнал с периодичностью 30 мин, при этом информация об изменении конфигурации записывается в журнал не чаще одного раза в минуту.

18.6.2.3 Испытания и проверки коммутатора сети 460.

18.6.2.3.1 Проверка распределения ресурсов.

.1 должно быть проверено, что согласно документации предприятия (изготовителя), предусмотрено средство конфигурирования потоков, определяемых комбинацией из идентификатора интерфейса, MAC или IP адреса, номера протокола и номера порта;

.2 должно быть проверено, что согласно документации предприятия (изготовителя) предусмотрено средство распределения сетевого ресурса для всех зарегистрированных потоков;

.3 для проведения данной проверки необходимо обеспечить регистрацию всего входящего и исходящего трафика. При помощи симулятора необходимо создать как зарегистрированный, так и незарегистрированный трафик. Должно быть подтверждено, что изделием передается только входящий и исходящий трафик, а весь незарегистрированный трафик блокируется;

.4 необходимо проверить, что согласно документации предприятия (изготовителя) предусмотрена возможность ограничения общего объема трафика посредством распределения ресурсов, для каждого из интерфейсов с узлом сети 450 и узлом сети 460;

.5 для проверки необходимо подключить к изделию при помощи симулятора два узла сети 460 и настроить их на передачу друг другу трафика максимального объема (согласно установкам). Должно быть проверено, что весь трафик проходит через изделие. После этого необходимо на 10 мин увеличить трафик на 50 % сверх установленного максимального значения и проверить что чрезмерный трафик заблокирован;

.6 если изделие поддерживает VLAN, то должно быть проверено, что согласно документации изготовителя имеются средства для настройки виртуальных сетей (VLAN) для каждого из интерфейсов;

.7 если изделие поддерживает VLAN, то должно быть проверено, что согласно документации имеется поддержка протокола IEEE 802.1Q;

.8 необходимо проверить, что согласно документации изготовителя имеются средства для фильтрации многоадресного трафика при помощи отслеживания IGMP;

.9 для проверки фильтрации многоадресного сетевого трафика необходимо при помощи симулятора подключить к изделию параллельно или последовательно коммутатор сети 460, маршрутизатор сети 460, узел сети 460 и узел сети 450. После этого в изделии задать многоадресную группу для фильтрации трафика при помощи отслеживания IGMP и проверить, что изделие отправляет запросы о членстве для этой многоадресной группы.

18.6.2.3.2 Проверка предотвращения петель.

.1 должно быть проверено, что согласно документации в изделии имеется механизм предотвращения петель;

.2 для изделий, поддерживающих протокол RSTP, должно быть проверено, что, что согласно документации предприятия (изготовителя) изделие поддерживает протокол RSTP версии IEEE 802.1D-2004;

.3 для проверки необходимо подключить в кольцевую топологию три коммутатора сети 460, к каждому из которых подсоединен хотя бы один узел сети 460, и начать одноадресную передачу. Необходимо проверить, что изделие не дублирует данные на других коммутаторах;

.4 для проверки необходимо подключить в кольцевую топологию три коммутатора сети 460, к каждому из которых подсоединен хотя бы один узел сети 460, и начать одноадресную передачу. После этого необходимо отсоединить любой кабель между соседними коммутаторами и проверить, что данные доступны для узлов сети 460 в

течение 5 с. Повторить проверку, отключая поочередно каждый кабель между коммутаторами.

18.6.2.3.3 Проверка общей безопасности.

.1 необходимо проверить, что согласно документации предприятия (изготовителя) изделие не использует функции беспроводной локальной сети или точки доступа;

.2 должно быть проверено, что при наличии VLAN не используется туннелирование.

18.6.2.3.4 Проверка отказа в обслуживании.

Необходимо проверить, что согласно документации, в изделии имеется механизм предотвращения DoS-атак по протоколам ICMP и IGMP.

18.6.2.3.5 Проверка контроля доступа к настройке конфигурации.

.1 необходимо проверить, что согласно документации предприятия (изготовителя), доступ для внесения изменений в конфигурацию изделия предоставляется только авторизованному пользователю;

.2 должно быть проверено, что авторизация пользователя, необходимая для изменения настроек изделия, базируется по крайней мере на восьмизначном пароле или RSA ключах;

.3 должно быть проверено, что пароли, не имеющие хотя бы три из четырех типов символов (строчные, заглавные, цифры, специальные символы) не могут быть использованы при изменении пароля;

.4 необходимо проверить, что в руководстве пользователя даны указания по использованию надежных паролей (если применимо).

18.6.2.3.6 Проверка контроля доступа к сети.

.1 необходимо проверить, что согласно документации предприятия (изготовителя), в изделии предусмотрены средства для разрешения и запрещения потока по IP адресу, номеру протокола и номеру порта для каждого физического порта;

.2 должно быть проверено, что для каждого физического порта имеется возможность разрешения или запрещения устройства по MAC адресу. Если изделие предназначено для установки в защищенной зоне, должно быть проверено, что эти средства конфигурируются для включения и отключения авторизации по MAC адресу.

18.6.2.3.7 Проверка дополнительных требований безопасности.

.1 должно быть проверено, что изделие продолжает нормальную работу с последней сохраненной конфигурацией при повторном включении питания после выключения (или сбоя) питания;

.2 должно быть проверено, что в изделии предусмотрены средства для возврата к предыдущей сохраненной конфигурации;

.3 необходимо проверить, что в документации содержаться указания по установке изделия в физически защищенном месте.

18.6.2.3.8 Проверка функции мониторинга.

.1 должно быть проверено, что изделие обеспечивает мониторинг следующей информации: информация об интерфейсе, список соседних MAC-адресов для каждого интерфейса, изменение соседних MAC-адресов;

.2 должно быть проверено, что изделие отправляет информацию о конфигурации сети в ответ на SNMP запрос от функции мониторинга сети. Необходимо проверить, что при изменении конфигурации (например изменение соседнего MAC-адреса) информация о событии передается по крайней мере либо системным журналом (безусловная отправка) либо посредством SNMP-ловушки (по запросу функции мониторинга сети). Также должно быть проверено, что информации о конфигурации передается системным журналом не чаще одного раза в минуту;

.3 должно быть проверено, что изделие отправляет информацию о загрузке входных и выходных интерфейсов в процентах (усредненную за 5 мин) в ответ на SNMP запрос от функции мониторинга сети. Необходимо проверить, что при существенном изменении загрузки (трафик превышает установленное в шкале от 0 % до 100 % ограничение) информация об этом событии передается системным журналом (безусловная отправка) либо посредство SNMP-ловушки (по запросу функции мониторинга сети). Также должно быть проверено, что информация передается через системный журнал не чаще одного раза в 3 с.

18.6.2.4 Испытания и проверки маршрутизатора сети 460.

18.6.2.4.1 Проверка разделения трафика.

.1 должно быть проверено, что согласно документации изготовителя, в изделии предусмотрены средства для передачи всех данных или части данных между сетью 460 и контролируемыми сетями (или другими сетями 460);

.2 должна быть проверена возможность ограничения максимального объема трафика между сетью 460 и контролируемыми сетями (или другими сетями 460). Проверка должна проводиться в соответствии с инструкцией предприятия (изготовителя);

.3 для изделий, поддерживающих VLAN, должно быть проверено, что согласно документации изготовителя, изделие обеспечивает возможность установления и разрыва соединения между сетью 460 и контролируемыми сетями (или другими сетями 460) с VLAN;

.4 если изделие поддерживает VLAN, то должно быть проверено, что согласно документации имеется поддержка протокола IEEE 802.1Q;

.5 необходимо проверить, согласно документации предприятия (изготовителя) имеются средства для фильтрации многоадресного трафика при помощи отслеживания IGMP;

.6 для проверки фильтрации многоадресного сетевого трафика необходимо при помощи симулятора подключить к изделию параллельно или последовательно коммутатор сети 460, маршрутизатор сети 460, узел сети 460 и узел сети 450. После этого в изделии задать многоадресную группу для фильтрации трафика при помощи слежения IGMP и проверить, что изделие отправляет запросы о членстве для этой многоадресной группы.

18.6.2.4.2 Проверка распределения ресурсов.

.1 для проведения данной проверки необходимо обеспечить регистрацию всего входящего и исходящего трафика. При помощи симулятора необходимо создать как зарегистрированный, так и незарегистрированный трафик. Должно быть подтверждено, что изделием передается только входящий и исходящий трафик, а весь незарегистрированный трафик блокируется;

.2 необходимо проверить, что согласно документации предприятия (изготовителя) предусмотрена возможность ограничения общего объема трафика, посредством распределения ресурсов, для каждого из интерфейсов с узлом сети 450 и узлом сети 460;

.3 для проверки необходимо подключить к изделию при помощи симулятора два узла сети 460 и настроить их на передачу друг другу трафика максимального объема (согласно установкам). Должно быть проверено, что весь трафик проходит через изделие. После этого необходимо на 10 мин увеличить трафик на 50 % сверх установленного максимального значения и проверить что чрезмерный трафик заблокирован;

.4 необходимо проверить, что согласно документации предприятия (изготовителя), в изделии предусмотрены средства для разрешения и запрещения потока по IP адресу, номеру протокола и номеру порта для каждого физического порта.1 Должно быть проверено, что предусмотрены средства для распределения сетевого ресурса для всех зарегистрированных потоков;

.5 если изделие поддерживает VLAN, должно быть проверено, что предусмотрены средства для ограничения общего объема трафика до заданного значения для каждого подключения VLAN к контролируемым сетям и сетям 460 при помощи распределения ресурсов.

18.6.2.4.3 Проверка приоритизации трафика.

.1 необходимо выполнить проверку по следующей методике:

использованием симулятора создать трафик с тремя различными уровнями приоритета, включая самый низкий приоритет;

в изделии задать ограничение трафика, достаточное только для прохождения трафика наивысшего приоритета;

увеличить объем трафика с самым низким приоритетом вплоть до момента пока не произойдет потеря данных.

Проверка считается пройденной, если процент потери данных трафика наивысшего приоритета – самый низкий, а процент потери данных трафика с самым низким приоритетом – наивысший.

.2 для проверки необходимо для каждого порта создать на 30 с объем трафика, превышающий на 50 % физическую пропускную способность канала (или установленную максимальную входную скорость передачи данных), после этого снизить объем трафика до значения, составляющего 50 % от физической пропускной способности канала

(или установленной максимальной входной скорости передачи данных). Необходимо проверить, что происходило падение трафика нижнего приоритета до тех пор, пока объем поступающего трафика не был уменьшен до 50 % от физической пропускной способности канала (или установленной максимальной входной скорости передачи данных);

.3 в процессе проверки для каждого порта должно быть подтверждено, что трафик с наивысшим приоритетом передается без потерь до тех пор, пока объем трафика, переданного за последние 30 с, не превысит значение установленной максимальной входной скорости передачи данных для конкретного порта, после чего допускается падение трафика данных с наивысшим приоритетом;

.4 должно быть проверено, что отбрасывание трафика сообщается самостоятельно системным журналом, либо в качестве ответа на SNMP-ловушку.

18.6.2.4.4 Проверка общих требований безопасности.

.1 необходимо проверить, что согласно документации предприятия (изготовителя) изделие не использует функции беспроводной локальной сети или точки доступа;

.2 должно быть проверено, что при наличии VLAN не используется туннелирование.

18.6.2.4.5 Проверка отказа в обслуживании.

Необходимо проверить, что согласно документации предприятия (изготовителя), в изделии имеется механизм предотвращения DoS-атак по протоколам ICMP и IGMP.

18.6.2.4.6 Проверка контроля доступа к настройке конфигурации.

.1 необходимо проверить, что согласно документации предприятия (изготовителя), доступ для внесения изменений в конфигурацию изделия предоставляется только авторизованному пользователю;

.2 должно быть проверено, что авторизация пользователя, необходимая для изменения настроек изделия, базируется по крайней мере на восьмизначном пароле или RSA ключах;

.3 должно быть проверено, что пароли, не имеющие хотя бы три из четырех типов символов (строчные, заглавные, цифры, специальные символы) не могут быть использованы при изменении пароля;

.4 необходимо проверить, что в руководстве пользователя даны указания по использованию надежных паролей (если применимо).

18.6.2.4.7 Проверка контроля доступа к сети.

.1 необходимо проверить, что согласно документации, в изделии предусмотрены средства для разрешения и запрещения потока по IP адресу, номеру протокола и номеру порта для каждого физического порта;

.2 должно быть проверено, что для каждого физического порта имеется возможность разрешения или запрещения устройства по MAC адресу. Если изделие предназначено для установки в защищенной зоне, должно быть проверено, что эти средства конфигурируются для включения и отключения авторизации по MAC адресу.

18.6.2.4.8 Проверка дополнительных требований безопасности.

.1 должно быть проверено, что изделие продолжает нормальную работу с последней сохраненной конфигурацией при повторном включении питания после выключения (или сбоя) питания;

.2 должно быть проверено, что в изделии предусмотрены средства для возврата к предыдущей сохраненной конфигурации;

.3 необходимо проверить, что в документации предприятия (изготовителя) содержаться указания по установке изделия в физически защищенном месте.

18.6.2.4.9 Проверка функции мониторинга.

.1 должно быть проверено, что изделие обеспечивает мониторинг следующей информации: информация об интерфейсе, список соседних MAC-адресов для каждого интерфейса, изменение соседних MAC адресов;

.2 должно быть проверено, что изделие отправляет информацию о конфигурации сети в ответ на SNMP запрос от функции мониторинга сети. Если изделие поддерживает VLAN, то необходимо также проверить, что информация о текущей конфигурации VLAN отправляется в ответ на SNMP запрос. Должно быть проверено, что при изменении конфигурации (например изменение соседнего MAC адреса) информация о событии передается по крайней мере либо системным журналом (безусловная отправка) либо посредством SNMP-ловушки (по запросу функции мониторинга сети). Также должно быть проверено, что информации о конфигурации передается системным журналом не чаще одного раза в минуту;

.3 должно быть проверено, что изделие отправляет информацию о загрузке входных и выходных интерфейсов в процентах (усредненную за 5 мин) в ответ на SNMP запрос от функции мониторинга сети. Необходимо проверить, что при существенном изменении загрузки (трафик превышает установленное в шкале от 0 % до 100 % ограничение) информация об этом событии передается системным журналом (безусловная отправка) либо посредство SNMP-ловушки (по запросу функции мониторинга сети). Также должно быть проверено, что информация передается через системный журнал не чаще одного раза в 3 с.

18.6.2.5 Испытания и проверки шлюза сети 460.

18.6.2.5.1 Проверка отказа в обслуживании.

Необходимо проверить, что согласно документации предприятия (изготовителя), в изделии имеется механизм предотвращения DoS-атак по протоколам ICMP и IGMP.

18.6.2.5.2 Проверка контроля доступа к настройке конфигурации.

.1 необходимо проверить, что согласно документации предприятия (изготовителя), доступ для внесения изменений в конфигурацию изделия предоставляется только авторизованному пользователю;

.2 должно быть проверено, что авторизация пользователя, необходимая для изменения настроек изделия, базируется по крайней мере на восьмизначном пароле или RSA ключах;

.3 должно быть проверено, что пароли, не имеющие хотя бы три из четырех типов символов (строчные, заглавные, цифры, специальные символы) не могут быть использованы при изменении пароля;

.4 необходимо проверить, что в руководстве пользователя даны указания по использованию надежных паролей (если применимо).

18.6.2.5.3 Проверка безопасности связи.

.1 должно быть проверено, что согласно документации предприятия (изготовителя), прямое соединение между неконтролируемыми сетями и сетью 460 может разрешено только в шлюзе сети 460;

.2 необходимо при помощи симулятора установить VPN соединение, между сетью 460 и неконтролируемой сетью и проверить, что VPN действительно предоставляется через это соединение;

.3 необходимо проверить, что в документации предприятия (изготовителя) указан алгоритм шифрования, используемый для VPN. Алгоритм шифрования может быт как ассиметричным, так и симметричным:

асимметричный алгоритм шифрования должен иметь длину ключа не менее 2048 бит и уровень защиты не ниже RSA;

симметричный алгоритм шифрования иметь длину ключа не менее 256 бит и уровень защиты не ниже AES;

.4 должно быть проверено, что согласно документации, доставка сертификатов базируется на цепочки доверия, или что обмен закрытыми ключами (сертификатами) осуществляется безопасным ручным способом, или с использованием комбинации ручного метода и сообщений.

18.6.2.5.4 Проверка межсетевого экрана.

.1 должно быть проверено, что в заводских настройках все прямые подключения к сетям 460 отключены;

.2 для проверки необходимо в соответствии с документацией предприятия (изготовителя) установить изделие между сетью 460 и неконтролируемой сетью. Затем при помощи сетевого сканера с функцией сканирования портов, просканировать весь диапазон адресов сети 460, демилитаризированной зоны и неконтролируемой сети. С помощью программного обеспечения для захвата пакетов, работающего в режиме «смешанный», необходимо проверить, что изделие не пропускает следующие категории пакетов, идущих в направлении от неконтролируемой сети в сеть 460 и в обратном направлении:

UDP и TCP сканирование портов в диапазоне 1 ─ 65535 для всего внутреннего диапазона адресов сети 460;

UDP и TCP сканирование портов в диапазоне 1 ─ 65535 для всего диапазона адресов демилитаризированной зоны (при ее наличии);

UDP и TCP сканирование портов в диапазоне 1 ─ 65535 для диапазона неконтролируемой сети.

.3 необходимо проверить, что изделие регистрирует трафик как внешнее/внутреннее правило брандмауэра, которое состоит из IP адреса отправителя, IP адреса получателя, протокола и номера порта;

.4 необходимо проверить, что изделием обеспечивается возможность предоставления списка всех прямых подключений за последние 12 мес;

.5 должно быть проверено, что изделие обеспечивает возможность предоставления списка активированных прямых подключений между сетями 460 и неконтролируемыми сетями. Список должен содержать следующую информацию: IP адрес отправителя, IP адрес получателя, время начала и окончания соединения, протокол и номер порта;

.6 необходимо проверить, что, разрешение на установления прямого подключения к узлу сети 460 из неконтролируемой сети, может быть дано только со стороны сети 460. Необходимо проверить, что согласно документации изготовителя это подключение не может быть активировано со стороны неконтролируемой сети.1 Также необходимо проверить, что имеются средства, обеспечивающие выполнение этой операции только после получения разрешения, например, от вахтенного офицера;

.7 должно быть проверено, что изделие автоматически завершает все прямые соединения по прошествии предустановленного времени, не превышающего 4 ч (если пользователь не продлевал сеанс);

.8 должно быть проверено, что изделие завершает все прямые соединения автоматически при простое соединения в течение предустановленного времени, не превышающего 10 мин;

.9 должно быть проверено, что выводится индикация и создается предостережение при установлении прямого соединения между сетью 460 и неконтролируемой сетью.

18.6.2.5.5 Проверка сервера приложений.

.1 должно быть проверено, что согласно документации изготовителя на сервере приложений имеются средства для аутентификации клиентов, подключенных через неконтролируемые сети (например, с использованием пароля);

.2 должно быть проверено, что пересылка или маршрутизация третьего уровня выключена (т.е. маршрутизация пакетов запрещена);

.3 необходимо проверить соответствие изделия требованиям 18.6.2.2;

.4 необходимо проверить, что в документации предприятия (изготовителя) содержится описание средств защиты от вредоносных программ для соответствующей компьютеризированной платформы.

18.6.2.5.6 Проверка совместного доступа к файловому хранилищу в демилитаризированной зоне.

.1 должно быть проверено, что файл может быть загружен и выгружен между демилитаризированной зоной и неконтролируемыми сетями (если предусмотрено);

.2 должно быть проверено, что файл может быть загружен и выгружен между демилитаризированной зоной и сетями 460 (если предусмотрено);

.3 если в пределах демилитаризированной зоной предоставляется доступ к файловому хранилищу, то необходимо проверить, что согласно документации изготовителя, обеспечивается поддержка протокола, такого как SMB или SFTP;

.4 должно быть проверено, что согласно документации, доступ изделия к файловому хранилищу и соответствующий трафик демилитаризованной зоны соответствует требованиям к другой функции сети и функции сети как указано в МЭК 61162-450 (если применимо).

18.6.2.5.7 Проверка дополнительных требований безопасности.

.1 должно быть проверено, что изделие продолжает нормальную работу с последней сохраненной конфигурацией при повторном включении питания после выключения (или сбоя) питания;

.2 должно быть проверено, что в изделии предусмотрены средства для возврата к предыдущей сохраненной конфигурации;

.3 необходимо проверить, что в документации содержаться указания по установке изделия в физически защищенном месте.

ПРИЛОЖЕНИЕ 1

СОСТАВ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ, ПОДЛЕЖАЩЕЙ ПРЕДСТАВЛЕНИЮ В РС, И ОБЪЕМ ПРОВОДИМЫХ ИСПЫТАНИЙ

Таблица 1

Код объекта технического наблюдения	Объект технического наблюдения	При оформлении СТО	
		перечень документации	перечень испытаний
15140000	**Кибербезопасность**		
15141000	Оборудование обеспечения кибербезопасности судовых систем управления и автоматизации	D1, D2, T1, T2, I1 [МЭК 62443-4-1:2018, МЭК 62443-4-2:2019], I2[1]	12.6.1 — 12.6.16
05410000	**Оборудование обеспечения кибербезопасности радио- и навигационного оборудования**		
05411000	Узел сети 450	D1, D2, T1, T2, I1 [МЭК 61162-450:2018]	МЭК 60945:2002, 18.6.2.1
05412000	Узел сети 460	D1, D2, T1, T2, I1 [МЭК 61162-450:2018]	МЭК 60945:2002, 18.6.2.2
05413000	Коммутатор сети 460	D1, D2, T1, T2, I1 [МЭК 61162-450:2018]	МЭК 60945:2002, 18.6.2.3
05414000	Маршрутизатор сети 460	D1, D2, T1, T2, I1 [МЭК 61162-450:2018]	МЭК 60945:2002, 18.6.2.4
05415000	Шлюз сети 460	D1, D2, T1, T2, I1 [МЭК 61162-450:2018]	МЭК 60945:2002, 18.6.2.5
[1] для оборудования, устанавливаемого во взрывоопасной зоне.			

».