Общество с ограниченной ответственностью «Нума Технологии»

Утвержден

АМБН.465689.0013Б-ЛУ

Программно-аппаратный комплекс Numa Edge

Задание по безопасности

выписка

АМБН.465689.0013Б

3 Определение проблемы безопасности

Данный раздел содержит описание следующих аспектов решаемой с использованием МЭ проблемы безопасности:

– угроз безопасности, которым необходимо противостоять средствами ОО;

– политики безопасности организации, которой должен следовать ОО;

– предположений безопасности относительно предопределенного использования ОО и среды функционирования ОО.

3.1 Угрозы

3.1.1 Угрозы, которым должен противостоять объект оценки

В настоящем ЗБ определены следующие угрозы, которым необходимо противостоять средствами ОО.

Угроза-1

1. Аннотация угрозы – несанкционированный доступ к информации, содержащейся в информационной системе.

2. Источники угрозы – внешний нарушитель, внутренний нарушитель.

3. Способ реализации угрозы – установление сетевых соединений со средствами вычислительной техники информационной системы или между ее сегментами, не предусмотренных технологией обработки информации.

4. Используемые уязвимости – наличие неконтролируемых сетевых подключений к информационной системе или между ее сегментами, недостатки настройки механизмов защиты информации.

5. Вид информационных ресурсов, потенциально подверженных угрозе – пользовательские данные, данные функций безопасности.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность, целостность, доступность.

7. Возможные последствия реализации угрозы – несанкционированный доступ к информации ресурсам ОО, нарушение режимов функционирования ОО.

Угроза-2

1. Аннотация угрозы – отказ в обслуживании информационной системы и (или) ее отдельных компонентов.

2. Источники угрозы – внешний нарушитель.

3. Способ реализации угрозы – установление не предусмотренных технологией обработки информации в информационной системе сетевых соединений с информационной системой и (или) ее отдельными компонентами для отправки множества сетевых пакетов (запросов) до заполнения ими сетевой полосы пропускания канала передачи данных или отправки специально сформированных аномальных сетевых пакетов (запросов) больших

размеров или нестандартной структуры.

4. Используемые уязвимости – наличие неконтролируемых сетевых подключений к информационной системе или между ее сегментами, уязвимости сетевых протоколов, недостатки настройки механизмов защиты, уязвимости в программном обеспечении программно-аппаратных средств ОО.

5. Вид информационных ресурсов, потенциально подверженных угрозе – пользовательские данные, сервисы информационной системы.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Возможные последствия реализации угрозы – невозможность обработки запросов уполномоченных пользователей ОО; невозможность предоставления доступа к компонентам ОО.

Угроза-3

1. Аннотация угрозы – несанкционированная передача информации из информационных систем в информационно-телекоммуникационные сети или иные информационные системы.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – внедрение вредоносного программного обеспечения для несанкционированной отправки защищаемой информации на средства вычислительной техники нарушителя; отправка защищаемой информации на средства вычислительной техники нарушителя пользователем информационной системы.

4. Используемые уязвимости – наличие неконтролируемых сетевых подключений к информационной системе или между ее сегментами, недостатки настройки механизмов защиты.

5. Вид информационных ресурсов, потенциально подверженных угрозе – пользовательские данные, данные функций безопасности.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность.

7. Возможные последствия реализации угрозы – утечка защищаемой информации.

Угроза-4 **1. Аннотация угрозы –** несанкционированное воздействие на ОО, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – отправка специально сформированных сетевых пакетов на интерфейсы ОО, приводящих к отключению, обходу или преодолению механизмов защиты ОО, с использованием штатных средств, предоставляемых ОО, а также специализированных инструментальных средств.

4. Используемые уязвимости – недостатки средств защиты информации, применяемых в сегментах ОО; недостатки собственных защитных механизмов ОО; недостатки настройки функциональных возможностей безопасности ОО.

5. Вид информационных ресурсов, потенциально подверженных угрозе – функции безопасности ОО, данные функций безопасности МЭ.

6. Нарушаемые свойства безопасности информационных ресурсов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушения режимов функционирования ОО.

Угроза-5

1. Аннотация угрозы – несанкционированное получение сведений о сети информационной системы, а также о ее узлах.

2. Источники угрозы – внешний нарушитель.

3. Способ реализации угрозы – сканирование ресурсов информационной системы с использованием специализированных инструментальных средств.

4. Используемые уязвимости – недостатки средств защиты информации, применяемых в сегментах ОО; недостатки или отсутствие механизмов маскирования сегментов ОО; недостатки настройки функциональных возможностей безопасности ОО.

5. Вид информационных ресурсов, потенциально подверженных угрозе – данные о конфигурации системы, данные об уязвимостях информационной системы, данные о настройках применяемых средств защиты информации.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность.

7. Возможные последствия реализации угрозы – проведение нарушителем целевой атаки на ресурсы информационной системы.

3.1.2 Угрозы, которым противостоит среда

В настоящем ЗБ определены следующие угрозы, которым должна противостоять среда функционирования ОО:

Угроза среды-1

1. Аннотация угрозы – нарушение целостности ПО ОО, настроек ОО.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированный доступ к ОО с использованием штатных и нештатных средств.

4. Используемые уязвимости – недостатки механизмов управления доступом, физической защиты оборудования ОО;

недостатки механизмов защиты журналов аудита ОО.

5. Вид информационных ресурсов, потенциально подверженных угрозе – программное обеспечение ОО, данные функций безопасности ОО.

6. Нарушаемые свойства безопасности информационных ресурсов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, неэффективность работы ОО.

3.2 Политика безопасности организации

Политика безопасности-1	Должно обеспечиваться блокирование передачи защищаемой информации, сетевых запросов и трафика, несанкционированно исходящих из информационной системы и (или) входящих в информационную систему, путем фильтрации информационных потоков.
Политика безопасности-2	Должно осуществляться присвоение информации состояния соединения только допустимых значений.
Политика безопасности-3	Должна осуществляться возможность предоставлять разрешительные/запретительные атрибуты безопасности для используемых пользователями отдельных команд.
Политика безопасности-4	Должна обеспечиваться интерпретация управляющих сигналов от средств защиты информации и блокирование соответствующего трафика.
Политика безопасности-5	Должно осуществляться разграничение доступа к управлению ОО и параметрами ОО на основе ролей уполномоченных лиц.
Политика безопасности-6	Должна обеспечиваться возможность управления работой ОО и параметрами ОО со стороны администраторов ОО.
Политика безопасности-7	Должны обеспечиваться идентификация и аутентификация администраторов ОО.

Политика безопасности-8	Должны обеспечиваться идентификация и аутентификация субъектов межсетевого взаимодействия до передачи ОО информационного потока получателю.
Политика безопасности-9	Должны обеспечиваться механизмы регистрации о возможных нарушениях безопасности.
Политика безопасности-10	Должны обеспечиваться механизмы распределения собственных ресурсов, а также установки безопасного состояния ФБО или предотвращения их перехода в опасное состояние после сбоев, прерывания функционирования или перезапуска.
Политика безопасности-11	Должны обеспечиваться запрет прямого взаимодействия узлов через ОО, возможность проверки разрешительных или запретительных атрибутов информации (в заголовках пакетов протоколов прикладного уровня, в поле данных пакетов протоколов прикладного уровня).
Политика безопасности-12	Должна обеспечиваться кластеризация ОО.
Политика безопасности-13	Должна обеспечиваться приоритизация контроля и фильтрации разных информационных потоков, а также выделения ресурсов, доступных для разных информационных потоков, обрабатываемых одновременно (в течение определенного периода времени).

3.3 Предположения безопасности

Предположения, связанные с физическими аспектами среды функционирования

Предположение-1	Должна обеспечиваться физическая защита ОО и терминалов, с которых выполняется его управление.

Предположения по отношению к аспектам связности среды функционирования

Предположение-2 Должно обеспечиваться исключение каналов связи защищаемой информационной системы с иными информационными системами в обход ОО.

Предположение-3 Должен обеспечиваться доверенный канал передачи данных между защищаемой информационной системой и ОО, а также между ОО и терминалом, с которого выполняется его управление.

Предположение-4 Должен обеспечиваться доверенный маршрут между ОО и администраторами ОО.

Предположение-5 Должно обеспечиваться взаимодействие ОО с сертифицированными на соответствие требованиям безопасности информации по соответствующему классу защиты средствами защиты информации (системами обнаружения вторжений, средствами антивирусной защиты и другими), от которых ОО получает управляющие сигналы.

Предположение-6 Должны быть обеспечены совместимость компонентов МЭ с компонентами средств вычислительной техники информационной системы, а также необходимые ресурсы для выполнения функций безопасности МЭ (в том числе изоляция данных и процессов МЭ от иных данных и процессов средства вычислительной техники, на котором он функционирует).

Предположение-7 Должно быть обеспечено функционирование МЭ в среде, сертифицированной на соответствие требованиям безопасности информации по соответствующему классу защиты операционной системы, или в среде, защищенной путем принятия мер защиты информации, соответствующих классу защищенности информационной системы (автоматизированной системы управления), для

использования в которой предназначается МЭ.

Предположение-8 Должны быть обеспечены тестирование и контроль целостности аппаратных средств, а также программного обеспечения базовой системы ввода-вывода, загрузчика и операционной системы МЭ или средства вычислительной техники, на котором он функционирует.

Предположение-9 Должна быть исключена возможность использования не прошедших сертификацию компонентов программно-технического средства, в котором интегрирован МЭ с иными видами средств защиты информации, при его эксплуатации.

Предположения, связанные с персоналом среды функционирования

Предположение-10 Персонал, ответственный за функционирование ОО, должен обеспечивать установку, настройку и эксплуатацию ОО в соответствии с правилами по безопасной настройке и руководством пользователя (администратора).

4 Цели безопасности

В данном разделе определяются цели безопасности для ОО и среды его поддержки. ОО является функционально завершенным, и его правильное функционирование не зависит от каких-либо других продуктов ИТ, кроме ОС.

4.1 Цели безопасности для ОО

Цель безопасности-1 Управление информационными потоками	ОО должен обеспечивать блокирование передачи защищаемой информации, сетевых запросов и трафика, несанкционированно исходящих из ОО и (или) входящих в ОО, путем фильтрации информационных потоков.
Цель безопасности-2 Управление состоянием соединений	ОО должен обеспечивать присвоение информации состояния соединения только допустимых значений.
Цель безопасности-3 Управление атрибутами безопасности команд пользователей	ОО должен обеспечивать возможность предоставлять разрешительные (запретительные) атрибуты безопасности для используемых пользователями отдельных команд.
Цель безопасности-4 Взаимодействие МЭ с отдельными типами СЗИ	ОО должен обеспечивать возможность взаимодействия с отдельными типами СЗИ и интерпретацию результатов их работы при осуществлении фильтрации пакетов данных и блокирования соответствующего трафика.
Цель безопасности-5 Разграничение доступа к управлению МЭ	ОО должен обеспечивать разграничение доступа к управлению ОО и параметрами ОО на основе ролей администраторов ОО.
Цель безопасности-6 Управление МЭ	ОО должен обеспечивать возможность управления работой ОО и параметрами ОО со стороны администраторов ОО.

Цель безопасности-7 Идентификация и аутентификация администраторов МЭ	ОО должен обеспечивать идентификацию и аутентификацию администраторов ОО.
Цель безопасности-8 Идентификация и аутентификация субъектов межсетевого взаимодействия	ОО должен обеспечивать идентификацию и аутентификацию субъектов межсетевого взаимодействия до передачи ОО информационного потока получателю.
Цель безопасности-9 Аудит безопасности МЭ	ОО должен располагать механизмами регистрации о возможных нарушениях безопасности.
Цель безопасности-10 Обеспечение бесперебойного функционирования МЭ	ОО должен располагать механизмами распределения собственных ресурсов, а также устанавливать безопасное состояние ФБО или предотвращать их переход в опасное состояние после сбоев, прерывания функционирования или перезапуска.
Цель безопасности-11 Посредничество в передаче информации сетевого трафика	ОО должен обеспечивать возможность запрета прямого взаимодействия узлов через ОО, возможность проверки разрешительных или запретительных атрибутов информации (в заголовках пакетов протоколов прикладного уровня, в поле данных пакетов протоколов прикладного уровня).
Цель безопасности-12 Кластеризация	ОО должен обеспечивать возможность кластеризации ОО.
Цель безопасности-13 Приоритизация	ОО должен обеспечивать возможность приоритизации контроля и фильтрации разных информационных потоков, а также выделения ресурсов, доступных для разных информационных

потоков, обрабатываемых одновременно (в течение определенного периода времени).

4.2 Цели безопасности для среды функционирования

В данном разделе дается описание целей безопасности для среды функционирования ОО.

Цель для среды функционирования ОО-1 Обеспечение доверенного канала	Должен обеспечиваться доверенный канал передачи данных между защищаемой ИС и ОО, а также между ОО и терминалом, с которого выполняется управление им.
Цель для среды функционирования ОО-2 Обеспечение доверенного маршрута	Должен быть обеспечен доверенный маршрут между ОО и администраторами ОО.
Цель для среды функционирования ОО-3 Обеспечение условий безопасного функционирования	Должно обеспечиваться исключение каналов связи защищаемой ОО с иными ИС в обход ОО.
Цель для среды функционирования ОО-4 Физическая защита ОО	Должна обеспечиваться физическая защита ОО и терминалов, с которых выполняется его управление.
Цель для среды функционирования ОО-5 Взаимодействие с доверенными продуктами информационных технологий	Должно обеспечиваться взаимодействие ОО с сертифицированными на соответствие требованиям безопасности информации по соответствующему классу защиты СЗИ (системами обнаружения вторжений, средствами антивирусной защиты и другими), от которых ОО получает управляющие сигналы.

Цель для среды функционирования ОО-6 Эксплуатация ОО	Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с эксплуатационной документацией.
Цель для среды функционирования ОО-7 Требования к персоналу	Персонал, ответственный за функционирование ОО, должен обеспечивать функционирование ОО, руководствуясь эксплуатационной документацией.
Цель для среды функционирования ОО-8 Поддержка аудита	Должна быть обеспечена поддержка средств аудита, используемых в ОО, и предоставление для них источника меток времени.
Цель для среды функционирования ОО-9 Исключение недоверенных компонентов	Должна быть исключена возможность использования не прошедших сертификацию компонентов программно-технического средства, в котором интегрирован ОО с иными видами средств защиты информации, при его эксплуатации.
Цель для среды функционирования ОО-10 Совместимость компонентов МЭ с компонентами средств вычислительной техники	Должны быть обеспечены совместимость компонентов МЭ с компонентами средств вычислительной техники информационной системы, а также необходимые ресурсы для выполнения функций безопасности МЭ (в том числе изоляция данных и процессов МЭ от иных данных и процессов средства вычислительной техники, на котором он функционирует).
Цель для среды функционирования ОО-11 Доверенная среда функционирования	Должно быть обеспечено функционирование МЭ в среде, сертифицированной на соответствие требованиям безопасности информации по соответствующему классу защиты операционной системы, или в среде, защищенной путем принятия мер защиты информации, соответствующих классу защищенности

	информационной системы (автоматизированной системы управления), для использования в которой предназначается МЭ.
Цель для среды функционирования ОО-12 Тестирование и контроль целостности среды функционирования	Должны быть обеспечены тестирование и контроль целостности аппаратных средств, а также программного обеспечения базовой системы ввода-вывода, загрузчика и операционной системы МЭ или средства вычислительной техники, на котором он функционирует

4.3 Обоснование целей безопасности

4.3.1 Обоснование целей безопасности для ОО

В таблице 4.1 приведено отображение целей безопасности для ОО на угрозы и политики безопасности организации.

Таблица 4.1 – Отображение целей безопасности для ОО на угрозы и политики безопасности

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10	Цель безопасности-11	Цель безопасности-12	Цель безопасности-13
Угроза - 1	X	X	X					X			X		
Угроза - 2	X	X	X					X			X	X	X
Угроза - 3	X	X	X					X			X		
Угроза - 4					X	X	X		X	X		X	X
Угроза - 5												X	
Политика безопасности-1	X												

Продолжение таблицы 4.1

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10	Цель безопасности-11	Цель безопасности-12	Цель безопасности-13
Политика безопасности-2		X											
Политика безопасности-3			X										
Политика безопасности-4				X									
Политика безопасности-5					X								
Политика безопасности-6						X							
Политика безопасности-7							X						
Политика безопасности-8								X					
Политика безопасности-9									X				
Политика безопасности-10										X			

Продолжение таблицы 4.1

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10	Цель безопасности-11	Цель безопасности-12	Цель безопасности-13
Политика безопасности-11											X		
Политика безопасности-12												X	
Политика безопасности-13													X

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2, Угроза-3** и реализацией политики безопасности **Политика безопасности-1**, так как обеспечивает блокирование передачи защищаемой информации, сетевых запросов и трафика, несанкционированно исходящих из информационной системы и (или) входящих в информационную систему, путем фильтрации информационных потоков.

Цель безопасности-2

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-2, Угроза-3** и реализации политики безопасности **Политика безопасности-2,** так как обеспечивает присвоение информации состояния соединения только допустимых значений.

Цель безопасности-3

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-2, Угроза-3** и реализации политики безопасности **Политика безопасности-3,** так как обеспечивает возможность предоставлять

разрешительные/запретительные атрибуты безопасности для используемых пользователями отдельных команд.

Цель безопасности-4

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-4**, так как обеспечивает возможность взаимодействия с отдельными типами средств защиты информации и интерпретацию результатов их работы при осуществлении фильтрации пакетов данных и блокирования соответствующего трафика.

Цель безопасности-5

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-4** и реализации политики безопасности **Политика безопасности-5**, так как обеспечивает возможность разграничения доступа к управлению ОО и параметрами ОО со стороны уполномоченных лиц.

Цель безопасности-6

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-4** и реализации политики безопасности **Политика безопасности-6**, так как обеспечивает возможность управления режимами выполнения функций безопасности ОО и параметрами ОО.

Цель безопасности-7

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-4** и реализации политики безопасности **Политика безопасности-7**, так как обеспечивает идентификацию и аутентификацию администраторов ОО.

Цель безопасности-8

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-2, Угроза-3** и реализации политики безопасности **Политика безопасности-8**, так как обеспечивает идентификацию и аутентификацию субъектов межсетевого взаимодействия до передачи ОО информационного потока получателю.

Цель безопасности-9

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-4** и реализации политики безопасности **Политика безопасности-9,** так как обеспечивает возможность регистрации событий, относящихся к возможным нарушениям безопасности.

Цель безопасности-10

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-4** и реализации политики безопасности **Политика безопасности-10**, так как обеспечивает возможность устанавливать безопасное состояние ФБО или предотвращать их переход в опасное состояние после сбоев, прерывания функционирования или перезапуска.

Цель безопасности-11

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-2, Угроза-3, Угроза-5** и реализации политики безопасности **Политика безопасности-11**, так как обеспечивает возможность устанавливать запрет прямого взаимодействия узлов через ОО, возможность проверки разрешительных или запретительных атрибутов информации.

Цель безопасности-12

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-2, Угроза-4** и реализации политики безопасности **Политика безопасности-12,** так как обеспечивает возможность кластеризации ОО.

Цель безопасности-13

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-2, Угроза-4** и реализации политики безопасности **Политика безопасности-13,** так как обеспечивает возможность приоритизации контроля и фильтрации разных информационных потоков, а также выделения ресурсов, доступных для разных информационных потоков, обрабатываемых одновременно (в течение определенного периода времени).

4.3.2 Обоснование целей безопасности для среды функционирования

В таблице 4.2 приведено отображение целей безопасности для среды на

предположения безопасности.

Таблица 4.2 – Отображение целей безопасности для среды на аспекты среды безопасности

	Аспекты среды безопасности										
	Угроза среды-1	**Предположение-1**	**Предположение-2**	**Предположение-3**	**Предположение-4**	**Предположение-5**	**Предположение-6**	**Предположение-7**	**Предположение-8**	**Предположение-9**	**Предположение-10**
Цель для среды функционирования ОО-1				X							
Цель для среды функционирования ОО-2					X						
Цель для среды функционирования ОО-3			X								
Цель для среды функционирования ОО-4	X	X									
Цель для среды функционирования ОО-5	X					X					
Цель для среды функционирования ОО-6											X
Цель для среды функционирования ОО-7											X
Цель для среды функционирования ОО-8	X										
Цель для среды функционирования ОО-9										X	
Цель для среды функционирования ОО-10							X				
Цель для среды функционирования ОО-11								X			
Цель для среды функционирования ОО-12									X		

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией

предположения безопасности **Предположение-3**, так как обеспечивает доверенный канал передачи данных между защищаемой ИС и ОО, а также между ОО и терминалом, с которого выполняется управление им.

Цель для среды функционирования ОО-2

Достижение этой цели безопасности необходимо в связи с реализацией редположения безопасности **Предположение-4**, так как обеспечивает оверенный маршрут между ОО и администраторами ОО.

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-2**, так как обеспечивает условия безопасного функционирования.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1** и противостоянием угрозе безопасности для среды **Угроза среды-1**, так как обеспечивает физическую защиту ОО (или СВТ, на котором он функционирует) и терминалов, с которых выполняется его управление.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-5** и противостоянием угрозе безопасности для среды **Угроза среды-1**, так как обеспечивает взаимодействие МЭ с сертифицированными на соответствие требованиям безопасности информации по соответствующему классу защиты СЗИ, от которых ОО получает управляющие сигналы.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-10**, так как обеспечивает

установку, настройку и управление атрибутами безопасности в соответствии с эксплуатационной документацией.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо с реализацией предположение безопасности **Предположение-10**, так как обеспечивается благонадежное выполнении обязанностей персоналом ответственным за функционирование ОО.

Цель для среды функционирования ОО-8

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза среды-1**, так как обеспечивается поддержка средств аудита, используемых в ОО.

Цель для среды функционирования ОО-9

Достижение этой цели безопасности необходимо с реализацией предположение безопасности **Предположение-9**, так как обеспечивается исключение возможности использования не прошедших сертификацию компонентов программного или программно-технического средства, в котором интегрирован ОО с иными СЗИ, при его эксплуатации.

Цель для среды функционирования ОО-10

Достижение этой цели безопасности необходимо с реализацией предположение безопасности **Предположение-6**, так как обеспечивается совместимость компонентов ОО с компонентами СВТ ИС, а также необходимые ресурсы для выполнения функций безопасности ОО (в том числе изоляция данных и процессов ОО от иных данных и процессов СВТ, на котором он функционирует).

Цель для среды функционирования ОО-11

Достижение этой цели безопасности необходимо с реализацией предположение безопасности **Предположение-7**, так как обеспечивается

функционирование ОО в среде, сертифицированной на соответствие требованиям безопасности информации по соответствующему классу защиты операционной системы, или в среде, защищенной путем принятия мер защиты информации, соответствующих классу защищенности ИС (автоматизированной системы управления), для использования в которой предназначается ОО.

Цель для среды функционирования ОО-12

Достижение этой цели безопасности необходимо с реализацией предположение безопасности **Предположение-8**, так как обеспечивается тестирование и контроль целостности аппаратных средств, а также программного обеспечения базовой системы ввода-вывода, загрузчика и операционной системы ОО или СВТ, на котором он функционирует.

Общество с ограниченной ответственностью «Нума Технологии»

Утвержден

АМБН.465689.001ТУ–ЛУ

Программно-аппаратный комплекс Numa Edge

Технические условия

АМБН.465689.001ТУ

Содержание

Настоящие технические условия (далее – ТУ) распространяются на программно-аппаратный комплекс Numa Edge АМБН.465689.001 (далее – Изделие), производимый ООО «НумаТех».

Изделие является программно-техническим межсетевым экраном, реализующим в информационно-телекоммуникационных сетях (сетях передачи данных, использующих семейство протоколов TCP/IP) функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков.

Изделие предназначено для использования в составе информационных систем в целях защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа к ней.

Изделие может применяться как на физической, так и на логической границе информационной системы, а также между физическими или логическими границами сегментов информационной системы.

Изделие может применяться:

– в государственных информационных системах до 1 класса защищенности в соответствии с требованиями документа «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (введен в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г.);

– в информационных системах для обеспечения до 1 уровня защищенности персональных данных в соответствии с требованиями документа «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (введен в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г.);

– в системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а

также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);

– при защите значимых объектов критической информационной инфраструктуры до первой категории включительно (Приказ ФСТЭК от 25декабря 2017 г № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

Изделие поставляется в одном из 14 аппаратных исполнений. Технические характеристики аппаратных исполнений Изделия указаны в документе «Формуляр» АМБН.465689.001ФО.

Пример записи при заказе Изделия: Программно-аппаратный комплекс Numa Edge X Y АМБН.465689.001, где X – модель аппаратного исполнения Изделия, Y – условный тип предустановленного программного обеспечения.

Настоящий документ разработан в соответствии с ГОСТ 2.114-2016.

1 Технические требования

1.1 Основные параметры и характеристики

1.1.1 Программно-аппаратный комплекс Numa Edge АМБН.465689.001 должен соответствовать требованиям настоящих технических условий.

1.1.2 Изделие должно соответствовать требованиям руководящего документа «Требования к межсетевым экранам» (ФСТЭК России, 2016 г.), а также методическим документам «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016 г.) и «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016 г.), а также Задания по безопасности АМБН.465689.001ЗБ, «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденного приказом ФСТЭК России от 02 июня 2020 г. № 76 по 4 уровню доверия.

1.1.3 Изделие предназначено для обеспечения безопасности информации и управления информационными потоками в сетях передачи данных (локальных вычислительных сетях) информационных систем и их сегментов, использующих протоколы семейства TCP/IP.

1.1.4 Изделие должно реализовывать следующие функции безопасности, в соответствии с требованиями документов: «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), а также «Задания по безопасности» 643.АМБН.465689.001ЗБ с расширенными компонентами функциональных требований безопасности:

- контроль и фильтрация;
- идентификация и аутентификация;

– регистрация событий безопасности (аудит);

– обеспечение бесперебойного функционирования и восстановление;

– тестирование и контроль целостности;

– преобразование сетевых адресов;

– маскирование;

– приоритизация информационных потоков;

– управление (администрирование);

– взаимодействие с другими средствами защиты информации.

1.1.5 Изделие должно обеспечивать реализацию следующих функций необходимых для работ в сетях передачи данных корпоративного уровня:

– функционирование в режиме маршрутизации;

– возможность объединения сетевых интерфейсов в «сетевой мост»;

– статическая маршрутизация;

– динамическая маршрутизация с поддержкой протоколов RIP, OSPF, BGP;

– маршрутизация на основании политик (Policy-Based Routing);

– множественные таблицы маршрутизации – резервирование каналов и балансировка нагрузки;

– маршрутизация многоадресных передач;

– построение туннелей (с применением протоколов GRE, IP-IP, SIT);

– агрегация (объединение) сетевых интерфейсов (в том числе статическое или с применением протокола LACP);

– сервисы DHCP и DNS;

– ретрансляция DHCP запросов (DHCP-relay);

– поддержка протокола SNMP (Simple Network Management Protocol);

– модификация сетевого трафика в соответствии с заданными политиками;

– клонирование сетевого трафика в соответствии с заданными

политиками;

– трансляция сетевых адресов и портов (NAT/PAT);

– регистрация статистики сетевого трафика, включая нагрузку, типы проходящих пакетов, отправителей и получателей сетевого трафика;

– передача статистики сетевого трафика на внешние сервисы-коллекторы по протоколам NetFlow и sFlow.

1.1.6 В дополнение к функциям безопасности, заявленным в подразделах 1.1.4-1.1.5 настоящих технических условий СКЗИ «МагПро КриптоПакет» версия 4.0 СЕИУ.00009-05 (исполнение 7, исполнение 8), предустановленное в программно-аппаратный комплекс Numa Edge АМБН.465689.001 с программным обеспечением «Межсетевой экран Numa Edge версия 1.0» 643.АМБН.00004-01 (исполнение 2), обеспечивает:

– создание и проверку электронной подписи в соответствии с ГОСТ Р 34.10 для файлов и данных, содержащихся в областях оперативной памяти;

– зашифрование и расшифрование в соответствии с ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и ГОСТ 28147-89 (только для взаимодействия с ПО, не поддерживающим ГОСТ Р 34.12-2015) фалов и данных, содержащихся в областях оперативной памяти;

– имитозащиту в соответствии с ГОСТ Р 34.13-2015, HMAC на основе ГОСТ Р 34.11-2012, а также ГОСТ 28147-89 (только для взаимодействия с ПО, не поддерживающим ГОСТ Р 34.13-2015) фалов и данных, содержащихся в областях оперативной памяти;

– вычисление ключа парной связи по алгоритму VKO с использованием как эфемерных, так и долговременных пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10;

– вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11 для файлов и данных, содержащихся в областях оперативной памяти;

– выработку случайного числа заданной длины;

– вычисление открытых и закрытых ключей проверки подписи в

соответствии с ГОСТ Р 34.10;

– формирование производного сеансового ключа;

– импорт криптографических ключей в СКЗИ и их экспорт из СКЗИ;

– реализацию протокола TLS с использованием российских криптонаборов, определенных реализациями ТК26.

1.1.7 ПАК Numa Edge реализован и поставляется в одном из 14 аппаратных исполнений, реализованных на аппаратных платформах с предустановленным программным обеспечением «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01) в одном из двух исполнений, описанных в таблице 1.

Таблица 1 – Типы исполнений ПО, устанавливаемых в ПАК Numa Edge

Условный номер исполнения ПО	Условный тип исполнения ПО	Наименование ПО
Исполнение 1	FW	программное обеспечение «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01)
Исполнение 2	VPN	программное обеспечение «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01) с предустановленным СКЗИ «МагПро КриптоПакет» версия 4.0 СЕИУ.00009-05 исполнение 7, исполнение 8

Состав аппаратных исполнений приведен таблице 2.

Таблица 2 – Состав аппаратных исполнений Изделия

Условный номер аппаратного исполнения Изделия	Модель аппаратного исполнения Изделия в соответствии с номенклатурой производителя
Исполнение 1	Numa Edge-10
Исполнение 2	Numa Edge-25
Исполнение 3	Numa Edge-50
Исполнение 4	Numa Edge-55
Исполнение 5	Numa Edge-100
Исполнение 6	Numa Edge-200
Исполнение 7	Numa Edge-1000

Условный номер аппаратного исполнения Изделия	Модель аппаратного исполнения Изделия в соответствии с номенклатурой производителя
Исполнение 8	Numa Edge-1100
Исполнение 9	Numa Edge-2000
Исполнение 10	Numa Edge-3000
Исполнение 11	Numa Edge 40R
Исполнение 12	Numa Edge 100R
Исполнение 13	Numa Edge 180R
Исполнение 14	Numa Edge 25R

1.1.8 Комплектация аппаратных исполнений Изделия представлены в таблице 3.

Таблица 3 – Комплектация аппаратных исполнений Изделия

Модель аппаратного исполнения	Комплектация аппаратных исполнений Изделия
Numa Edge 10	Компьютер NCA-1010B на базе процессора Intel Atom E3825, с оперативной памятью типа DDR3L 1067 МГц до 8 Гбайт, встроенные интерфейсы 3 x RJ45 GbE, порты ввода-вывода 1 x USB 2.0, 1 x USB 3.0, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 25	Компьютер NCA-1210B на базе процессора Intel Atom C2358, оперативной памятью типа DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 4 x RJ45 GbE, порты ввода-вывода 2 x USB type A, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 25R	Мини-компьютер АТБ-АТОМ-1 (модель АТБ-АТОМ-1.3) на базе процессора Intel Atom E3845, оперативной памятью типа 1 x DDR3L 1333 / 1600 MHz до 8 Гб, встроенные сетевые интерфейсы 3 x 2.5GbE; консольный порт 1 x RS-232C (RJ-45), интерфейс USB: 1 x USB 2.0, 1 x USB 3.0; 1 x HDMI порт; внешний источник питания
Numa Edge 40R	Сервер «Аквариус» T30 S100DC на базе процессора Intel Atom 3338 Series, чипсет Intel C3000, оперативная память типа DDR4 1866/2400 МГц до 32 Гбайт, встроенные интерфейсы 2 x USB 3.0 Type A, 1 x Консоль RS232, 1 x Вывод Com для Lcp, 1 x Разъем

Модель аппаратного исполнения	Комплектация аппаратных исполнений Изделия
	VGA, 4 × 1GbE RJ-45, 2 x 1GbE SFP, внешний блок питания.
Numa Edge 50	Компьютер FW-7551SED на базе процессора Intel Atom C2558, оперативной памятью типа 2 x DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 6 x RJ45, порты ввода-вывода 2 x USB 2.0, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 55	Компьютер FW-7551SEB на базе процессора Intel Atom C2558, оперативной памятью типа 2 x DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 4 x RJ45 GbE и 2 x SFP GbE, порты ввода-вывода 2 x USB 2.0, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 100	Компьютер FW-7573B на базе процессора Intel Atom C2518, оперативной памятью типа 2 x DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 6 x RJ45 GbE, 1 модуль расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 100R	Сервер «Аквариус» T30 S001DC на базе процессора Intel Atom 3558 Series, чипсет Intel C3000, оперативная память типа DDR4 1866/2400 МГц до 32 Гбайт, встроенные интерфейсы 2 x USB 3.0 Type A, 1 x Консоль RS232, 1 x Вывод Com для Lcp, 1 x Разъем VGA, 4 × 1GbE RJ-45, 2 x 1GbE SFP, одинарный/сдвоенный блок питания.
Numa Edge 180R	Сервер «Аквариус» T30 S001DC на базе процессора Intel Atom 3758Series, чипсет Intel C3000, оперативная память типа DDR4 1866/2400 МГц до 32 Гбайт, встроенные интерфейсы 2 x USB 3.0 Type A, 1 x Консоль RS232, 1 x Вывод Com для Lcp, 1 x Разъем VGA, 4 × 1GbE RJ-45, 2 x 1GbE SFP, одинарный/сдвоенный блок питания.
Numa Edge 200	Компьютер NCA-4210B на базе процессора Intel Skylake/Kabylake/ Intel Xeon E3, чипсетом C236, оперативной памятью типа 2 x DDR4 2400 МГц до 32 Гбайт, встроенные интерфейсы 6 x RJ45 GbE и 2 x SFP,1 модуль расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 3.0, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 1000	Компьютер NCA-5210B на базе процессора Intel Skylake/Kabylake/ Intel Xeon E3, с чипсетом C236, оперативной памятью типа DDR4 2400 МГц до 64 Гбайт, встроенные интерфейсы 12 x RJ45 GbE, 4 x

Модель аппаратного исполнения	Комплектация аппаратных исполнений Изделия
	SFP GbE, 2 модуля расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, IPMI, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 1100	Компьютер NCA-5210C на базе процессора Intel Skylake/Kabylake/ Intel Xeon E3, с чипсетом C236, оперативной памятью типа DDR4 2400 МГц до 64 Гбайт, 4 модуля расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, IPMI, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 2000	Компьютер FW-5510A на базе процессора Intel Xeon E5, чипсетом C612, оперативной памятью типа DDR4 1600/1866/2133 МГц до 256 Гбайт, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, служебный порт RJ45, 4 модуля расширения опционально, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 3000	Компьютер FW-8894 на базе процессора Intel Xeon E5, чипсетом C612, оперативной памятью типа DDR4 2133 МГц до 512 Гбайт, 4 модуля расширения, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, IPMI, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов

В таблице 4 приведены модули расширения, доступные для опционального комплектования аппаратных исполнений Изделия. Необходимость установки модулей расширения определяется Заказчиком при размещении заказа на производство Изделия.

Таблица 4 – Модули расширения аппаратных исполнений Изделия

Модель модуля расширения	Edge-M1C4	Edge-M1C8	Edge-M1F4	Edge-M1F8	Edge-M10F2	Edge-M10F4	Edge-M40F2	Edge-R10F4	Edge-R1C4	Edge-R1C8
Описание модуля	4 порта RJ-45 1 Gb	8 портов RJ-45 1 Gb	4 порта SFP 1 Gb	8 портов SFP 1 Gb	2 порта SFP+ 10 Gb	4 порта SFP+ 10 Gb	2 порта QSFP+ 40 Gb	4 порта 10GbE SFP+	4 порта RJ-45 1GE	8 портов RJ45 1GE
Numa Edge 10	-	-	-	-	-	-	-	-	-	-
Numa Edge 25	-	-	-	-	-	-	-	-	-	-

Модель модуля расширения	Edge-M1C4	Edge-M1C8	Edge-M1F4	Edge-M1F8	Edge-M10F2	Edge-M10F4	Edge-M40F2	Edge-R10F4	Edge-R1C4	Edge-R1C8
Numa Edge 25R	-	-	-	-	-	-	-	-	-	-
Numa Edge 40R	-	-	-	-	-	-	-	-	-	-
Numa Edge 50	-	-	-	-	-	-	-	-	-	-
Numa Edge 55	-	-	-	-	-	-	-	-	-	-
Numa Edge 100	+	+	+	+	+	+	+	-	-	-
Numa Edge 100R	-	-	-	-	-	-	-	+	+	+
Numa Edge 180R	-	-	-	-	-	-	-	+	+	+
Numa Edge 200	+	+	+	+	+	+	+	-	-	-
Numa Edge 1000	+	+	+	+	+	+	+	-	-	-
Numa Edge 1100	+	+	+	+	+	+	+	-	-	-
Numa Edge 2000	+	+	+	+	+	+	+	-	-	-
Numa Edge 3000	+	+	+	+	+	+	+	-	-	-

поставляется с предустановленным микропрограммным обеспечением базовой системы ввода вывода Numa BIOS 643.АМБН.00001-01 (далее – МПО БСВВ).

БСВВ Numa BIOS 643.АМБН.00001-01 включен в единый реестр российских программ для электронных вычислительных машин и баз данных (Реестровая запись №5467 от 24.06.2019 произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.06.2019 №335).

1.1.9 Контрольные суммы предустановленного в ПАК Numa Edge АМБН.465689.001 ПО «Межсетевой экран Numa Edge версия 1.0» должны иметь значение, указанное в таблице 5 документа «Формуляр» АМБН.465689.001ФО.

1.1.10 Программная часть Изделия 643.АМБН.00004-01 должна соответствовать требованиям раздела 3 «Требования к программе» документа «Программа и методика испытаний» 643.АМБН.00004-01 51 01.

1.1.11 Аппаратные платформы должны быть работоспособными.

1.2 Комплектность

1.2.1 Комплектность Изделия в каждом конкретном случае определяется договором поставки Изделия Заказчику.

1.2.2 При приемке и поставке Изделия должна проверяться его комплектность, в которую входят Изделия и документы, приведенные в таблице 5.

Таблица 5 – Комплектность Изделия

Обозначение	Наименование	Количество	Примечание
Изделие			
АМБН.465689.001	Программно-аппаратный комплекс Numa Edge		
Документация*			
АМБН.465689.001ФО	Программно-аппаратный комплекс Numa Edge. Формуляр		В печатном виде
АМБН.465689.001ФО-1	Программно-аппаратный комплекс Numa Edge. Формуляр. Приложение		На компакт-диске
АМБН.465689.001ПС	Программно-аппаратный комплекс Numa Edge. Паспорт		В печатном виде
643.АМБН.00004-01 32 01	Руководство администратора		На компакт-диске
643.АМБН.00004-01 32 02	Руководство администратора. Построение виртуальных частных сетей (VPN) на основе протокола OpenVPN		На компакт-диске. **
643.АМБН.00004-01 32 03	Руководство администратора. Краткое руководство по настройке		В печатном виде
643.АМБН.00004-01 32 04	Руководство администратора. Построение частных сетей на основе набора протоколов IPSec		На компакт-диске. **
643.АМБН.00004-01 32 05	Руководство администратора. Использование FTP proxy		На компакт-диске
643.АМБН.00004-01 32 06	Руководство администратора. Настройка Socks Proxy		На компакт-диске
643.АМБН.00004-01 32 07	Руководство администратора. Туннелирование IP		На компакт-диске
643.АМБН.00004-01 32 08	Руководство администратора.		На компакт-

Обозначение	Наименование	Количество	Примечание
	Настройка VPN с использованием протоколов PPTP и L2TP/IPSec		диске**
643.АМБН.00004-01 32 09	Руководство администратора. Настройка LVS		На компакт-диске
643.АМБН.00004-01 32 10	Руководство администратора. Мониторинг и сигнализация неисправностей оборудования		На компакт-диске
643.АМБН.00004-01 88 01	Инструкция по проверке контрольных сумм		На компакт-диске
б/н	Установка и настройка утилиты numa-ssh		На компакт-диске
б/н	Сервисный сертификат		В печатном виде
№4199 от 26.12.2019	Копия сертификата соответствия ФСТЭК России на ПАК Numa Edge		В печатном виде
СЕИУ.00009-05 30	СКЗИ «МагПро КриптоПакет» версия 4.0. Формуляр		В печатном виде. **
б/н	Комплект документации для СКЗИ «МагПро КриптоПакет» версия 4.0		На компакт-диске. **
№СФ/114-4205 от 21.01.2022 №СФ/124-4260 от 21.01.2022	Копия сертификата соответствия ФСБ России на СКЗИ «МагПро КриптоПакет»		В печатном виде. **
Материалы			
643.АМБН.00004-01	Установочный пакет программного обеспечения «Межсетевой экран Numa Edge версия 1.0»		На компакт-диске
б/н	Коммуникационная программа ssh		На компакт-диске
б/н	Компакт-диск с документацией для ПАК Numa Edge		
б/н	Компакт-диск с дистрибутивом и документацией на СКЗИ «МагПро КриптоПакет» версия 4.0		**
* Примечание. Итоговый комплект документации к Изделию зависит от договора поставки. ** Только для ПАК Numa Edge с предустановленным программным обеспечением «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01) Исполнение 2.			

1.3 Маркировка

1.3.1 Маркировка и упаковка Изделия должна производиться в соответствии с «Инструкцией по маркировке и упаковке» 643.АМБН.00004-01 91 01 и «Инструкции по маркировке и упаковке» АМБН.465689.001И1.

1.3.2 Маркировка Изделия должна соответствовать требованиям технической документации изготовителя и должна включать в себя:

- обозначение товарного знака изготовителя;
- наименования Изделия;
- идентификатора СЗИ;
- заводского номера Изделия;
- дата изготовления.

Примечания.

1. Идентификатор СЗИ – идентификатор средства защиты информации, является уникальным параметром для каждой поставки Изделия, который:

- *содержится в Лицензионном сертификате;*
- *наносится на электронные носители, содержащие Изделие;*
- *указывается в формуляре Изделия;*

Идентификатор СЗИ имеет следующий формат РОСС RU.0001.4199.XXXXXX, где:

- *первая группа знаков содержит прописные буквы и цифры РОСС RU.0001, указывающие на систему сертификации ФСТЭК России;*
- *вторая группа знаков указывает на номер сертификата соответствия Изделия в системе сертификации ФСТЭК России;*
- *третья группа знаков указывает на номер лицензии в системе учета средств защиты информации, произведенных ООО «НумаТех».*

1.3.3 При маркировке Изделия на поверхности корпуса размещают маркировку с информацией о:

- наименование изготовителя;
- условное наименование Изделия;
- идентификатор СЗИ;
- заводской номер Изделия;
- дата производства Изделия.

1.3.4 При маркировке компакт-диска Изделия с ПО и эксплуатационной документацией на внешнюю часть наносят информацию о:

- наименовании Изделия;
- децимальный номер Изделия;
- идентификатор СЗИ;
- заводской номер Изделия;
- номер экземпляра.

1.3.5 Сертифицированное Изделие должен маркироваться идентификатором СЗИ. Идентификатор СЗИ должен быть указан:

- в подразделе 2.1, разделе 7 Формуляра АМБН.465689.001ФО;
- на компакт-диске с ПО и эксплуатационной документацией;
- на поверхности корпуса Изделия.

Идентификатор СЗИ должен регистрироваться ООО «НумаТех» в «Журнале учета выпущенных Изделий и учета идентификаторов СЗИ».

Номер экземпляра Изделия должен наноситься на электронный носитель, и приводиться в разделе 16 Формуляра АМБН.465689.001ФО.

1.4 Упаковка

1.4.1 Изделие упаковывается в тару изготовителя.

1.4.2 Упаковка Изделия должна обеспечивать выполнение требований по транспортированию и хранению в соответствии с ТУ.

1.4.3 Тара должна выдерживать без нарушения целостности конструкции воздействие механических нагрузок и климатических факторов, обеспечивать защиту упакованного в неё Изделия.

1.4.4 Упаковке подлежит укомплектованное Изделие, прошедшее приемо-сдаточные испытания.

Общество с ограниченной ответственностью «Нума Технологии»

УТВЕРЖДЕН
АМБН.465689.001ФО-ЛУ

Программно-аппаратный комплекс Numa Edge

Формуляр

АМБН.465689.001ФО

Листов 24

2023

Литера

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Формуляр является эксплуатационным документом, удостоверяющим гарантированные изготовителем основные характеристики программно-аппаратного комплекса Numa Edge АМБН.465689.001 (далее – Numa Edge или Изделие), определяющим комплектность поставки и содержащим данные, необходимые в период его эксплуатации.

1.2. Формуляр должен находиться в подразделении, ответственном за эксплуатацию Изделия.

1.3. Все записи в формуляре должны производиться чернилами или пастой черного, фиолетового или синего цвета четко и аккуратно и заверяться подписью лица, ответственного за ведение формуляра. Исправления записей должны быть оговорены и засвидетельствованы подписью лица, внесшего исправления, и скреплены печатью. Помарки, подчистки и незаверенные исправления не допускаются.

1.4. Правильность и своевременность заполнения формуляра контролируется ответственными должностными лицами.

1.5. Разделы 2, 4, 5, 6, 15 и 16 данного документа заполняются изготовителем, а разделы 7 и 12-14 при эксплуатации Изделия.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Сведения об Изделии:

Наименование Изделия: программно-аппаратный комплекс Numa Edge
Обозначение: АМБН.465689.001
Дата изготовления:
Наименование изготовителя: ООО «НумаТех»
Адрес: 196084, г. Санкт-Петербург, ул. Цветочная, д. 18, литера А, Бизнес-центр «Бизнес-Парк», оф. 424
Идентификатор СЗИ:
Заводской номер:
Исполнение предустановленного ПО:
Наименование страны производителя: Россия
Примечание.

Идентификатор СЗИ – идентификатор средства защиты информации, является уникальным параметром для каждого экземпляра Изделия, и при этом:

– *наносится на Изделие;*

– *указывается в формуляре Изделия.*

Идентификатор СЗИ имеет следующий формат РОСС RU.0001.4199.XXXXXX, где:

– *первая группа знаков содержит прописные буквы и цифры РОСС RU.0001, указывающие на систему сертификации ФСТЭК России;*

– *вторая группа знаков указывает на номер сертификата соответствия Изделия в системе сертификации ФСТЭК России;*

– *третья группа знаков указывает на номер лицензии в системе учета средств защиты информации, произведенных ООО «НумаТех».*

2.2. Изделие является программно-техническим межсетевым экраном, реализующим в информационно-телекоммуникационных сетях (сетях передачи данных, использующих семейство протоколов TCP/IP) функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков.

2.3. Изделие сертифицировано в системе сертификации средств защиты информации по требованиям безопасности информации ФСТЭК России № РОСС RU.0001.01БИ00 и является межсетевым экраном типа «А» четвертого класса защиты и межсетевым экраном типа «Б» четвертого класса защиты.

2.4. Согласно сертификату соответствия требованиям по безопасности информации №4199 (выдан ФСТЭК России от 26.12.2019 г.) программно-аппаратный комплекс соответствует требованиям документов:

– «Требования к межсетевым экранам», утвержденные приказом ФСТЭК России от 9 февраля 2016 г. № 9;

– «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016);

– «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016);

– Задание по безопасности АМБН.465689.0013Б;

– «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденного приказом ФСТЭК России от 02 июня 2020 г. № 76 по 4 уровню доверия.

– при выполнении указаний по эксплуатации, приведённых в разделе 11 настоящего формуляра.

2.5. Изделие может применяться:

– в государственных информационных системах до 1 класса защищенности в соответствии с требованиями документа «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (введен в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г.);

– в информационных системах для обеспечения до 1 уровня защищенности персональных данных в соответствии с требованиями документа «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (введен в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г.);

– в системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);

– при защите значимых объектов критической информационной инфраструктуры до первой категории включительно (Приказ ФСТЭК от 25 декабря 2017 г № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1. Состав исполнений Изделия

3.1.1. ПАК Numa Edge поставляется в одном из 14 аппаратных исполнений, реализованных на аппаратных платформах с предустановленным программным обеспечением «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01) в одном из двух исполнений, описанных в таблице 1.

Таблица 1 – Типы исполнений ПО, устанавливаемых в ПАК Numa Edge

Условный номер исполнения ПО	Условный тип исполнения ПО	Наименование ПО
Исполнение 1	FW	программное обеспечение «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01)
Исполнение 2	VPN	программное обеспечение «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01) с предустановленным СКЗИ «МагПро КриптоПакет» версия 4.0 СЕИУ.00009-05 исполнение 7, исполнение 8

Программное обеспечение «Межсетевой экран Numa Edge версия 1.0» 643.АМБН.00004-01 зарегистрировано в реестре отечественного ПО за регистрационным номером № 7123 от 03.11.2020 г. запись произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 30.10.2020 №567.

Состав аппаратных исполнений приведен таблице 2.

Таблица 2 – Состав аппаратных исполнений Изделия

Условный номер аппаратного исполнения Изделия	Модель аппаратного исполнения Изделия в соответствии с номенклатурой производителя
Исполнение 1	Numa Edge 10
Исполнение 2	Numa Edge 25
Исполнение 3	Numa Edge 50
Исполнение 4	Numa Edge 55
Исполнение 5	Numa Edge 100
Исполнение 6	Numa Edge 200
Исполнение 7	Numa Edge 1000
Исполнение 8	Numa Edge 1100
Исполнение 9	Numa Edge 2000
Исполнение 10	Numa Edge 3000
Исполнение 11	Numa Edge 40R
Исполнение 12	Numa Edge 100R
Исполнение 13	Numa Edge 180R
Исполнение 14	Numa Edge 25R

Характеристики аппаратных платформ приведены в таблице 3.

Таблица 3 – Комплектность аппаратных исполнений Изделия

Модель аппаратного исполнения	Комплектация аппаратных исполнений Изделия
Numa Edge 10	Компьютер Lanner NCA-1010B на базе процессора Intel Atom E3825, с оперативной памятью типа DDR3L 1067 МГц до 8 Гбайт, встроенные интерфейсы 3 x RJ45 GbE, порты ввода-вывода 1 x USB 2.0, 1 x USB 3.0, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 25	Компьютер Lanner NCA-1210B на базе процессора Intel Atom C2358, оперативной памятью типа DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 4 x RJ45 GbE, порты ввода-вывода 2 x USB type A, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 25R	Мини-компьютер АТБ-АТОМ-1 (модель АТБ-АТОМ-1.3) на базе процессора Intel Atom E3845, оперативной памятью типа 1 x DDR3L 1333 / 1600 MHz до 8 Гб, встроенные сетевые интерфейсы 3 x 2.5GbE; консольный порт 1 x RS-232C (RJ-45), интерфейс USB: 1 x USB 2.0, 1 x USB 3.0; 1 x HDMI порт; внешний источник питания.
Numa Edge 40R	Сервер «Аквариус» T30 S100DC на базе процессора Intel Atom 3338 Series, чипсет Intel C3000, оперативная память типа DDR4 1866/2400 МГц до 32 Гбайт, встроенные интерфейсы 2 x USB 3.0 Type A, 1 x Консоль RS232, 1 x Вывод Com для Lcp, 1 x Разъем VGA, 4 × 1GbE RJ-45, 2 x 1GbE SFP, внешний блок питания.
Numa Edge 50	Компьютер Lanner FW-7551SED на базе процессора Intel Atom C2558, оперативной памятью типа 2 x DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 6 x RJ45, порты ввода-вывода 2 x USB 2.0, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 55	Компьютер Lanner FW-7551SEB на базе процессора Intel Atom C2558, оперативной памятью типа 2 x DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 4 x RJ45 GbE и 2 x SFP GbE, порты ввода-вывода 2 x USB 2.0, 1 x RJ45; служебный порт RJ45, внешний блок питания
Numa Edge 100	Компьютер Lanner FW-7573B на базе процессора Intel Atom C2518, оперативной памятью типа 2 x DDR3 1333/1600 МГц до 16 Гбайт, встроенные интерфейсы 6 x RJ45 GbE, 1 модуль расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 100R	Сервер «Аквариус» T30 S001DC на базе процессора Intel Atom 3558 Series, чипсет Intel C3000, оперативная память типа DDR4 1866/2400 МГц до 32 Гбайт, встроенные интерфейсы 2 x USB 3.0 Type A, 1 x Консоль RS232, 1 x Вывод Com для Lcp, 1 x Разъем VGA, 4 × 1GbE RJ-45, 2 x 1GbE SFP, одинарный/сдвоенный блок питания.
Numa Edge 180R	Сервер «Аквариус» T30 S001DC на базе процессора Intel Atom 3758Series, чипсет Intel C3000, оперативная память типа DDR4 1866/2400 МГц до 32 Гбайт, встроенные интерфейсы 2 x USB 3.0 Type A, 1 x Консоль RS232, 1 x Вывод Com для Lcp, 1 x Разъем VGA, 4 × 1GbE RJ-45, 2 x 1GbE SFP, одинарный/сдвоенный блок питания.

Модель аппаратного исполнения	Комплектация аппаратных исполнений Изделия
Numa Edge 200	Компьютер Lanner NCA-4210B на базе процессора Intel Skylake/Kabylake/ Intel Xeon E3, чипсетом C236, оперативной памятью типа 2 x DDR4 2400 МГц до 32 Гбайт, встроенные интерфейсы 6 x RJ45 GbE и 2 x SFP,1 модуль расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 3.0, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 1000	Компьютер Lanner NCA-5210B на базе процессора Intel Skylake/Kabylake/ Intel Xeon E3, с чипсетом C236, оперативной памятью типа DDR4 2400 МГц до 64 Гбайт, встроенные интерфейсы 12 x RJ45 GbE, 4 x SFP GbE, 2 модуля расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, IPMI, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 1100	Компьютер Lanner NCA-5210C на базе процессора Intel Skylake/Kabylake/ Intel Xeon E3, с чипсетом C236, оперативной памятью типа DDR4 2400 МГц до 64 Гбайт, 4 модуля расширения опционально, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, IPMI, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 2000	Компьютер Lanner FW-5510A на базе процессора Intel Xeon E5, чипсетом C612, оперативной памятью типа DDR4 1600/1866/2133 МГц до 256 Гбайт, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, служебный порт RJ45, 4 модуля расширения опционально, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов
Numa Edge 3000	Компьютер Lanner FW-8894 на базе процессора Intel Xeon E5, чипсетом C612, оперативной памятью типа DDR4 2133 МГц до 512 Гбайт, 4 модуля расширения, порты ввода-вывода 1 x RJ45 GbE, 2 x USB 2.0, IPMI, служебный порт RJ45, встроенный блок питания, жидкокристаллический экран 2 строки по 20 символов

3.2. В таблице 4 приведены модули расширения, доступные для опционального комплектования аппаратных исполнений Изделия. Необходимость установки модулей расширения определяется Заказчиком при размещении заказа на производство Изделия.

Таблица 4 – Модули расширения аппаратных платформ Изделия

Модель модуля расширения	Edge-M1C4	Edge-M1C8	Edge-M1F4	Edge-M1F8	Edge-M10F2	Edge-M10F4	Edge-M40F2	Edge-R10F4	Edge-R1C4	Edge-R1C8
Описание модуля	4 порта RJ-45 1 Gb	8 портов RJ-45 1 Gb	4 порта SFP 1 Gb	8 портов SFP 1 Gb	2 порта SFP+ 10 Gb	4 порта SFP+ 10 Gb	2 порта QSFP+ 40 Gb	4 порта 10GbE SFP+	4 порта RJ-45 1GE	8 портов RJ45 1GE
Numa Edge 10	-	-	-	-	-	-	-	-	-	-
Numa Edge 25	-	-	-	-	-	-	-	-	-	-
Numa Edge 25R	-	-	-	-	-	-	-	-	-	-
Numa Edge 40R	-	-	-	-	-	-	-	-	-	-

Модель модуля расширения	Edge-M1C4	Edge-M1C8	Edge-M1F4	Edge-M1F8	Edge-M10F2	Edge-M10F4	Edge-M40F2	Edge-R10F4	Edge-R1C4	Edge-R1C8
Описание модуля	4 порта RJ-45 1 Gb	8 портов RJ-45 1 Gb	4 порта SFP 1 Gb	8 портов SFP 1 Gb	2 порта SFP+ 10 Gb	4 порта SFP+ 10 Gb	2 порта QSFP+ 40 Gb	4 порта 10GbE SFP+	4 порта RJ-45 1GE	8 портов RJ45 1GE
Numa Edge 50	-	-	-	-	-	-	-	-	-	-
Numa Edge 55	-	-	-	-	-	-	-	-	-	-
Numa Edge 100	+	+	+	+	+	+	+	-	-	-
Numa Edge 100R	-	-	-	-	-	-	-	+	+	+
Numa Edge 180R	-	-	-	-	-	-	-	+	+	+
Numa Edge 200	+	+	+	+	+	+	+	-	-	-
Numa Edge 1000	+	+	+	+	+	+	+	-	-	-
Numa Edge 1100	+	+	+	+	+	+	+	-	-	-
Numa Edge 2000	+	+	+	+	+	+	+	-	-	-
Numa Edge 3000	+	+	+	+	+	+	+	-	-	-

3.3. Изделие реализует следующие функции безопасности, в соответствии с требованиями документов: «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), а также «Задания по безопасности» 643.АМБН.465689.0013Б с расширенными компонентами функциональных требований безопасности:

- контроль и фильтрация;
- идентификация и аутентификация;
- регистрация событий безопасности (аудит);
- обеспечение бесперебойного функционирования и восстановление;
- тестирование и контроль целостности;
- преобразование сетевых адресов;
- маскирование;
- приоритизация информационных потоков;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации.

3.4. Изделие обеспечивает реализацию следующих функций необходимых для работ в сетях передачи данных корпоративного уровня:

- функционирование в режиме маршрутизации или «моста» (в том числе одновременно – для разных сетевых интерфейсов);

– статическая маршрутизация;
– динамическая маршрутизация с поддержкой протоколов RIP, OSPF, BGP;
– маршрутизация на основании политик (Policy-Based Routing);
– множественные таблицы маршрутизации – резервирование каналов и балансировка нагрузки;
– маршрутизация многоадресных передач;
– построение туннелей (с применением протоколов GRE, IP-IP, SIT);
– агрегация (объединение) сетевых интерфейсов (в том числе статическое или с применением протокола LACP);
– сервисы DHCP и DNS;
– ретрансляция DHCP запросов (DHCP-relay);
– поддержка протокола SNMP (Simple Network Management Protocol);
– модификация сетевого трафика в соответствии с заданными политиками;
– клонирование сетевого трафика в соответствии с заданными политиками;
– трансляция сетевых адресов и портов (NAT/PAT);
– регистрация статистики сетевого трафика, включая нагрузку, типы проходящих пакетов, отправителей и получателей сетевого трафика;
– передача статистики сетевого трафика на внешние сервисы-коллекторы по протоколам NetFlow и sFlow.

3.5. В дополнение к функциям безопасности, заявленным в подразделах 3.3, 3.4 настоящего Формуляра, СКЗИ «МагПро КриптоПакет» версия 4.0 СЕИУ.00009-05 (исполнение 7, исполнение 8), предустановленное в программно-аппаратный комплекс Numa Edge АМБН.465689.001 с программным обеспечением «Межсетевой экран Numa Edge версия 1.0» 643.АМБН.00004-01 (исполнение 2), обеспечивает:

– создание и проверку электронной подписи в соответствии с ГОСТ Р 34.10 для файлов и данных, содержащихся в областях оперативной памяти;
– зашифрование и расшифрование в соответствии с ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и ГОСТ 28147-89 (только для взаимодействия с ПО, не поддерживающим ГОСТ Р 34.12-2015) фалов и данных, содержащихся в областях оперативной памяти;
– имитозащиту в соответствии с ГОСТ Р 34.13-2015, HMAC на основе ГОСТ Р 34.11-2012, а также ГОСТ 28147-89 (только для взаимодействия с ПО, не поддерживающим ГОСТ Р 34.13-2015) фалов и данных, содержащихся в областях оперативной памяти;
– вычисление ключа парной связи по алгоритму VKO с использованием как эфемерных, так и долговременных пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10;
– вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11 для фалов и данных, содержащихся в областях оперативной памяти;
– выработку случайного числа заданной длины;
– вычисление открытых и закрытых ключей проверки подписи в соответствии с ГОСТ Р 34.10;
– формирование производного сеансового ключа;
– импорт криптографических ключей в СКЗИ и их экспорт из СКЗИ;
– реализацию протокола TLS с использованием российских криптонаборов, определенных реализациями ТК26.

3.6. Подсчет контрольных сумм Изделия осуществляется согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00004-01 88 01 с использованием сертифицированной программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Трафарет 2.0» (Сертификат ФСТЭК России №2031 от 03.02.2010), либо свободно распространяемой утилиты «gost12sum» (по алгоритму ГОСТ Р 34.11-2012, 256 бит).

Таблица 5 – Контрольные суммы Изделия

ПАК Numa Edge	КС ГОСТ Р 34.11-94 (Трафарет 2.0)	КС ГОСТ Р 34.11-2012 (256 бит)
с установленным ПО «Межсетевой экран Numa Edge версия 1.0» Исполнение 1		
с установленным ПО «Межсетевой экран Numa Edge версия 1.0» Исполнение 2		

4. КОМПЛЕКТНОСТЬ

4.1. Комплектность Изделия приведена в таблице 6.

Таблица 6 – Комплектность Изделия

Обозначение	Наименование	Кол-во	Примечание
Изделие			
АМБН.465689.001	Программно-аппаратный комплекс Numa Edge		Зав.№:
Документация*			
АМБН.465689.001ФО	Программно-аппаратный комплекс Numa Edge. Формуляр		В печатном виде
АМБН.465689.001ФО-1	Программно-аппаратный комплекс Numa Edge. Формуляр. Приложение		На компакт-диске
АМБН.465689.001ПС	Программно-аппаратный комплекс Numa Edge. Паспорт		В печатном виде
643.АМБН.00004-01 32 01	Руководство администратора.		На компакт-диске
643.АМБН.00004-01 32 02	Руководство администратора. Построение виртуальных частных сетей (VPN) на основе протокола OpenVPN		На компакт-диске. **
643.АМБН.00004-01 32 03	Руководство администратора. Краткое руководство по настройке.		В печатном виде
643.АМБН.00004-01 32 04	Руководство администратора. Построение частных сетей на основе набора протоколов IPSec		На компакт-диске. **
643.АМБН.00004-01 32 05	Руководство администратора. Использование FTP proxy		На компакт-диске
643.АМБН.00004-01 32 06	Руководство администратора. Настройка Socks Proxy		На компакт-диске
643.АМБН.00004-01 32 07	Руководство администратора. Туннелирование IP		На компакт-диске
643.АМБН.00004-01 32 08	Руководство администратора. Настройка VPN с использованием протоколов PPTP и L2TP/IPSec		На компакт-диске**
643.АМБН.00004-01 32 09	Руководство администратора. Настройка LVS		На компакт-диске
643.АМБН.00004-01 32 10	Руководство администратора. Мониторинг и сигнализация неисправностей оборудования		На компакт-диске
643.АМБН.00004-01 88 01	Инструкция по проверке контрольных сумм		На компакт-диске
б/н	Установка и настройка утилиты numa-ssh		На компакт-диске
б/н	Сервисный сертификат		В печатном виде
№4199 от 26.12.2019	Копия сертификата соответствия ФСТЭК России на ПАК Numa Edge		В печатном виде

Обозначение	Наименование	Кол-во	Примечание
СЕИУ.00009-05 30	СКЗИ «МагПро КриптоПакет» версия 4.0. Формуляр		В печатном виде. **
б/н	Комплект документации для СКЗИ «МагПро КриптоПакет» версия 4.0		На компакт-диске. **
№СФ/114-4205 от 21.01.2022 №СФ/124-4260 от 21.01.2022	Копия сертификата соответствия ФСБ России на СКЗИ «МагПро КриптоПакет»		В печатном виде. **
Материалы			
643.АМБН.00004-01	Установочный пакет программного обеспечения «Межсетевой экран Numa Edge версия 1.0»		На компакт-диске
б/н	Коммуникационная программа ssh		На компакт-диске
б/н	Компакт-диск с документацией для ПАК Numa Edge		
б/н	Компакт-диск с дистрибутивом и документацией на СКЗИ «МагПро КриптоПакет» версия 4.0		**
* Примечание. Итоговый комплект документации к Изделию зависит от договора поставки. ** Только для ПАК Numa Edge с предустановленным программным обеспечением «Межсетевой экран Numa Edge версия 1.0» (643.АМБН.00004-01) Исполнение 2.			

5. СВИДЕТЕЛЬСТВО О ПРИЁМКЕ

Программно-аппаратный комплекс Numa Edge

наименование Изделия и аппаратного исполнения

АМБН.465689.001

Обозначение

заводской номер

изготовлен и принят в соответствии с обязательными требованиями государственных стандартов, действующим ТУ и признан годным для эксплуатации.

Дата выпуска:

число, месяц, год

Начальник производственного отдела

личная подпись *расшифровка подписи*

М.П.

число, месяц, год

Генеральный директор

личная подпись *расшифровка подписи*

М.П.

число, месяц, год

6. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Программно-аппаратный комплекс Numa Edge

наименование Изделия и аппаратного исполнения

АМБН.465689.001

обозначение

заводской номер

маркированный идентификатором СЗИ:

РОСС RU.0001.4199.

идентификатор СЗИ

упакован ООО «НумаТех»

наименование или код изготовителя (организации)

согласно требованиям, предусмотренным инструкцией по маркировке и упаковке АМБН.465689.001И1

Дата упаковки:

число, месяц, год

Упаковку произвел:

личная подпись *расшифровка подписи*

7. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

7.1. Периодический контроль основных характеристик Изделия заключается в проверке его контрольной суммы. Проверка проводится при первичном закреплении Изделия за ответственным лицом и в дальнейшем не реже одного раза в год.

7.2. Проверка контрольных сумм выполняется согласно документу «Инструкция по проверке контрольных сумм» 643.АМБН.00004-01 88 01.

7.3. Результаты периодического контроля основных характеристик (контрольные суммы) фиксируются в таблице 7.

Таблица 7 – Контроль основных характеристик при эксплуатации и хранении

Проверяемая характеристика		Дата проведения измерения							
Наименование измерения	Величина	20__ г.		20__ г.		20__ г.		20__ г.	
		Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)
Контрольная сумма Изделия (ГОСТ Р 34.11-94 «Трафарет 2.0»)									
Контрольная сумма Изделия («ГОСТ Р 34.11-2012» (256 бит))									

Примечания:

1. Подсчет КС производился сертифицированной программой фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Трафарет 2.0» (Сертификат ФСТЭК России № 2031 от 03.02.2010), а также свободно распространяемой утилитой «gost12sum» (по алгоритму ГОСТ Р 34.11-2012 256 бит).

2. При несовпадении полученного значения контрольной суммы со значением, указанным в таблицах 5 и 7 (в графе «Величина» таблицы 7 указывается значение контрольной суммы, приведенное в таблице 5, в зависимости от средства контрольного суммирования), необходимо прекратить использование Изделия до окончания расследования данного инцидента и принятия, необходимых мер по его устранению, а также обратиться в техническую поддержку изготовителя. Если контрольная сумма совпадает со значением, приведенным в таблице 5, то Изделие допускается к эксплуатации до следующей проверки контрольной суммы.

3. Данная проверка также проводится по истечении гарантийного срока программного Изделия.

8. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

8.1. Изготовитель гарантирует соответствие комплекта поставки Изделия требованиям разделов 3 и 4 настоящего Формуляра, работоспособность аппаратной платформы Изделия, а также качества Изделия согласно требованиям технических условий АМБН.465689.001ТУ при соблюдении эксплуатирующей организацией условий транспортирования, хранения и эксплуатации, установленных в Формуляре.

8.2. В случае если во время эксплуатации Изделия были внесены изменения в программное обеспечение Изделия и/или его аппаратную конфигурацию, нарушил правила его транспортирования, эксплуатации и хранения, указанные в документации на Изделие, то действие сертификата соответствия и гарантии на Изделие прекращается с момента внесения изменений и/или нарушения правил транспортировки, эксплуатации и хранения.

8.3. Изготовитель осуществляет гарантийное обслуживание Изделия в соответствии с пакетами услуг гарантийного обслуживания, состав и содержание сервисов которых закрепляется Изготовителем в «Политике сервисного сопровождения Продуктов производства НумаТех» (далее - Политика сервисного сопровождения), публикуемой на официальном сайте Изготовителя (www.numatech.ru).

8.4. Гарантийный срок на Изделие составляет 12 месяцев от даты приемки Изделия представителем приобретающей организации.

8.5. Изготовитель на возмездной основе предоставляет возможность продления гарантийного срока эксплуатации Изделия по истечении срока, указанного в п. 8.4, и (или) расширения качества сервисов гарантийного обслуживания Изделия, за счет приобретения дополнительных пактов услуг, предусмотренных действующей Политике сервисного сопровождения.

8.6. Продление гарантийного срока обслуживания и (или) расширение качества сервисов гарантийного обслуживания Изделия возможно в течение 5 лет от даты производства Изделия.

8.7. Гарантийный срок на Изделие и качество сервисов гарантийного обслуживания Изделия указывается в Сервисном сертификате Изделия, наличие которого обеспечивает возможность обращения в сервисную службу Изготовителя.

8.8. В течение гарантийного срока Изготовитель обязуется безвозмездно устранить дефекты Изделий путем их ремонта или замены на аналогичные Изделия при условии соблюдения Заказчиком правил и условий хранения, транспортировки, монтажа, установки и эксплуатации. Гарантийное обслуживание производится на территории Производителя в соответствии со спецификацией пакета сервисов гарантийного обслуживания доступной для Заказчика Изделия.

9. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

9.1. Изготовитель осуществляет техническую поддержку Изделия в соответствии с пакетами услуг технической поддержки, состав и содержание сервисов которых закрепляется Изготовителем в Политике сервисного сопровождения, публикуемой на официальном сайте Изготовителя (www.numatech.ru).

9.2. Изготовитель оказывает базовую техническую поддержку Изделия, в рамках которой изготовитель обеспечивает поиск ошибок реализации и уязвимостей в Изделии на протяжении срока действия технической поддержки, а также обязательства по своевременному информированию заказчика о найденных ошибках и уязвимостях путем рассылок.

9.3. Обязательный срок действия базовой технической поддержки Изделия определяется сроком действия сертификата соответствия на Изделие (согласно Государственному реестру сертифицированных средств защиты информации ФСТЭК России № РОСС RU.0001.01БИ00). По решению изготовителя срок действия технической поддержки может превышать сроком действия сертификата соответствия на Изделие, до информирования ФСТЭК России об окончании технической поддержки Изделия.

9.4. Услуги технической поддержки уровня «Стандарт» доступны приобретающей организации в течение 12 месяцев от даты приемки Изделия представителем приобретающей организации.

9.5. Срок действия технической поддержки Изделия и качество сервисов технической поддержки указывается в Сервисном сертификате Изделия, наличие которого обеспечивает возможность обращения в сервисную службу Изготовителя.

9.6. Иные виды технической поддержки (расширение сервисов технической поддержки) предоставляются изготовителем на возмездной основе, в соответствии с Политикой сервисного сопровождения.

9.7. Контактные данные сервисной службы ООО «НумаТех»

Адрес:	196084, г. Санкт-Петербург, ул. Цветочная, д. 18, лит. А, оф. 424, БЦ «Бизнес-парк»
Телефон:	(812) 3090601 доб.220
E-mail:	support@numatech.ru
Портал:	support.numatech.ru
Режим работы:	Пн. – Пт.: 10:00 – 19:00

10. УКАЗАНИЯ ПО ОБНОВЛЕНИЮ

10.1. Изготовитель осуществляет поиск уязвимостей Изделия, в том числе с использованием Банка данных угроз ФСТЭК России (http://bdu.fstec.ru/), общедоступных баз данных уязвимостей CVE (http://cve.mitre.org/) и других баз данных уязвимостей. При выявлении критичной уязвимости изготовитель незамедлительно разрабатывает меры, направленные на нейтрализацию выявленной уязвимости, и доводит содержание этих мер до заказчика. При необходимости (для нейтрализации выявленной уязвимости) внесения изменений в Изделие процедура выполняется в соответствии с пунктами 71-74 Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. № 55.

10.2. Информация о выходе обновлений и мер, направленных на нейтрализацию выявленной уязвимости, публикуется на сайте изготовителя Изделия (https://www.numatech.ru/).

10.3. При выходе обновления, исправляющего критические уязвимости, указывается обязательность обновления продукта или применения мер, направленных на нейтрализацию выявленной уязвимости. Также на сайте изготовителя размещается информация о контрольной сумме обновления необходимой для верификации обновления.

10.4. Загрузка обновления осуществляется с сервера изготовителя. Ссылка для загрузки предоставляется при обращении в сервисную службу изготовителя. Обновление Изделия может быть получено при наличии у потребителя действующего сертификата (ключа) технической поддержки. Также, по запросу, может быть выслано заверенное извещение об изменении формуляра, содержащее контрольные суммы установленного средства защиты информации с примененным обновлением.

10.5. Обновление Изделия осуществляется в соответствии инструкцией изготовителя, со-

провождающей каждое выпускаемое обновление.

10.6. Обновление комплекса выполняется в следующем порядке:

– получение дистрибутива обновления и инструкции по его применению;

– проведение верификации продукта – расчет контрольных сумм полученного дистрибутива обновления и их сравнение с контрольными суммами, указанными на сайте изготовителя;

– выполнение обновления продукта. По результатам применения обновления делается запись в разделе 16 документа «Формуляр» АМБН.465689.001ФО.

11. УСЛОВИЯ ТРАНСПОРТИРОВАНИЯ, ХРАНЕНИЯ И ЭКСПЛУАТАЦИИ

11.1. Транспортирование Изделия

11.1.1. Допускается транспортирование Изделия любым видом транспорта без ограничения скорости и расстояния в упаковке, обеспечивающей выполнение таких условий:

– температура воздуха – от минус 10 до плюс 50 °С;

– относительная влажность – от 10 до 90 % при температуре не выше плюс 25 °С;

– атмосферное давление – от $8{,}4\times10^4$ до $10{,}7\times10^4$ Па (от 630 до 800 мм рт.ст.);

– массовая концентрация пыли в воздухе – не более 0,75 мг/м^3.

11.2. При попадании Изделия в экстремальные температурные условия необходимо до начала эксплуатации выдержать Изделие при температуре плюс 25 °С не менее двух часов.

11.2.1. При транспортировании должна обеспечиваться защита Изделия от:

– механических повреждений;

– проникновения влаги;

– проникновения грязи и пыли;

– длительного воздействия прямого солнечного света.

11.3. Хранение Изделия

11.3.1. Документация на Изделие, компакт-диск, аппаратная часть Изделия должны храниться в капитальных отапливаемых помещениях на стеллаже или в упаковке, поставляемой изготовителем, в условиях, соответствующих условиям эксплуатации Изделия, при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей. При хранении не допускаются резкие перепады температуры (более 20 °С в час) и воздействия внешних магнитных полей напряженностью более 4000 А/м.

11.4. Указание по эксплуатации

11.5. Условия эксплуатации Изделия:

– температура окружающей среды – от плюс 5 до плюс 35 °С;

– относительная влажность воздуха – не более 80% при температуре не выше плюс 25 °С;

– атмосферное давление – от $8{,}6\times10^4$ Па до $10{,}6\times10^4$ Па (от 645 до 795 мм рт. ст.).

11.6. Не допускается использовать Изделие для обработки информации, содержащей сведения, составляющие государственную тайну.

11.7. Эксплуатация Изделия возможна только при реализации следующих организационно-технических мер:

– при использовании Изделия с предустановленным ПО в исполнении 2 обязательно требуется выполнять требования п.1.3 документа «Руководство администратора. Построение вир-

туальных частных сетей (VPN) на основе протокола OpenVPN» 643.АМБН.00004-01 32 02;

– при первоначальной настройке Изделия необходимо изменить заводские установки паролей на доступ к функциям администрирования Изделия;

– необходимо наличие администратора безопасности, отвечающего за правильную эксплуатацию и настройку Изделия;

– в отношении АРМ администратора безопасности должен быть реализован комплекс организационных и технических мер, соответствующий требованиям по безопасности информации, предъявляемым и (или) реализованным на объекте информатизации, в составе которого эксплуатируется Изделие;

– администрирование Изделия должно осуществляться с рабочего места, на котором должно быть установлено средство антивирусной защиты с последними обновлениями антивирусных баз;

– каналы управления Изделия, расположенные в пределах контролируемой зоны, должны быть защищены организационно-техническими мерами;

– для защиты каналов управления Изделия, выходящих за переделы контролируемой зоны, должны применяться методы и средства, устойчивые к пассивному и/или активному прослушиванию сети и сертифицированные в установленном порядке или должен быть запрещён удалённый доступ для администрирования Изделия по незащищённым каналам связи;

– необходимо сохранение в секрете идентификаторов (имен) и паролей (кодов) администратора Изделия;

– обеспечение сохранности Изделия и физической целостности его аппаратной части;

– регулярно выполнять контроль состава установленного программного обеспечения на предмет его соответствия политике безопасности предприятия, а в случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения, работа должна быть прекращена; по данному факту должно быть проведено служебное расследование комиссией и организованы работы по анализу и ликвидации негативных последствий данного нарушения;

– при необходимости реализация защиты от электромагнитного, акустического и других видов излучения, в том числе проведение специальных исследований технических средств;

– эксплуатация Изделия должна осуществляться в строгом соответствии с эксплуатационными документами на Изделие;

– установка (переустановка, обновление) ПО Изделия должны осуществляться с оригинальных лицензионных дистрибутивных носителей (копий эталонных компакт-дисков) или инсталляционного (-ных) файла(-ов) (или архивов их содержащих), размещённых в специальном разделе сайта изготовителя, и полученных установленным порядком;

– изменение версии ПО Изделия на другую версию возможно только в том случае, если изготовителем подтверждено соответствие данной версии ПО Изделия требованиям безопасности информации путем проведения анализа уязвимостей и периодических испытаний Изделия и его ПО.

12. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

12.1. При обнаружении несоответствия упаковочной тары, комплектности и маркировки поставляемого программного Изделия требованиям настоящего формуляра заказчик обязан в течение двух месяцев со дня поставки Изделия направить рекламацию изготовителю.

12.2. При возникновении ситуации, когда не выполняются требования эксплуатационной документации в процессе эксплуатации программного Изделия, заказчик направляет поставщику рекламацию с сопроводительным письмом с точным описанием сбойной ситуации, характера ее проявления, даты ее обнаружения и условий возникновения.

12.3. Перед отправкой изготовителю все рекламации в обязательном порядке подписываются руководителем подразделения, принявшего или эксплуатирующего Изделие.

12.4. Все рекламации должны направляться в ООО «НумаТех» по указанному адресу в письменном виде: 196084, г. Санкт-Петербург, ул. Цветочная, д. 18 литера А, офис 424.

12.5. Изготовитель принимает рекламацию, если не установлена вина пользователя в возникновении дефекта в Изделии.

12.6. Поступающие рекламации регистрируются в журнале учета рекламаций. Срок рассмотрения рекламаций – один месяц со дня получения рекламации.

12.7. Содержание рекламаций и меры, принятые по ним, записывают в настоящем формуляре.

Учет предъявленных рекламаций

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

13. СВЕДЕНИЯ О ХРАНЕНИИ

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятия с хранения		

14. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

15. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

Основание (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись ответственного лица за проведение изменения	Подпись лица, ответственного за эксплуатацию программного Изделия

16. ОСОБЫЕ ОТМЕТКИ

Документ «Формуляр. Приложение» АМБН.465689.001ФО-1 расположен на компакт-диске, входящим в комплект поставки.

Настоящий Комплект Изделия учтен в системе учета средств защиты информации идентификатором РОСС RU.0001.4199. , экз. №

Таблица 8 – Сведения об обновлении ПАК Numa Edge

№	Дата проведения обновления	Должность, фамилия лица, выполнившего обновление	Подпись

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	изменённых	замененных	новых	аннулированных					
1	6-20				36	АМБН.01.05		Усатых	30.12.2020
2	7, 12-15				36	АМБН.01.11		Усатых	17.08.2022
3	3, 5-10, 13,19				22	АМБН.01.12		Усатых	10.10.2022
4	7-9, 11-13, 23				24	АМБН.01.15		Усатых	23.06.2023