УТВЕРЖДЕН

ФРКЕ.467759.003ПП-ЛУ

ViPNet Coordinator IG 5

ПРАВИЛА ПОЛЬЗОВАНИЯ

ФРКЕ.467759.003ПП

2023

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

Аннотация

Настоящие правила пользования (далее – ПП) составлены в соответствии с требованиями документа [1] и распространяются на ViPNet Coordinator IG 5 ФРКЕ.467759.003 (далее – ViPNet Coordinator IG 5, продукт).

Документ предназначен для ознакомления пользователей продукта с:

– назначением и основными характеристиками продукта;
– правилами работы с продуктом;
– правилами работы с ключевой информацией и ключевыми носителями;
– порядком распространения и учета продукта;
– требованиями по обеспечению безопасности при вводе в эксплуатацию, эксплуатации и выводе продукта из эксплуатации.

Содержание

Перечень используемых сокращений 5
1 Назначение и основные характеристики 6
1.1 Назначение, область применения, основные характеристики безопасности 6
1.2 Вид и формат защищаемой информации 8
1.3 Состав, варианты исполнений и комплектаций 8
1.4 Условия эксплуатации 8
1.4.1 Климатические условия эксплуатации 8
1.4.2 Ограничения по использованию 9
1.5 Дополнительные программные и технические средства 9
1.6 Средства управления 10
2 Ключевая система и ключевые носители 13
2.1 Характеристики ключевой системы 13
2.2 Управление ключевой информацией 13
2.2.1 Меры защиты ключевой информации 13
2.2.2 Порядок формирования и ввода ключей 14
2.2.3 Порядок хранения и использования ключевой информации и ключевых носителей 16
2.2.4 Порядок резервирования ключевой информации 16
2.2.5 Плановая смена и обновление ключей 16
2.2.6 Порядок действий при компрометации ключей 16
2.3 Порядок уничтожения ключей и ключевых носителей 18
3 Порядок распространения и учета 19
3.1 Порядок поставки и приемки 19
3.2 Правила транспортирования и хранения 20
3.3 Порядок учета 21
4 Требования по обеспечению безопасности при вводе в эксплуатацию 23
4.1 Требования к размещению 23
4.2 Требования к персоналу 24
4.3 Инициализация и ввод в эксплуатацию 25
4.3.1 Подготовка к работе 25
4.3.2 Процедура подключения 26
4.3.3 Требования к настройкам 27
4.3.4 Ввод в эксплуатацию 28
5 Требования по обеспечению безопасности при эксплуатации 30
5.1 Общие требования по защите от несанкционированного доступа 30
5.2 Требования к аутентификации и разграничению доступа 31
5.3 Режимы работы 36
5.4 Регистрация событий 37

5.5 Требования по обеспечению целостности 38
5.6 Порядок обеспечения работоспособности 41
5.6.1 Порядок контроля работоспособности 41
5.6.2 Тестирование функционирования ViPNet Coordinator IG 5 43
5.6.3 Тестирование работы фильтров защищенной сети 44
5.6.4 Тестирование работы фильтров открытой сети 44
5.6.5 Порядок резервирования 45
5.6.6 Восстановление работоспособности 46
5.6.7 Обновление ПО 47
5.6.8 Порядок действий при выявлении уязвимостей в процессе эксплуатации 49
6 Требования по обеспечению безопасности при выводе из эксплуатации и передаче в ремонт 51
6.1 Порядок передачи в ремонт 51
6.2 Порядок вывода из эксплуатации 51
6.3 Утилизация 52
Список используемой литературы 54
Приложение А Пример формы протокола контрольной проверки ViPNet Coordinator IG 5 56
Приложение Б Акт о вводе в эксплуатацию 58

Перечень используемых сокращений

АСУ	–	автоматизированные системы управления
АСУ ТП	–	автоматизированные системы управления производственными и технологическими процессами
ИС	–	информационная система
ИТС	–	информационно-телекоммуникационная сеть
КИИ	–	критическая информационная инфраструктура
МЭ	–	межсетевой экран
НСД	–	несанкционированный доступ
ПАК	–	программно-аппаратный комплекс
ПО	–	программное обеспечение
ПП	–	правила пользования
СЗЗ	–	специальный защитный знак
СКЗИ	–	средство криптографической защиты информации
СПО	–	специальное программное обеспечение

1 Назначение и основные характеристики

1.1 Назначение, область применения, основные характеристики безопасности

ViPNet Coordinator IG 5 – индустриальный шлюз безопасности, обеспечивающий криптографическую защиту информации, передаваемой между защищенными сегментами частной виртуальной сети (VPN) ViPNet, и фильтрацию IP-трафика с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сеть связи общего пользования.

ViPNet Coordinator IG 5 выполняет функции устройства межсетевого экранирования (далее – МЭ), обеспечивающего фильтрацию открытых пакетов, в том числе и туннелируемых, в соответствии с заданной политикой безопасности.

ViPNet Coordinator IG 5 соответствует 4 классу защиты МЭ, 4 уровню доверия и может использоваться:

- для защиты персональных данных, конфиденциальной, служебной, коммерческой и другой информации, не содержащей сведений, составляющих государственную тайну, в целях повышения уровня защищенности информационных систем (далее – ИС) государственных и коммерческих структур;
- в государственных ИС до класса защищенности К1 включительно, в автоматизированных системах управления технологическими процессами (далее – АСУ ТП) до класса защищенности К1 включительно, в ИС персональных данных для обеспечения защищенности персональных данных до 1 уровня включительно, в ИС общего пользования II класса, в том числе для обеспечения базовых и адаптированных мер защиты информации;
- в автоматизированных системах управления (далее – АСУ), ИС, информационно-телекоммуникационных сетях (далее – ИТС), которые отнесены к объектам критической информационной инфраструктуры (далее – КИИ) или к значимым объектам КИИ до категории значимости 1 включительно, в том числе для выполнения мер по обеспечению безопасности значимых объектов КИИ Российской Федерации.

ViPNet Coordinator IG 5 может использоваться в указанных выше системах для выполнения базовых и адаптированных мер защиты информации [2], [3], [4], [5], [6].

ViPNet Coordinator IG 5 устанавливается:

- на логической или физической границе (периметре) ИС, АСУ, ИТС;
- между логическими или физическими границами сегментов ИС, АСУ, ИТС;

– на границе (периметре) АСУ;
– между операторским (диспетчерским) уровнем АСУ и уровнем автоматического управления АСУ;
– между уровнем автоматического управления АСУ и полевым уровнем АСУ;
– между физическими границами сегментов АСУ как операторского (диспетчерского) уровня, так и уровня автоматического управления.

Функциональные возможности ViPNet Coordinator IG 5 приведены в разделе 3 «Основные характеристики» формуляра [7].

При выполнении требований, изложенных в настоящих ПП и другой эксплуатационной документации на продукт, ViPNet Coordinator IG 5 соответствует требованиям следующих документов:

– «Требования к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну», установленным для класса КС3;
– «Специальные требования к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации», по уровню $КС_Б$;
– «Требования по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну», установленным для уровня $КС_Б$;
– «Временные требования к устройствам типа межсетевые экраны», установленным для 4 класса защищенности;
– «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);
– «Профиль защиты межсетевых экранов типа «Д» четвертого класса защиты. ИТ.МЭ.Д4.ПЗ» (ФСТЭК России, 2016);
– «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 4 уровню доверия;
– «Программно-аппаратный комплекс ViPNet Coordinator IG 5. Задание по безопасности» ФРКЕ.467759.003Д1.

Соответствие вышеуказанным требованиям подтверждается наличием сертификатов ФСБ России и ФСТЭК России.

1.2 Вид и формат защищаемой информации

ViPNet Coordinator IG 5 обеспечивает криптографическую защиту информации, не содержащей сведений, составляющих государственную тайну (персональные данные, служебная и коммерческая тайны и другая информация конфиденциального характера), передаваемой в IP-пакетах по сети связи общего пользования.

1.3 Состав, варианты исполнений и комплектаций

Комплектность ViPNet Coordinator IG 5 по исполнениям приведена в формуляре [7].

Исполнение ViPNet Coordinator IG 5 – программно-аппаратный комплекс (далее – ПАК) на базе аппаратной платформы и специального программного обеспечения (далее – СПО).

Технические характеристики аппаратных платформ приведены в документе [15].

1.4 Условия эксплуатации

1.4.1 Климатические условия эксплуатации

ViPNet Coordinator IG 5 подлежит эксплуатации в условиях, исключающих:

- механические, тепловые и электрические повреждения;
- воздействие химических и вредных веществ;
- попадание внутрь влаги, песка, сажи, пыли (в том числе токопроводящей) и иных посторонних предметов.

Допускается эксплуатация ViPNet Coordinator IG 5 только в условно-чистой атмосфере в соответствии с ГОСТ 15150-69.

ViPNet Coordinator IG 5 подлежит эксплуатации в условиях, приведенных в таблице 1.

Таблица 1 – Условия эксплуатации ViPNet Coordinator IG 5 в зависимости от аппаратной платформы

Аппаратная платформа	Пониженная рабочая температура, °С	Повышенная рабочая температура, °С	Относительная влажность воздуха при температуре плюс 25 °С не более, %
IG10 I1	минус 20[1]	плюс 60	90
IG10 I2	минус 40	плюс 60	90
IG100 I1	минус 40	плюс 60	90
IG100 I4	минус 40	плюс 60	90
IG100 I5	минус 40	плюс 60	90
IG1000 Q1	плюс 10	плюс 35	90

[1] От минус 40 °С для исполнения без модуля Wi-Fi.

Подробно допустимые условия эксплуатации аппаратных платформ ViPNet Coordinator IG 5 и меры безопасности описаны в документе [15].

1.4.2 Ограничения по использованию

СПО ViPNet Coordinator IG 5 является замкнутой операционной средой. Установка дополнительного программного обеспечения (далее – ПО) на аппаратную платформу ViPNet Coordinator IG 5 невозможна.

Ограничений на эксплуатацию ViPNet Coordinator IG 5 при его использовании в соответствии с эксплуатационной документацией и при соблюдении настоящих ПП нет.

1.5 Дополнительные программные и технические средства

Необходимо наличие у пользователя (в эксплуатирующей организации) следующих сторонних средств, поддерживающих функционирование ViPNet Coordinator IG 5 и не входящих в комплект поставки:

- компьютера (консоли) с портом RS-232 или USB, операционной системой Windows или Linux любых версий для установки справочников и ключей на ViPNet Coordinator IG 5 и локального управления продуктом;

Примечание – К ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1 в качестве альтернативы консоли можно подключать монитор и клавиатуру.

- сетевого кросс-кабеля или патч-корда Ethernet для соединения компьютера с аппаратной платформой ViPNet Coordinator IG 5;
- USB-носителей, отформатированных с использованием одной из поддерживаемых файловых систем: FAT32, ext2, ext3 или ext4, для записи:
  - дистрибутива ключей (далее – ключевой носитель);
  - файла обновления СПО исходной версии для возможности возврата к ней при некорректном обновлении СПО;
  - файла образа СПО для установки на аппаратную платформу после удаления ПО и возврата к заводскому состоянию;
  - файла конфигурации ViPNet Coordinator IG 5 для восстановления или переноса ее на другой ПАК;
- USB-токена, сертифицированного по требованиям ФСБ России (Рутокен ЭЦП 3.0), для хранения ключей пользователя при аутентификации по сертификату и авторизации пользователя (далее – устройство аутентификации);

– консольного кабеля RS-232 с разъемами DB9 и RJ45 (например, Cisco CAB-CONSOLE-RJ45)[2];
– консольного кабеля RS-232 с разъемами DB9[3];
– переходника USB-DB9 (при отсутствии консольного порта RS-232 на компьютере);
– ПО для терминального подключения через консольный порт (например, minicom/picocom (Linux), putty (Windows));
– компьютера (автоматизированного рабочего места (далее – АРМ) администратора ViPNet Coordinator IG 5) с операционной системой Windows или Linux любых версий и установленными:
  – клиентским ПО ViPNet (ViPNet Client) и SSH-клиентом для удаленного управления продуктом по протоколу SSH;
  – клиентским ПО ViPNet (ViPNet Client и ViPNet PKI Client[4]) и веб-браузером (Microsoft Edge, Google Chrome или Mozilla Firefox последних версий) для удаленного управления продуктом через веб-интерфейс;
– средств антивирусной защиты, сертифицированных на соответствие требованиям ФСБ России и (или) ФСТЭК России, для установки на:
  – защищенные сетевые узлы, которые взаимодействуют с ViPNet Coordinator IG 5;
  – АРМ администратора ViPNet Coordinator IG 5.

1.6 Средства управления

Для удаленного управления ViPNet Coordinator IG 5 требуется, чтобы в организации была развернута сеть ViPNet, управление и мониторинг состояния которой выполняются с помощью ViPNet Prime.

Для управления ViPNet Coordinator IG 5 могут использоваться:

– командный интерпретатор;
– веб-интерфейс[5];
– внешнее устройство, переключающее состояние входной линии GPIO[6];
– ViPNet Prime.

Командный интерпретатор запускается автоматически после аутентификации пользователя ViPNet Coordinator IG 5 локально (при подключении с помощью консоли или

[2] Кроме ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.
[3] Только для ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.
[4] Только при управлении ViPNet Coordinator IG 5 с помощью ViPNet Prime.
[5] Для исполнений ViPNet Coordinator IG100 I1, ViPNet Coordinator IG100 I4, ViPNet Coordinator IG100 I5 и ViPNet Coordinator IG1000 Q1.
[6] При функционировании ViPNet Coordinator IG 5 в качестве МЭ типа «Д».

монитора и клавиатуры[7]) и удаленно (при подключении с других узлов сети ViPNet по протоколу SSH).

Посредством командного интерпретатора или веб-интерфейса пользователь может просматривать настройки и администрировать ViPNet Coordinator IG 5 после прохождения процедуры аутентификации. Удаленное подключение к ViPNet Coordinator IG 5 с помощью веб-интерфейса по протоколам HTTP и HTTPS и с помощью командного интерпретатора по протоколу SSH разрешено только с защищенных узлов ViPNet, связанных с ПАК, с ключами, выданными привилегированным пользователям ViPNet Coordinator IG 5.

По умолчанию удаленный доступ к ViPNet Coordinator IG 5 запрещен. Управлять политиками доступа к ViPNet Coordinator IG 5 может только администратор ViPNet Coordinator IG 5. Чтобы разрешить доступ, администратор ViPNet Coordinator IG 5 должен создать сетевой фильтр защищенной сети. В данном фильтре нужно указать идентификатор или группу идентификаторов защищенных узлов сети ViPNet, для которых должен быть разрешен доступ. Подробно настройка удаленного доступа к ViPNet Coordinator IG 5 описана в документе [9].

Запрещено предоставлять доступ к ViPNet Coordinator IG 5 по протоколу SSH пользователям, работающим с техническими средствами, отличными от АРМ администратора (см. подраздел 1.5). Подробнее о подключении к ViPNet Coordinator IG 5 по протоколу SSH см. в документе [8].

С помощью внешнего устройства, переключающего состояние входной линии GPIO, пользователь может выполнять переключение ViPNet Coordinator IG 5 в специальный режим[8] работы и обратно. Подробное описание режимов работы ViPNet Coordinator IG 5 приведено в документе [9].

ViPNet Prime используется администратором сети ViPNet для формирования структуры сети ViPNet, задания основных параметров сетевых узлов, централизованной отправки справочников, ключей и обновлений ПО на сетевые узлы ViPNet. С помощью ViPNet Prime задаются адреса доступа к ViPNet Coordinator IG 5, параметры подключения ViPNet Coordinator IG 5 к внешней сети, адреса туннелируемых узлов, формируются и пересылаются на ViPNet Coordinator IG 5 политики безопасности. С помощью модуля ViPNet Prime Policy Management на ViPNet Coordinator IG 5 передаются сетевые фильтры и правила трансляции адресов и команда по переключению режима работы для межсетевого экрана типа «Д».

Подробное описание управления ViPNet Coordinator IG 5 приведено в документе [10].

---

[7] Для ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.

[8] Под переключением ViPNet Coordinator IG 5 в специальный режим подразумевается переключение заранее настроенного набора сетевых фильтров. Специальный режим предназначен для чрезвычайных ситуаций в работе системы, обновление СПО ViPNet Coordinator IG 5, справочников и ключей в этом режиме невозможно.

Подробное описание способов управления ViPNet Coordinator IG 5 приведено в документах [8] и [11].

2 Ключевая система и ключевые носители

2.1 Характеристики ключевой системы

Ключевая информация ViPNet Coordinator IG 5 включает в себя:

– ключи сетевого узла;

– ключи аутентификации пользователя.

Ключи сетевого узла – симметричные ключи, которые используются для шифрования и имитозащиты справочно-ключевой информации, хранящейся на внутреннем дисковом накопителе ViPNet Coordinator IG 5, а также информации, передаваемой между ViPNet Coordinator IG 5 и остальными узлами сети ViPNet.

Ключи сетевого узла создаются в ViPNet Prime и поставляются в составе дистрибутива формата ds5. Дистрибутив ключей используется в процессе инициализации ViPNet Coordinator IG 5. Порядок формирования и ввода ключей приведен в п. 2.2.2.

Ключи аутентификации пользователя – асимметричная ключевая пара, которая состоит из закрытого ключа и сертификата открытого ключа. Данный вид ключей используется для аутентификации пользователя и установления защищенного соединения при подключении к ViPNet Coordinator IG 5. Подробная информация о процедуре аутентификации приведена в подразделе 5.2.

Срок действия и процедура плановой смены ключей приведены в п. 2.2.5.

2.2 Управление ключевой информацией

2.2.1 Меры защиты ключевой информации

При эксплуатации ViPNet Coordinator IG 5 должны выполняться следующие организационно-технические меры защиты ключевой информации:

– ограничение доступа к ключевой информации за счет разграничения полномочий сотрудников, ответственных за эксплуатацию (см. подраздел 4.2);

– надежное хранение (см. п. 2.2.3);

– регулярная смена (см. п. 2.2.5);

– обновление при компрометации (см. п. 2.2.6);

– резервирование (см. п. 2.2.4);

– безопасное уничтожение (см. подраздел 2.3);

– применение устройств аутентификации, сертифицированных по требованиям ФСБ России (см. подраздел 1.5).

Обращение с ViPNet Coordinator IG 5 с введенной ключевой информацией, а также с ключевыми носителями и устройствами аутентификации, должно выполнятся в соответствии с инструкцией [12] и настоящими ПП.

Должны быть приняты меры по надежному сохранению в тайне PIN-кодов, паролей доступа, ключевой и аутентификационной информации.

Ответственность за соблюдение требований по обеспечению безопасности при смене, хранении, вводе, выводе и уничтожении ключевой информации должна быть возложена на одно или несколько уполномоченных эксплуатирующей организацией лиц из числа доверенных пользователей, обладающих максимальным уровнем полномочий для эксплуатации продукта.

Ответственность за сохранность персональной аутентификационной информации и паролей доступа несет сам пользователь.

Передача ключевых носителей и устройств аутентификации в случаях, предусмотренных настоящими ПП, должна выполняться доверенным способом.

При обращении с ключевой информацией, ключевыми носителями и устройствами аутентификации запрещено:

- разглашать содержимое ключевого носителя, в том числе выводить ключевую информацию на дисплей, принтер и иные средства вывода и отображения информации, или передавать носитель лицам, которым не разрешен доступ к нему;
- разглашать PIN-коды ключевых носителей (устройств аутентификации) и пароли доступа;
- использовать ключевые носители (устройства аутентификации) в режимах, не предусмотренных функционированием ViPNet Coordinator IG 5;
- записывать на ключевые носители (устройства аутентификации) постороннюю информацию;
- оставлять ключевые носители (устройства аутентификации) без присмотра;
- копировать содержимое ключевых носителей, если это не предусмотрено п. 2.2.4.

2.2.2 Порядок формирования и ввода ключей

Администратор ViPNet Prime доверенным способом передает дистрибутив ключей на ключевом носителе администратору ViPNet Coordinator IG 5 (лицу, ответственному за инициализацию продукта, в соответствии с ролевой моделью эксплуатирующей организации, описанной в подразделе 5.2). Подробное описание установки дистрибутива ключей, а также последовательность действий администратора ViPNet Coordinator IG 5 (лица, ответственного за инициализацию продукта) при инициализации продукта приведены в документе [9].

Для организации работы кластера горячего резервирования ViPNet Coordinator IG 5 (см. п. 5.6.6) на оба узла кластера вводятся ключи одного и того же дистрибутива. В иных

случаях запрещено использовать один и тот же дистрибутив ключей для инициализации нескольких ViPNet Coordinator IG 5.

Ввод новых ключей и справочной информации при изменении структуры сети ViPNet производится централизованно из ViPNet Prime.

Ключи аутентификации пользователей могут быть созданы:

1) средствами ViPNet Coordinator IG 5 – для двух локальных учетных записей пользователей с ролями:
   - администратор (имя учетной записи admin);
   - аудитор (имя учетной записи user);
2) средствами ViPNet Prime – для централизованных учетных записей пользователей, прошедших аутентификацию в ViPNet Prime.

Первый раз ключи аутентификации администратора продукта с локальной учетной записью создаются в ViPNet Coordinator IG 5 и записываются на персональное устройство аутентификации при инициализации продукта. Дальнейшая смена ключей аутентификации администратора описана в пп. 2.2.5 и 2.2.6.

Создание ключей аутентификации для аудитора с локальной учетной записью может инициировать любой администратор ViPNet Coordinator IG 5, имеющий локальный доступ к продукту либо удаленный доступ по протоколу SSH.

Действующими для администратора продукта с локальной учетной записью и для аудитора будут только последние созданные в ViPNet Coordinator IG 5 ключи аутентификации.

Пользователи, прошедшие аутентификацию в ViPNet Prime, инициируют создание ключей аутентификации и запроса на выпуск сертификата с помощью ViPNet PKI Client. Ключи аутентификации создаются на устройстве аутентификации. Запрос на выпуск сертификата записывается на USB-носитель и передается в удостоверяющий центр. Удостоверяющий центр по запросу выпускает сертификат для аутентификации пользователя, который записывается на устройство аутентификации. Сертификат передается администратору ViPNet Prime. Администратор ViPNet Prime загружает изданный сертификат, а также корневой сертификат удостоверяющего центра в ViPNet Prime, ассоциирует сертификат пользователя с учетной записью этого пользователя, после чего возвращает персональное устройство аутентификации пользователю.

Подробное описание способов установки ключей, а также последовательность действий при их установке приведены в документе [9].

2.2.3 Порядок хранения и использования ключевой информации и ключевых носителей

Ключевые носители должны храниться в шкафах (ящиках, сейфах, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. При отсутствии условий хранения ключевые носители должны быть уничтожены в соответствии с требованиями подраздела 2.3.

Пользователем должны быть приняты меры по надежному хранению устройства аутентификации.

2.2.4 Порядок резервирования ключевой информации

Резервирование ключей узла средствами продукта, а также резервное копирование ключей аутентификации пользователей невозможно.

Не рекомендуется создавать копии дистрибутивов ключей, если это не предусмотрено политикой информационной безопасности эксплуатирующей организации. Обращение с резервными копиями, а также с ключевыми носителями, которые их содержат, должно выполняться так же, как с остальной ключевой информацией и ключевыми носителями.

2.2.5 Плановая смена и обновление ключей

Плановая смена ключей сетевого узла производится дистанционно (по сети) из ViPNet Prime до истечения срока действия ключей. Срок действия устанавливается при формировании ключей сетевого узла в ViPNet Prime и не превышает 15 месяцев. Контроль за соблюдением сроков действия ключей и своевременностью их смены выполняется группой администраторов ViPNet Prime. В ViPNet Coordinator IG 5 реализовано оповещение о скором истечении срока действия ключей.

Процедура смены ключей аутентификации пользователей с локальными учетными записями описана в документах [8] и [11], пользователей, прошедших аутентификацию в ViPNet Prime – в документе [16]. Срок действия ключей аутентификации не превышает 12 месяцев. Контроль за соблюдением сроков действия ключей аутентификации и своевременностью их смены выполняет пользователь ViPNet Coordinator IG 5 самостоятельно. В ViPNet Coordinator IG 5 реализовано оповещение о скором истечение срока действия сертификатов пользователей (по умолчанию за тридцать дней до истечения срока действия).

Администратор ViPNet Coordinator IG 5 может настроить оповещения об истечении срока действия ключей согласно документу [8].

2.2.6 Порядок действий при компрометации ключей

Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. События, квалифицируемые как факт

компрометации ключей, определяются лицом, уполномоченным эксплуатирующей организацией, в соответствии с политикой безопасности эксплуатирующей организации.

Ключи всегда считаются скомпрометированными в следующих случаях:

– посторонние лица могли получить неконтролируемый физический доступ к аппаратным компонентам ViPNet Coordinator IG 5;
– посторонние лица могли получить доступ к ключам, хранящимся на узле защищаемой ИС или ключевом носителе (устройстве аутентификации);
– смена или увольнение лиц, имевших доступ к ключевой информации, ключевым носителям и паролям доступа;
– имеются обоснованные подозрения на утечку информации.

Ключи аутентификации пользователя считаются скомпрометированными в следующих случаях:

– посторонние лица могли получить доступ к устройству аутентификации;
– устройство аутентификации было утеряно;
– увольнение или смена пользователя, владевшего устройством аутентификации.

Решение о факте компрометации ключей принимает администратор ViPNet Coordinator IG 5 (лицо, уполномоченное эксплуатирующей организацией).

Порядок действий при компрометации ключей ViPNet Coordinator IG 5:

1) администратор ViPNet Coordinator IG 5 незамедлительно блокирует работу ViPNet Coordinator IG 5, ключи которого были скомпрометированы, с помощью удаления справочников и ключей или сброса к заводским настройкам[9] [8];
2) администратор ViPNet Coordinator IG 5 уведомляет администратора ViPNet Prime о факте и обстоятельствах компрометации;
3) администратор ViPNet Prime формирует новый дистрибутив ключей, записывает его на ключевой носитель и передает администратору ViPNet Coordinator IG 5 с оформлением соответствующей записи в журнале поэкземплярного учета средств криптографической защиты информации (далее – СКЗИ);
4) администратор ViPNet Coordinator IG 5 выполняет инициализацию ViPNet Coordinator IG 5, используя новый дистрибутив ключей с ключевого носителя (см. п. 2.2.2).

При компрометации аутентификационной информации пользователя администратор ViPNet Coordinator IG 5 (лицо, уполномоченное эксплуатирующей организацией) должен

[9] Сброс к заводским настройкам выполняется только на ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.

незамедлительно заблокировать доступ учетной записи данного пользователя к ViPNet Coordinator IG 5 и выполнить процедуру смены аутентификационной информации. Подробное описание процедуры смены аутентификационной информации при компрометации приведено в документах [8] (для пользователей с локальными учетными записями) и [16] (для пользователей, прошедших аутентификацию в ViPNet Prime).

2.3 Порядок уничтожения ключей и ключевых носителей

Уничтожение ключевой информации, а также ее резервных копий (при наличии) должно выполняться в следующих случаях:

- плановое обновление ключевой информации (см. п. 2.2.5);
- компрометация ключевой информации (см. п. 2.2.6);
- смена лиц, ответственных за хранение и использование персональной ключевой информации и ключевых носителей (см. п. 2.2.3);
- передача продукта в ремонт (см. подраздел 6.1);
- вывод продукта из эксплуатации (см. подраздел 6.2).

Ответственность за уничтожение ключевой информации, ключевых носителей несет администратор ViPNet Coordinator IG 5.

Администратор ViPNet Coordinator IG 5 может удалить ключи с помощью командного интерпретатора по команде admin remove keys или выполнив сброс к заводским настройкам[9] в соответствии с документом [8]. Событие удаления ключей фиксируется в журнале СКЗИ (подробнее о регистрации событий см. в подразделе 5.4).

Удаление ключей, расположенных на ключевых носителях, необходимо выполнять с помощью сертифицированных средств гарантированного уничтожения информации. Если удаление информации невозможно без повреждения носителя, на котором она расположена, то необходимо уничтожить носитель способом, полностью исключающим возможность восстановления и использования информации.

После удаления ключей, расположенных на ключевых носителях, должна быть сделана соответствующая отметка в журнале поэкземплярного учета СКЗИ.

3 Порядок распространения и учета

Учет и обеспечение безопасности ViPNet Coordinator IG 5 при транспортировании и хранении должны осуществляться в соответствии с положениями документа [12].

3.1 Порядок поставки и приемки

Поставка ViPNet Coordinator IG 5 осуществляется от изготовителя либо через авторизованных партнеров.

При приемке ViPNet Coordinator IG 5 пользователю (уполномоченному лицу эксплуатирующей организации) необходимо проверить:

1. Целостность корпуса продукта.
2. Наличие и целостность специальных защитных знаков (далее – СЗЗ) на корпусе продукта:

   а) корпус ViPNet Coordinator IG 5 должен быть без механических повреждений (сколов, царапин, вмятин);

   б) на корпусе должны быть размещены СЗЗ;

   в) номера СЗЗ на корпусе ViPNet Coordinator IG 5 должны совпадать с номерами СЗЗ, указанными в разделе 5 «Свидетельство о маркировке, упаковке и приемке» формуляра [7];

   г) СЗЗ не должны иметь повреждений и замятий.

3. Подлинность СЗЗ путем проверки элементов защиты согласно рисунку 1:

   а) микротекст с динамическим эффектом перетекания – четко читается при поднесении увеличительного стекла к верхним горизонтальным линиям на СЗЗ;

   б) дифракционные микролинзы – цвет радужно переливается от центра к краям квадрата микролинзы при изменении угла наклона СЗЗ;

   в) диагональные надписи «VIRTUAL PRIVATE NETWORK» – просматриваются невооруженным глазом и радужно переливаются при изменении угла наклона СЗЗ;

   г) гильоширные линии с динамическим эффектом – радужно переливаются при изменении угла наклона СЗЗ;

   д) логотип «ViPNet» – серый цвет надписи динамически изменяется при изменении угла наклона СЗЗ.

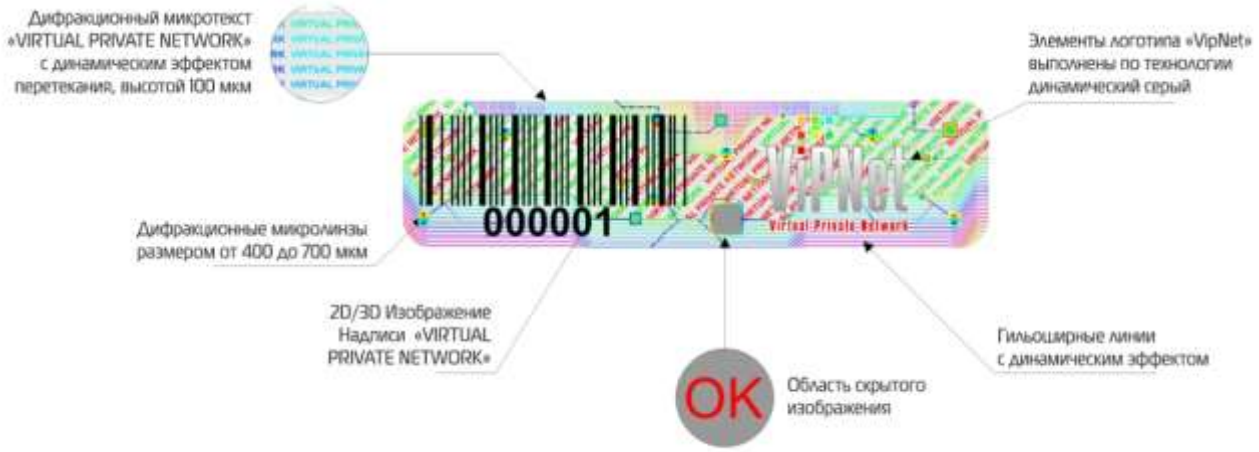

Рисунок 1 – Вид самоклеящейся этикетки «ViPNet» (СЗЗ)

Примечание – СЗЗ обеспечивают надежное сцепление с поверхностью и предотвращают попытку удаления СЗЗ или повторного переклеивания. При отклеивании СЗЗ расслаивается в произвольном направлении.

4. Маркировку продукта на соответствие информации, указанной в разделе 5 «Свидетельство о маркировке, упаковке и приемке» формуляра [7].
5. Комплектность продукта на соответствие информации, указанной в разделе 4 «Комплектность» формуляра [7] и в договоре на поставку.
6. Оптический диск из комплекта поставки на наличие механических повреждений.
7. Целостность дистрибутива СПО путем сравнения его контрольной суммы с информацией, указанной в разделе 11 «Контрольные суммы» формуляра [7]. Метод расчета контрольной суммы также указан в разделе 11 «Контрольные суммы» формуляра [7].

3.2 Правила транспортирования и хранения

ViPNet Coordinator IG 5 подлежит транспортированию в упаковке изготовителя в следующих условиях:

– температура окружающей среды от минус 40 до плюс 50 °С;
– верхнее значение относительной влажности воздуха 100 % при температуре плюс 25 °С;
– атмосферное давление от 84 до 107 кПа (от 630 до 800 мм. рт. ст.);
– без прямого воздействия солнечных лучей, атмосферных осадков, пыли и грязи;
– без воздействия агрессивных примесей (паров кислот, щелочей).

Транспортирование оптического диска, входящего в комплект поставки, должно осуществляться в упаковке изготовителя, не допуская ударов, механических повреждений и иных воздействий, которые могут привести к потере информации на оптическом диске.

В части воздействия механических факторов транспортирование должно производиться в соответствии с ГОСТ 23216, условия транспортирования «С».

ViPNet Coordinator IG 5 может транспортироваться автомобильным, железнодорожным (в закрытых транспортных средствах) или авиационным транспортом (в обогреваемых герметизированных отсеках) в условиях, исключающих механические повреждения.

Условия хранения в части воздействия климатических факторов должны соответствовать условиям хранения группы 5 («ОЖ4») по ГОСТ 15150 со следующими уточнениями:

- температура окружающей среды от минус 20 до плюс 40 °С;
- верхнее значение относительной влажности воздуха 98 % при температуре плюс 25 °С;
- атмосферное давление от 84 до 107 кПа (от 630 до 800 мм. рт. ст.);
- без прямого воздействия солнечных лучей, атмосферных осадков, пыли и грязи;
- без воздействия агрессивных примесей (паров кислот, щелочей).

В помещениях для хранения содержание пыли, паров кислот и щелочей, агрессивных газов и других вредных примесей, вызывающих коррозию, не должно превышать содержания коррозионно-активных агентов для атмосферы типа I по ГОСТ 15150.

После транспортирования ViPNet Coordinator IG 5 или хранения при температуре ниже температуры эксплуатации необходимо выдержать его в выключенном состоянии при температуре плюс 20 °С не менее 4 часов.

Оптический диск подлежит хранению в закрытых отапливаемых помещениях на расстоянии не менее 50 см от источников тепла и влаги, без прямого воздействия солнечных лучей, пыли, грязи и агрессивных примесей (паров кислот, щелочей).

Рекомендуется хранить оптический диск на стеллажах в вертикальном положении в упаковке изготовителя либо в специальных контейнерах в условиях, исключающих перемещения и вибрации оптического диска, а также воздействия на него ударов.

При постановке ViPNet Coordinator IG 5 на хранение в разделе 8 «Сведения о хранении» формуляра [7] проставляется соответствующая отметка.

3.3 Порядок учета

Изготовитель ведет поэкземплярный учет изготовленных ViPNet Coordinator IG 5.

Допускается выполнять учет ViPNet Coordinator IG 5 с оформлением формуляра на группу (партию) ViPNet Coordinator IG 5. В этом случае группы (диапазоны) серийных номеров и регистрационных номеров поставляемых ViPNet Coordinator IG 5 указываются в

формуляре [7]. При оформлении формуляра [7] на группу ViPNet Coordinator IG 5 в разделе «Свидетельство о маркировке, упаковке и приемке» формуляра [7] указываются:

- серийные номера ViPNet Coordinator IG 5;
- регистрационные номера СКЗИ;
- идентификаторы средства защиты информации (далее – СЗИ);
- номера СЗЗ,

входящих в группу.

Для последовательно идущих серийных номеров, регистрационных номеров СКЗИ, идентификаторов СЗИ и номеров СЗЗ, входящих в группу, допускается указание диапазона. Диапазон должен состоять из разделенных знаком «-» первого и последнего серийных номеров, регистрационных номеров СКЗИ, идентификаторов СЗИ или номеров СЗЗ, входящих в группу.

При получении продукта от изготовителя и вводе продукта в эксплуатацию поэкземплярный учет ViPNet Coordinator IG 5 осуществляется в эксплуатирующей организации. Для этого администратор (лицо, ответственное за эксплуатацию продукта) вносит регистрационный номер СКЗИ, зафиксированный в формуляре [7], в журнал поэкземплярного учета СКЗИ.

Допускается создавать необходимое количество учтенных копий формуляра [7] (с пометкой «Копия») и оптического диска с эксплуатационной документацией на ViPNet Coordinator IG 5.

4 Требования по обеспечению безопасности при вводе в эксплуатацию

4.1 Требования к размещению

При размещении ViPNet Coordinator IG 5 следует руководствоваться следующими требованиями:

1. ViPNet Coordinator IG 5 должен быть размещен в контролируемой зоне. В эксплуатирующей организации должны быть приняты меры по расположению, специальному оборудованию, охране и организации режима места размещения ViPNet Coordinator IG 5, которые должны:
   - обеспечивать безопасность информации ограниченного доступа, в том числе ключевой информации;
   - исключать возможность несанкционированного копирования конфиденциальной информации и ключевой информации, умышленного повреждения или кражи ViPNet Coordinator IG 5 и носителей информации ограниченного доступа, в том числе ключевой информации.
2. Если ViPNet Coordinator IG 5 планируется разместить и эксплуатировать в помещении, в котором циркулирует речевая акустическая и (или) визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены автоматизированные системы и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, то ViPNet Coordinator IG 5 должно быть подвергнуто проверкам по выявлению устройств, предназначенных для негласного получения информации.
3. Локальный доступ к ViPNet Coordinator IG 5 для лиц, не являющихся привилегированными пользователями, должен быть ограничен организационно-техническими мерами.
4. Необходимо обеспечить доверенный канал передачи данных между защищаемой информационной системой и ViPNet Coordinator IG 5, между ViPNet Coordinator IG 5 и средством управления и мониторинга ViPNet Coordinator IG 5, с которого выполняется управление ViPNet Coordinator IG 5.
5. Необходимо обеспечить доверенную связь (маршрут) между ViPNet Coordinator IG 5 и пользователями ViPNet Coordinator IG 5.

6. Необходимо исключить возможность создания каналов связи защищаемой информационной системы с иными информационными системами в обход ViPNet Coordinator IG 5.

При эксплуатации ViPNet Coordinator IG 5 необходимо выполнять действующие в Российской Федерации требования по защите информации от утечки по техническим каналам.

Формуляр и оптический диск с документацией на ViPNet Coordinator IG 5 должны храниться с продуктом. Доступ к формуляру должен быть только у лица, ответственного за ведение формуляра. Должны быть приняты меры защиты от подмены формуляра и другой эксплуатационной документации на продукт.

4.2 Требования к персоналу

Правом доступа к ViPNet Coordinator IG 5 должны обладать только пользователи, изучившие эксплуатационные документы на продукт, ознакомленные с политикой информационной безопасности эксплуатирующей организации и обладающие необходимой квалификацией и навыками работы со средствами вычислительной техники. Пользователи должны быть ознакомлены с эксплуатационной документацией на продукт под подпись.

В эксплуатирующей организации должны быть назначены должностные лица, отвечающие за:

- контроль соблюдения политики информационной безопасности эксплуатирующей организации;
- инициализацию и ввод продукта в эксплуатацию;
- эксплуатацию, вывод из эксплуатации и утилизацию продукта в соответствии с документацией на него;
- обращение с ключевой информацией и ключевыми носителями;
- назначение и смену аутентификационной информации субъектов доступа к функциям продукта в соответствии с ролевой моделью, приведенной в подразделе 5.2.

Ответственность за соблюдение всех вышеперечисленных требований может быть возложена на одно или несколько уполномоченных эксплуатирующей организацией лиц из числа доверенных (привилегированных) пользователей, обладающих максимальным уровнем полномочий для эксплуатации продукта.

В связи с тем, что корректное выполнение привилегированными пользователями своих обязанностей существенным образом влияет на безопасность информации как ViPNet Coordinator IG 5, так и связанных с ними сегментов сети, естественным требованием является их доверенность и высокая профессиональная подготовка.

Доверенность привилегированных пользователей означает, что они не относятся к потенциальным нарушителям, то есть не будут предпринимать умышленных действий (или бездействия), которые могут привести к реализации угроз безопасности информации. Соответствующий уровень доверенности пользователей достигается путем проведения комплексных проверок на этапе подбора персонала. Контроль над уровнем доверенности пользователей должен обеспечиваться как на техническом уровне (при помощи системы аудита), так и при помощи организационных мер (реализация положений политики безопасности, контроль со стороны службы безопасности).

Профессионализм привилегированных пользователей означает, что они обладают необходимой квалификацией и навыками работы со средствами вычислительной техники и не могут совершить какие-либо непреднамеренные действия (бездействия), которые могут привести к реализации угроз безопасности информации. Высокий уровень профессиональной подготовки привилегированных пользователей должен поддерживаться за счет периодического повышения квалификации, прохождения курсов. Контроль уровня профессионализма привилегированных пользователей проводится в ходе периодических проверок квалификации (аттестаций). Периодичность повышения квалификации и проверок квалификации определяется регламентирующими документами эксплуатирующей организации.

Назначение и смена привилегированных пользователей, а также решение об их доверенности, в силу своей важности, должны быть утверждены приказами (распоряжениями) руководителя организации (подразделения), ответственного за обеспечение защиты информации. Кроме того, должны быть определены меры по обеспечению высокой степени профессиональной подготовки привилегированных пользователей и утверждены инструкции, регламентирующие порядок и правила выполнения привилегированными пользователями своих функциональных обязанностей.

При смене лиц, ответственных за эксплуатацию продукта или хранение ключевой информации, ключевую и аутентификационную информацию, к которой они имели доступ, следует считать скомпрометированной. В этом случае необходимо провести процедуру, описанную в п. 2.2.6.

4.3 Инициализация и ввод в эксплуатацию

4.3.1 Подготовка к работе

Подготовка продукта к работе выполняется администратором безопасности (лицом, ответственным за ввод продукта в эксплуатацию).

Перед вводом в эксплуатацию ViPNet Coordinator IG 5 необходимо:

1) проверить соблюдение требований, изложенных в подразделах 4.1, 4.2;
2) проверить ViPNet Coordinator IG 5 по критериям, приведенным в подразделе 3.1;

3) удостовериться в наличии, работоспособности и правильной настройке дополнительных средств, необходимых для совместного функционирования с ViPNet Coordinator IG 5. Требования к настройкам дополнительных средств, перечисленных в подразделе 1.5, приведены в п. 4.3.3;
4) удостовериться в отсутствии подключенного дополнительного оборудования, не предусмотренного требованиями и рекомендациями настоящих правил пользования и других эксплуатационных документов на ViPNet Coordinator IG 5.

При необходимости (неустранимые ошибки, замена оборудования или иные ситуации, требующие восстановления компонентов ViPNet Coordinator IG 5), администратор безопасности может произвести переустановку СПО ViPNet Coordinator IG 5 (кроме ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1).

4.3.2 Процедура подключения

Подключение ViPNet Coordinator IG 5 выполняется администратором безопасности (лицом, ответственным за ввод продукта в эксплуатацию). К подключению ViPNet Coordinator IG 5 допускаются лица, изучившие эксплуатационную документацию на ViPNet Coordinator IG 5.

При условии использования в ViPNet Coordinator IG 5 3G/4G-модема[10] потребуется установка SIM-карты[11]. Для этого администратор безопасности должен выполнить следующие действия:

- удалить защитную пломбу и открыть крышку разъема для SIM-карты;
- установить SIM-карту в соответствии с документом [15];
- в соответствии с регламентом эксплуатирующей организации выполнить пломбирование корпуса, т. е. нанести защитные пломбы и занести в раздел 12 «Особые отметки» формуляра запись об установке SIM-карты, содержащую следующие сведения:
  - дата, время и место проведения работ;
  - должность, фамилия, инициалы и подпись сотрудника, проводившего работы;
  - перечень произведенных работ (установка или замена SIM-карты);
  - серийный номер пломбы (при необходимости).

Перед началом эксплуатации ViPNet Coordinator IG 5 на нем должны быть установлены справочники и ключи. Существует несколько способов установки справочников и ключей на

[10] Входит в комплект поставки по согласованию с заказчиком.
[11] SIM-карта не входит в комплект поставки ViPNet Coordinator IG 5.

ViPNet Coordinator IG 5 (способ установки зависит от способа подключения к ViPNet Coordinator IG 5):

– через компьютер по каналу Ethernet и протоколу TFTP[12] при подключении к ViPNet Coordinator IG 5 компьютера через сетевой кросс-кабель или патч-корд Ethernet и технологический адрес;
– через консоль или с помощью монитора и клавиатуры[13] с использованием ключевого носителя, подключенного к ViPNet Coordinator IG 5 .

На компьютере должны быть включены стандартные службы Telnet (или SSH) и TFTP, которые необходимы для выполнения следующих функций:

– для подключения к ViPNet Coordinator IG 5 (Telnet или SSH);
– для переноса справочников и ключей на ViPNet Coordinator IG 5 (TFTP).

В целях обеспечения правил электробезопасности перед подключением компьютера для локального управления ViPNet Coordinator IG 5 необходимо выключать ViPNet Coordinator IG 5, а также отключать аппаратную платформу от сети электропитания.

Периферийные устройства подключаются к ViPNet Coordinator IG 5 только на время проведения соответствующих работ (ввод в эксплуатацию, резервное копирование конфигурационных файлов и другое). По завершении работ порты для подключения периферийных устройств должны быть опечатаны, ViPNet Coordinator IG 5 работает в автономном режиме.

Подробное описание процедуры подключения ViPNet Coordinator IG 5 приведено в документе [9].

4.3.3 Требования к настройкам

Настройка ViPNet Coordinator IG 5 выполняется администратором безопасности. Конфигурация ViPNet Coordinator IG 5 должна соответствовать требованиям эксплуатационных документов ViPNet Coordinator IG 5 в полном объеме. Для изменения параметров необходимо ввести пароль администратора безопасности и выполнить следующие действия:

1. Настроить сетевые фильтры в соответствии с [8] и [11].
2. Настроить сетевые интерфейсы в соответствии с [8] и [11].
3. Настроить маршрутизацию IP-трафика в соответствии с [8] и [11].

[12] TFTP (Trivial File Transfer Protocol – простой протокол передачи файлов) используется главным образом для первоначальной загрузки бездисковых рабочих станций.
[13] Только для ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.

Примечание – Для проверки подлинности маршрутов, полученных с других маршрутизаторов по протоколу OSPF, необходимо включить и настроить OSPF-аутентификацию на маршрутизаторах.

4. Включить регистрацию в журнале всех IP-пакетов и настроить размер журнала и интервал агрегации, исходя из интенсивности трафика, проходящего через сетевой узел.
5. Убедиться, что включено использование драйвера watchdog (параметру reboot в файле failover.ini присвоено значение yes), при необходимости включить его.
6. Проверить тип аутентификации пользователя (ввести команду hostname# iplir show authentication-type).

Примечание – Способ аутентификации задается администратором сети ViPNet в программе ViPNet Prime для всех узлов сети ViPNet, и его нельзя изменить на ViPNet Coordinator IG 5.

7. Если предполагается выполнять антивирусную проверку трафика[14, 15], синхронизировать время на ICAP-сервере антивирусного средства с ViPNet Coordinator IG 5.

Подробное описание необходимых настроек, в том числе настроек дополнительных средств, приведено в документах [8], [11], [13], [14], а также в эксплуатационной документации на дополнительные средства.

4.3.4 Ввод в эксплуатацию

Ввод в эксплуатацию выполняет администратор безопасности (лицо, уполномоченное эксплуатирующей организацией). Подробный порядок ввода в эксплуатацию, включая процедуру инициализации и развертывания ключевой системы, приведен в документе [9].

По завершении инициализации должна быть выполнена настройка СПО ViPNet Coordinator IG 5 в соответствии с требованиями п. 4.3.3 и контроль его работоспособности в соответствии с п. 5.6.1.

По завершении работ неиспользуемые порты для подключения периферийных устройств необходимо опечатать.

На каждый ViPNet Coordinator IG 5 должен оформляться акт о вводе в эксплуатацию по типовой форме, принятой в эксплуатирующей организации. Пример формы акта приведен в приложении Б. Акт должен храниться у лица, ответственного за эксплуатацию продукта.

[14] Для исполнений ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1.
[15] Пользователем (эксплуатирующей организацией) должны использоваться средства антивирусной защиты, сертифицированные на соответствие требованиям ФСБ России и (или) ФСТЭК России.

Факт ввода ViPNet Coordinator IG 5 в эксплуатацию фиксируется в журнале поэкземплярного учета СКЗИ.

Факт закрепления ViPNet Coordinator IG 5 за лицом, ответственным за его эксплуатацию, фиксируется в формуляре [7].

5 Требования по обеспечению безопасности при эксплуатации

5.1 Общие требования по защите от несанкционированного доступа

Эксплуатация ViPNet Coordinator IG 5 должна осуществляться в полном соответствии с требованиями, изложенными в настоящих ПП и другой эксплуатационной документации на продукт.

В эксплуатирующей организации должна быть разработана и реализована политика информационной безопасности, включающая в себя организационно-технические и административные мероприятия, связанные с:

- установлением требований к размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены ViPNet Coordinator IG 5, и (или) хранятся ключевые носители к ним (см. п. 2.2.3), а также контролем за выполнением этих требований;
- обеспечением правильности функционирования ViPNet Coordinator IG 5;
- обеспечением правильности обработки и передачи информации;
- установлением правил и регламентов для сотрудников, допущенных к работе с информацией ограниченного доступа, и контролем за их соблюдением.

Ответственность за эксплуатацию ViPNet Coordinator IG 5, соблюдение требований и рекомендаций ПП и других эксплуатационных документов, а также за обеспечение конфиденциальности защищаемой информации при эксплуатации ViPNet Coordinator IG 5 несет администратор безопасности.

При эксплуатации продукта запрещается:

- оставлять без контроля ViPNet Coordinator IG 5 после прохождения аутентификации пользователя и до завершения сеанса работы;
- вносить не предусмотренные настоящими ПП изменения в СПО продукта или в его настройки;
- игнорировать установку критически важных обновлений, полученных от изготовителя;
- вскрывать корпус ViPNet Coordinator IG 5 либо применять к нему иное воздействие, которое может привести к нарушению целостности корпуса, за исключением случаев, предусмотренных эксплуатационной документацией на продукт;
- нарушать ограничения по использованию продукта, приведенные в п. 1.4.2;
- выполнять удаленное подключение к ViPNet Coordinator IG 5 с незащищенных сетевых узлов (любых сетевых узлов вне сети ViPNet);

– предоставлять доступ к ViPNet Coordinator IG 5 с использованием средств, отличных от перечисленных в подразделе 1.6;
– разглашать аутентификационную информацию и пароли доступа;
– нарушать правила обращения с ключевой информацией, ключевыми носителями и устройствами аутентификации, приведенные в п. 2.2.1;
– нарушать правила режима и охраны в помещении с размещенным ViPNet Coordinator IG 5;
– подключать к ViPNet Coordinator IG 5 дополнительное оборудование, не предусмотренное актом о вводе в эксплуатацию;
– нарушать функционирование других средств защиты информации в защищаемой ИС или иным способом нарушать правила политики безопасности эксплуатирующей организации;
– иным способом нарушать правила эксплуатации ViPNet Coordinator IG 5 либо умышленно скрывать факты нарушения правил эксплуатации.

В ViPNet Coordinator IG 5 при условии использования в ViPNet Coordinator IG 5 3G/4G-модема[16] допускается устанавливать SIM-карту[17] (в соответствии с документом [15]).

При несоблюдении требований правил пользования и другой эксплуатационной документации гарантии изготовителя и действие сертификатов соответствия требованиям ФСБ России и ФСТЭК России на продукт не распространяются.

Контроль соблюдения правил эксплуатации, а также все действия по обслуживанию и настройке введенного в эксплуатацию ViPNet Coordinator IG 5 должны выполняться администратором безопасности (лицом, уполномоченным для этого эксплуатирующей организацией) не реже 1 раза в месяц. Допускается совмещать эти проверки с регламентным контролем работоспособности продукта (см. п. 5.6.1).

5.2 Требования к аутентификации и разграничению доступа

В ViPNet Coordinator IG 5 предусмотрено разграничение полномочий субъектов доступа (пользователей) на основе ролевой модели управления доступом.

Поддерживаются следующие роли субъектов доступа:

– аудитор;
– администратор.

Аудитор может просматривать настройки и журналы ViPNet Coordinator IG 5.

[16] Входит в комплект поставки по согласованию с заказчиком.
[17] SIM-карта не входит в комплект поставки ViPNet Coordinator IG 5.

Администратор может изменять настройки ViPNet Coordinator IG 5, выполнять резервное копирование и восстановление настроек ViPNet Coordinator IG 5, выполнять экспорт журналов регистрации событий, а также просматривать их, обновлять СПО ViPNet Coordinator IG 5.

Подробное описание функций, полномочий, обязанностей и ограничений, а также особенностей аутентификации и доступных средств управления для каждой роли приведено в документах [8], [9], [11].

До прохождения аутентификации с ролями администратора или аудитора пользователю ViPNet Coordinator IG 5 предоставляются права, минимально необходимые и достаточные для использования сетевых сервисов продукта и выполнения криптографических операций при работе с ним.

Кроме того, доступ к ViPNet Coordinator IG 5 имеют пользователи ViPNet Prime со следующими ролями:

– аудитор устройства;
– пользователь из группы администраторов ViPNet Prime.

Перечень доступных каждой роли ViPNet Prime действий определен в документах [10], [16], [17].

ViPNet Coordinator IG 5 поддерживает учетные записи пользователей двух типов:

– локальные;
– централизованные.

К локальным учетным записям относятся:

– учетная запись user с ролью аудитора (пароль по умолчанию – user). Используется при инициализации ViPNet Coordinator IG 5, после чего блокируется. Чтобы использовать учетную запись user после инициализации ViPNet Coordinator IG 5, необходимо разблокировать ее в соответствии с [8];
– учетная запись admin с ролью администратора (пароль задается при инициализации ViPNet Coordinator IG 5).

Примечание – Изменить имена локальных учетных записей user и admin, их роли, или добавить другие локальные учетные записи невозможно.

Централизованные учетные записи – учетные записи пользователей ViPNet Coordinator IG 5, созданные в ViPNet Prime. При использовании централизованной учетной записи пользователь будет иметь права администратора или аудитора в ViPNet Coordinator IG 5 в зависимости от роли его учетной записи в ViPNet Prime.

Имя централизованной учетной записи может совпадать с именем локальной (user или admin). В таком случае в качестве имени пользователя в командном интерпретаторе ViPNet Coordinator IG 5 необходимо вводить префикс center\ (например, center\admin). Ограничения на количество централизованных учетных записей отсутствуют.

Доступ к функциям ViPNet Coordinator IG 5 возможен только после аутентификации пользователей.

Аутентификация пользователя выполняется с помощью:

1) сертификата;
2) пароля.

Примечание – Использование аутентификации только по паролю возможно только в монопользовательском режиме.

Аутентификация по паролю доступна как при локальном, так и удаленном подключении к ПАК по протоколам SSH и HTTP/HTTPS. Доступ по протоколам SSH и HTTP/HTTPS возможен только при соблюдении условий, приведенных в подразделе 1.6.

Пароли должны соответствовать следующим требованиям:

- минимальная длина пароля 8 символов;
- максимальная длина пароля 31 символ;
- в пароле должны присутствовать символы каждой из следующих категорий:
  - строчные буквы английского алфавита от «a» до «z»;
  - прописные буквы английского алфавита от «A» до «Z»;
  - десятичные цифры от «0» до «9»;
  - символы, не принадлежащие к алфавитно-цифровому набору «!», «@», «#», «$», «%», «^», «&», «*», «(», «)», «-», «_», «+», «=», «;», «:», «'», «"», «,», «.», «<», «>», «/», «?», «\», «|», «`», «~», «[», «]», «{», «}»;
- использование трех и более символов, расположенных подряд на клавиатуре, недопустимо;
- использование трех и более символов, идущих подряд в алфавитном порядке, недопустимо;
- задание пароля, совпадающего с одним из трех последних паролей, недопустимо;
- пароли должны быть случайны и не связаны каким-либо образом с конкретным пользователем, например, с датой его рождения.

Смена пароля должна выполняться пользователями не реже 1 раза в 180 дней. Контроль за своевременной сменой пароля выполняет пользователь этого пароля.

Ответственность за соответствие паролей требованиям настоящих ПП и частоту их смены несет пользователь ViPNet Coordinator IG 5.

Способ аутентификации устанавливается в ViPNet Prime для всех узлов сети ViPNet. Его нельзя изменить на ViPNet Coordinator IG 5.

Аутентификация на ViPNet Coordinator IG 5 с использованием централизованных учетных записей возможна только при наличии доступа ViPNet Coordinator IG 5 к ViPNet Prime.

Локальный доступ пользователей к ViPNet Coordinator IG 5 выполняется по сертификату.

Удаленный доступ к ViPNet Coordinator IG 5 по протоколу SSH для пользователей с централизованной учетной записью запрещен. Пользователи с локальными учетными записями могут выполнить аутентификацию по паролю.

Удаленный доступ к ViPNet Coordinator IG 5 по протоколу HTTP/HTTPS для пользователей с локальными учетными записями предоставляется после аутентификации по паролю, а для пользователей с централизованными учетными записями – по сертификату.

Порядок доступа к ViPNet Coordinator IG 5 с использованием локальных и централизованных учетных записей описан в документах [8] и [11].

Для аутентификации по сертификату используется устройство аутентификации, на котором хранятся сертификат и закрытый ключ пользователя.

Устройство аутентификации использует два PIN-кода:

– PIN-код администратора для очистки памяти устройства аутентификации и сброса PIN-кода пользователя. Задается средством управления устройством аутентификации (USB-токеном);
– PIN-код пользователя для доступа к сертификату в памяти устройства аутентификации. Задается на ViPNet Coordinator IG 5 (только для локальных пользователей) или средством управления устройством аутентификации (USB-токеном).

Первичная аутентификация пользователя выполняется при инициализации ViPNet Coordinator IG 5. Используются данные локальной учетной записи аудитора (имя пользователя user и пароль user). Затем в процессе инициализации задается пароль локальной учетной записи администратора admin. В процессе эксплуатации ViPNet Coordinator IG 5 данный пароль может быть изменен (см. документы [8] и [11]).

После инициализации ViPNet Coordinator IG 5 локальная учетная запись аудитора user отключена. Для использования данной учетной записи необходимо включить ее и задать пароль.

В процессе инициализации при установке в ViPNet Coordinator IG 5 дистрибутива ключей задается PIN-код пользователя устройства аутентификации. Данный PIN-код будет использоваться локальным администратором admin для доступа к сертификату на устройстве аутентификации при аутентификации на ViPNet Coordinator IG 5.

Подробно процесс инициализации ViPNet Coordinator IG 5 описан в документе [9].

При ошибке аутентификации, например, когда ключ на устройстве аутентификации не соответствует сертификату, нарушена целостность сертификата или он отозван удостоверяющим центром, учетная запись блокируется на 10 минут.

После десяти неудачных попыток ввода PIN-кода доступ к устройству аутентификации будет заблокирован.

В данных случаях необходимо выпустить новый сертификат пользователя ViPNet Coordinator IG 5 согласно описанию, приведенному в документе [8].

Если пользователь ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1 не может пройти аутентификацию по ряду причин, например:

- истек срок действия ключей или лицензии в момент, когда не было связи с ViPNet Prime;
- некорректно обновлены справочники и ключи;
- утрачен пароль;
- программный сбой, неправильная настройка ПО или аппаратной платформы;
- замена батарейки на аппаратной платформе,

необходимо выполнить сброс к заводским настройкам, восстановить настройки ViPNet Coordinator IG 5 из резервной копии индивидуальной конфигурации (подробно о резервировании см. в п. 5.6.5). При отсутствии резервной копии индивидуальной конфигурации необходимо выполнить инициализацию ViPNet Coordinator IG 5. Подробно сброс к заводским настройкам и инициализация ViPNet Coordinator IG 5 описаны в документе [8].

Пользователем ViPNet Coordinator IG 5 (в эксплуатирующей организации) должны быть приняты меры по надежному сохранению в тайне PIN-кодов, паролей доступа, аутентификационной информации.

Ответственность за соблюдение требований по обеспечению безопасности при смене, хранении, вводе и уничтожении персональной аутентификационной информации должна быть возложена на владельца этой информации.

При обращении с аутентификационной информацией и устройствами аутентификации запрещено разглашать аутентификационную информацию в том числе выводить ее на дисплей, принтер и иные средства вывода и отображения информации, или передавать устройство аутентификации лицам, которым не разрешен доступ к нему. Также необходимо соблюдать

требования защиты ключевой информации на устройствах аутентификации, приведенные в п. 2.2.1.

При предоставлении некорректных аутентификационных данных доступ к функциям ViPNet Coordinator IG 5 блокируется.

ViPNet Coordinator IG 5 контролирует неуспешные попытки аутентификации. Пользователю дается три попытки для ввода правильного пароля без включения временной задержки доступа к механизмам аутентификации. После третьего ввода неправильного пароля делается прогрессивная задержка $3\times2^{(n-4)}$ сек., где n – номер попытки. При перезагрузке ViPNet Coordinator IG 5 счетчик не сбрасывается. Счетчик сбрасывается в случае успешной аутентификации. В случае использования неправильного имени пользователя попытки не учитываются, при этом счетчик на неуспешные попытки ввода пароля ведется раздельно для всех пользователей.

Все события успешной и неуспешной аутентификации пользователей фиксируются в журнале СКЗИ с указанием источника события (субъекта доступа).

При вводе пароля или PIN-кода вручную с клавиатуры вводимые символы скрываются.

В случае возможной компрометации (подозрении на компрометацию) аутентификационной информации пользователя и при условии, что доступ посторонних лиц к ключевой информации и к узлам защищаемой ИС невозможен, следует изменить аутентификационную информацию и продолжить работу. Если доступ посторонних лиц возможен, следует считать ключи скомпрометированными. Администратор ViPNet Coordinator IG 5 должен незамедлительно заблокировать доступ учетной записи данного пользователя к функциям продукта и выполнить процедуру смены его аутентификационной информации.

5.3 Режимы работы

Доступность функций ViPNet Coordinator IG 5 зависит от режима работы продукта.

В ViPNet Coordinator IG 5 при работе в качестве МЭ типа «А» и «Б» реализованы следующие режимы работы:

– режим инициализации;
– штатный режим;
– режим ограниченного функционирования.

В ViPNet Coordinator IG 5 при работе в качестве МЭ типа «Д» реализованы следующие режимы работы:

– режим инициализации;
– штатный режим;

– специальный режим;
– режим регламентного обслуживания;
– режим ограниченного функционирования.

Подробно режимы работы ViPNet Coordinator IG 5, способы и ограничения перехода между режимами описаны в документе [9]. Порядок действий для переключения между режимами работы ViPNet Coordinator IG 5 приведен в документах [8] и [11].

5.4 Регистрация событий

ViPNet Coordinator IG 5 ведет регистрацию (аудит, протоколирование) событий, значимых для эксплуатации. Регистрация событий выполняется автоматически. Ведутся следующие журналы регистрации событий:

– журнал регистрации IP-пакетов, в который заносится информация об IP-пакетах (зашифрованных и открытых), проходящих через сетевые интерфейсы ViPNet Coordinator IG 5;
– журнал пакетов промышленных протоколов, в который заносится информация обо всех пакетах, обработанных правилами фильтрации промышленных протоколов на прикладном уровне;
– журнал переключений кластера горячего резервирования, в который заносятся события о работе системы защиты от сбоев в режиме кластера горячего резервирования;
– журнал транспортных MFTP-конвертов, в который транспортный сервер (MFTP) записывает информацию о полностью принятых, отправленных, удаленных и поврежденных транспортных конвертах;
– журнал аудита, который содержит события, связанные с выполнением запросов пользователей, в том числе от ViPNet Prime и служебных запросов ViPNet Coordinator IG 5;
– журнал СКЗИ, который содержит события, связанные с криптографическими операциями, например, выпуском сертификатов локальных пользователей;
– журнал DNS-запросов, который содержит информацию о DNS-запросах, позволяющую следить, к каким ресурсам обращаются узлы сети и выявлять проблемы в настройках сети;
– системный журнал событий, в который записывается информация о важных программных и аппаратных событиях работы ViPNet Coordinator IG 5.

Защита файловой системы ViPNet Coordinator IG 5 от переполнения обеспечивается:

– для журнала регистрации IP-пакетов и журнала пакетов промышленных протоколов путем перезаписи более старых событий при заполнении файла журнала. Размер файла журнала задается администратором;
– для журнала аудита и системного журнала событий путем ротации при достижении файлом журнала размера, заданного администратором. В случае достижения предельного размера производится создание нового файла, текущий файл при этом сохраняется на внутренний носитель (диск) ViPNet Coordinator IG 5;
– для системного журнала, журнала аудита, журнала СКЗИ, журнала DNS-запросов и журнала транспортных MFTP-конвертов путем выгрузки на внешний носитель с возможной очисткой журналов на внутреннем носителе (диске) по команде администратора.

При достижении заданного администратором предельного размера файла генерируется предупреждение путем записи в системный журнал событий.

Доступ к журналам регистрации событий, а также защита записей журналов от удаления и подмены, контролируются механизмами ViPNet Coordinator IG 5.

Аудитору доступен просмотр журналов регистрации событий.

Администратору доступны следующие действия с журналами регистрации событий:

– просмотр журналов;
– управление настройками журналов;
– архивирование системного журнала событий (по умолчанию в архив добавляются ротированные файлы журнала);
– экспорт журналов (журнала регистрации IP-пакетов, журнала пакетов промышленных протоколов, журнала аудита, журнала СКЗИ и системного журнала событий).

Подробно порядок действий с журналами регистрации событий описан в документах [8] и [11].

Списки событий, регистрируемых в журнале регистрации IP-пакетов и системном журнале, приведены в документе [8]. Также в документе [8] описана структура записи журнала регистрации IP-пакетов для экспорта по сети в формате CEF.

5.5 Требования по обеспечению целостности

До включения ViPNet Coordinator IG 5 администратор обязан проверить:

– корпус продукта на наличие дефектов, позволяющих осуществить несанкционированный доступ (далее – НСД);

– целостность защитных пломб, печатей на корпусе продукта, портах ввода-вывода;
– целостность и подлинность СЗЗ на корпусе аппаратной платформы (см. методику в подразделе 3.1);
– отсутствие подключенных к продукту устройств, не предусмотренных актом о вводе в эксплуатацию.

В ViPNet Coordinator IG 5 предусмотрены следующие меры контроля целостности аппаратной платформы:

– пусковые тесты для контроля целостности и работоспособности составных частей аппаратной платформы, необходимых для загрузки СПО ViPNet Coordinator IG 5;
– контроль целостности файловой системы на носителе NAND flash;
– контроль работоспособности сетевого оборудования (только в режиме кластера горячего резервирования).

Контроль целостности и работоспособности составных частей аппаратной платформы продукта, необходимых для загрузки СПО ViPNet Coordinator IG 5, выполняется встроенными в загрузчик U-Boot[18] или BIOS[19] средствами.

ViPNet Coordinator IG 5 оснащен встроенными механизмами контроля целостности СПО ViPNet Coordinator IG 5. При обнаружении неустранимых ошибок или нарушения целостности СПО ViPNet Coordinator IG 5 администратор получает сообщение о невозможности продолжения эксплуатации ViPNet Coordinator IG 5. Подробнее порядок действий администратора безопасности в таком случае описан в п. 5.6.6.

Перезагрузка ViPNet Coordinator IG 5 должна выполняться не реже, чем 1 раз в месяц. Перезагрузка может выполняться путем ввода в командном интерпретаторе команды machine reboot, с помощью веб-интерфейса или удержанием в течение 1-2 с кнопки Reset на передней панели ViPNet Coordinator IG 5[20].

В ViPNet Coordinator IG 5 также предусмотрен контроль целостности:

– образа начальной файловой системы;
– образа сжатой файловой системы ПО ViPNet;
– исполняемых и конфигурационных файлов СПО ViPNet Coordinator IG 5;
– файлов справочников и ключей.

Проверка целостности указанных файлов выполняется в следующих случаях:

– автоматически при включении ViPNet Coordinator IG 5 – пусковой контроль;

[18] Кроме исполнения ViPNet Coordinator IG1000 Q1.
[19] Только для исполнения ViPNet Coordinator IG1000 Q1.
[20] Кнопка Reset отсутствует на ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.

– автоматически 2 раза в сутки – периодический контроль;

– автоматически при обновлении СПО ViPNet Coordinator IG 5;

– администратором ViPNet Coordinator IG 5 с помощью команды machine self-test.

Автоматическая проверка целостности файлов выполняется средствами ViPNet Coordinator IG 5 с помощью встроенных скриптов. Список исполняемых файлов, контроль целостности которых критически важен с точки зрения безопасности функционирования продукта, приведен в разделе 11 «Контрольные суммы» формуляра [7].

Если обнаружено нарушение целостности данных в рамках пускового контроля, то загрузка ViPNet Coordinator IG 5 продолжается с предупреждением о нарушении целостности данных. Старт служб ПО ViPNet не выполняется, все сетевые интерфейсы отключаются (далее – режим ограниченного функционирования, подробнее о режимах функционирования ViPNet Coordinator IG 5 описано в документе [9]), но администратор ViPNet Coordinator IG 5 может сохранить конфигурацию и (или) воспользоваться инструкцией документа [8] по приведению ViPNet Coordinator IG 5 в состояние целостности.

При каждом старте служб ПО ViPNet происходит проверка контрольных сумм исполняемых модулей из состава ПО ViPNet и файлов конфигурации ViPNet Coordinator IG 5, защищенных контрольными суммами. Если обнаружено нарушение целостности ПО, то отображается сообщение об этом, а соответствующая служба не запускается.

Периодический контроль целостности файлов выполняется автоматически с интервалом 12 часов. Проверка адресных справочников и файлов конфигурации сервисов ПО ViPNet при этом не выполняется. При каждой периодической проверке в системный журнал заносится запись, содержащая время и результаты проверки. Для просмотра информации о последней периодической проверке используется команда admin show check integrity status. При обнаружении нарушения целостности в результате периодического контроля целостности ViPNet Coordinator IG 5 автоматически перезагружается.

Также контроль целостности СПО ViPNet Coordinator IG 5 должен выполняться администратором ViPNet Coordinator IG 5. Периодичность контроля целостности определяется внутренними правилами эксплуатирующей организации, но при этом контроль должен производиться не реже 1 раза в месяц.

Для выполнения контроля целостности СПО ViPNet Coordinator IG 5 реализована команда тестирования machine self-test. С помощью этой команды администратор ViPNet Coordinator IG 5 может проверить состояние файловых систем, целостность загружаемых образов файловых систем с СПО, целостность контрольных сумм исполняемых файлов и библиотек СПО ViPNet внутри распакованных в память образов, а также файлов конфигурации программ СПО ViPNet и ViPNet Coordinator IG 5.

Результат контроля целостности выводится на экран. Контрольные суммы исполняемых файлов должны соответствовать контрольным суммам, указанным в разделе 11 формуляра [7].

В случае нарушения целостности файлов СПО:

– на экран выводится сообщение о нарушении целостности файла;
– в журнале СКЗИ фиксируется факт нарушения целостности;
– если для искаженного файла имеется резервная копия, файл автоматически восстанавливается (см. п. 5.6.6);
– если резервная копия искаженного конфигурационного файла не найдена, службы, отвечающие за работу в сети ViPNet, не будут запущены либо будут остановлены. Сетевые интерфейсы будут выключены.

В случае обнаружения нарушения целостности администратор ViPNet Coordinator IG 5 обязан:

1) отключить ViPNet Coordinator IG 5 от каналов связи до устранения неисправностей;
2) провести расследование с целью выяснения возможных причин возникновения неисправностей;
3) провести анализ журналов регистрации событий для определения причин сбоя, а также выявления попыток НСД и сетевых атак;
4) при обнаружении признаков НСД к ViPNet Coordinator IG 5 уведомить администратора ViPNet Prime о возможной компрометации ключей узла;
5) устранить обнаруженные причины возникновения неисправностей или искажений данных;
6) предпринять действия для восстановления работоспособности ViPNet Coordinator IG 5 (см. п. 5.6.6);
7) принять решение о возможной компрометации ключей и выполнить соответствующие действия (см. п. 2.2.5);
8) при необходимости произвести обновление ключей узла (процедура обновления ключей описана в документе [8]).

5.6 Порядок обеспечения работоспособности

5.6.1 Порядок контроля работоспособности

Контроль работоспособности выполняется автоматически встроенными средствами ViPNet Coordinator IG 5 в следующих случаях:

– при включении ViPNet Coordinator IG 5;

– в процессе штатного функционирования ViPNet Coordinator IG 5.

ViPNet Coordinator IG 5 выполняет:

– проверку работоспособности криптографических алгоритмов;
– проверку работоспособности СПО;
– самотестирование встроенных механизмов контроля работоспособности.

Проверка работоспособности криптографических алгоритмов ViPNet Coordinator IG 5 включает в себя тестовые проверки криптографических функций драйвера шифрования. Тестовая проверка работоспособности драйвера шифрования производится один раз в 10 минут путем тестового выполнения функций шифрования и формирования имитовставки.

В состав ViPNet Coordinator IG 5 входит криптопровайдер, включающий криптографические библиотеки. Криптопровайдер проверяет свою работоспособность автоматически с помощью встроенных механизмов проверки работоспособности.

При загрузке СПО ViPNet Coordinator IG 5 система защиты от сбоев ViPNet Coordinator IG 5 выполняет постоянный контроль работоспособности основных служб ViPNet с момента старта с установкой периода оповещения.

Регламентный контроль работоспособности выполняется администратором ViPNet Coordinator IG 5 (лицом, уполномоченным эксплуатирующей организацией) в следующих случаях:

– при вводе ViPNet Coordinator IG 5 в эксплуатацию;
– при обновлении СПО ViPNet Coordinator IG 5;
– при изменении лица, ответственного за эксплуатацию ViPNet Coordinator IG 5;
– при подозрении на компрометацию или иной нештатной ситуации, возникшей в процессе эксплуатации;
– периодически 1 раз в год.

Список проверок, относящихся к регламентному контролю, приведен в приложении А.

Если политикой эксплуатирующей организации предусмотрено протоколировать результаты проведения регламентного контроля работоспособности, может быть использована форма протокола, приведенная в приложении А. Протоколы заверяются подписью лица, ответственного за эксплуатацию ViPNet Coordinator IG 5.

По окончании регламентного контроля дополнительные устройства, используемые для проверки, необходимо отключить, порты для подключения периферийных устройств опечатать.

При обнаружении фактов сбоев в работе ViPNet Coordinator IG 5 администратор ViPNet Coordinator IG 5 обязан:

1) отключить ViPNet Coordinator IG 5 от каналов связи до устранения неисправностей;
2) провести расследование с целью выяснения возможных причин возникновения неисправностей, провести анализ журнала регистрации событий с целью выявления попыток НСД и сетевых атак;
3) восстановить работоспособность ViPNet Coordinator IG 5 (см. п. 5.6.6);
4) принять меры для устранения выявленных нарушений и для предотвращения их повторения в дальнейшем.

Требования к контролю работоспособности дополнительных средств, необходимых для выполнения ViPNet Coordinator IG 5 заявленных в формуляре функций и соответствия заявленным требованиям, но не входящих в комплект поставки ViPNet Coordinator IG 5, приведены в эксплуатационной документации на эти средства.

В ViPNet Coordinator IG 5 реализован контроль состояния оборудования[21], который позволяет выявить причины неполадок и предотвратить выход из строя оборудования. Пользователь ViPNet Coordinator IG 5 имеет возможность просмотреть информацию, например:

– о перегреве процессора или модема;
– о состоянии дисковой памяти;
– о состоянии модема и установленном мобильном соединении.

Описание команд, которые используются для проверки состояния оборудования ViPNet Coordinator IG 5, приведено в документах [8] и [14].

Информация о перегреве оборудования и работе модема фиксируется также в системном журнале.

Также пользователь ViPNet Coordinator IG 5 имеет возможность запустить проверку дополнительной памяти с автоматическим восстановлением поврежденных секторов[21]. Подробное описание приведено в документах [8] и [14].

5.6.2 Тестирование функционирования ViPNet Coordinator IG 5

Тестирование функционирования ViPNet Coordinator IG 5 необходимо проводить администратору ViPNet Coordinator IG 5 периодически 1 раз в месяц (периодичность может

[21] Кроме ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.

устанавливаться внутренними правилами эксплуатации в организации). Тестирование ViPNet Coordinator IG 5 включает в себя:

– тестирование работы фильтров защищенной сети;
– тестирование работы фильтров открытой сети;
– регламентное тестирование работы ViPNet Coordinator IG 5.

Тестирование функционирования ViPNet Coordinator IG 5 должно проводиться в соответствии с методиками, приведенными в пп. 5.6.3–5.6.4.

5.6.3 Тестирование работы фильтров защищенной сети

Для проведения тестирования необходимо установить и настроить (на уровне сетевого доступа) любую имеющуюся защищенную станцию с установленным ПО ViPNet (далее – узел B), причем эта станция должна иметь связь со станцией ViPNet Coordinator IG 5 (далее – узел A).

Методика тестирования приведена в таблице 2. Для каждого пункта, выполняемого в ходе тестирования, необходимо проверить правильность статистики IP-пакетов на соответствующем интерфейсе, а также появление записей в журнале регистрации IP-пакетов с соответствующими типами событий.

Таблица 2 – Методика тестирования работы фильтров защищенной сети

Проверяемое свойство	Действие	Ожидаемый результат
Проверка работы фильтра по умолчанию для защищенного узла	На узле A для узла B удалить фильтр по умолчанию (секция VPN) для ICMP-протокола. Выполнить проверку доступа к узлу B (с помощью команды inet ping)	Запрос по команде inet ping не проходит. Исходящие пакеты блокируются с кодом события 3
Проверка работы фильтра для исходящих пакетов	На узле A для узла B добавить фильтр (в секцию VPN), разрешающий исходящие ICMP-пакеты с типом 8. Выполнить проверку доступа к узлу B (с помощью команды inet ping)	Запрос по команде inet ping проходит. Исходящие пакеты пропущены с кодом события 40
Проверка работы фильтра для входящих пакетов	На узле A для узла B удалить правило, созданное в предыдущем шаге, и добавить фильтр (в секцию VPN), запрещающий входящие ICMP-пакеты с типом 8. Выполнить проверку доступа к узлу B (с помощью команды inet ping)	Запрос по команде inet ping не проходит. Входящие пакеты блокированы с кодом события 3

5.6.4 Тестирование работы фильтров открытой сети

Для подготовки к тестированию необходимо установить и настроить (на уровне сетевого доступа) узел B, то есть станцию без какого-либо ПО, ограничивающего сетевой трафик.

Методика тестирования приведена в таблице 3. Для каждого пункта методики, выполняемого в ходе тестирования, необходимо проверить правильность статистики IP-пакетов на соответствующем интерфейсе, а также появление записей в журнале IP-пакетов с соответствующими типами событий.

Таблица 3 – Методика тестирования работы фильтров открытой сети

Проверяемое свойство	Действие	Ожидаемый результат
Исходящие открытые пакеты	На узле А проверить, что в секции открытой сети (local) есть разрешающие правила для исходящего icmp-протокола. Попытаться проверить доступ к узлу В (с помощью команды inet ping)	Запрос по команде inet ping проходит. Исходящие пакеты пропущены с кодом события 60
Входящие открытые пакеты	На узле А для узла В проверить, что в секции открытой сети (local) нет разрешающего правила для входящего icmp-протокола. Попытаться проверить доступ к узлу А с узла В (с помощью системной утилиты ping)	Запрос по команде ping не проходит. Входящие пакеты блокируются с кодом события 30

5.6.5 Порядок резервирования

Критически важные файлы СПО ViPNet Coordinator IG 5 автоматически копируются в резервный раздел диска (см. подраздел 5.5).

В ViPNet Coordinator IG 5 реализована возможность создания внешней резервной копии настроек:

– копии конфигурации VPN;

– индивидуальной конфигурации ViPNet Coordinator IG 5;

– универсальной конфигурации ViPNet Coordinator IG 5.

Копия конфигурации VPN – совокупность настроек ViPNet Coordinator IG 5, с помощью которой можно быстро переключиться между различными конфигурациями VPN и межсетевого экрана.

Копии конфигурации VPN могут создаваться:

– автоматически перед обновлением СПО или справочников и ключей;

– вручную по команде администратора ViPNet Coordinator IG 5.

Копии конфигурации VPN сохраняются в памяти ViPNet Coordinator IG 5. Подробно работа с копиями конфигурации VPN описана в документе [8].

Индивидуальная конфигурация позволяет выполнить возврат настроек ViPNet Coordinator IG 5 к состоянию, которое было на момент ее создания. Файл индивидуальной конфигурации зашифрован на ключе обмена и может быть использован только

на том ViPNet Coordinator IG 5, на котором установлен тот же дистрибутив ключей, при котором индивидуальная конфигурация была создана.

Индивидуальная конфигурация может использоваться:

– для восстановления настроек ViPNet Coordinator IG 5 в случае сбоя или некорректного обновления СПО;
– при замене неисправного ViPNet Coordinator IG 5, в том числе в кластере горячего резервирования.

Резервное копирование индивидуальной конфигурации может быть выполнено:

– автоматически на сервер ViPNet Prime по расписанию. По умолчанию резервное копирование происходит автоматически раз в сутки;
– вручную по команде администратора ViPNet Coordinator IG 5 на сервер ViPNet Prime, USB-носитель или в папку компьютера, подключенного к ViPNet Coordinator IG 5 (АРМ администратора).

Подробно работа с копиями индивидуальной конфигурации ViPNet Coordinator IG 5 описана в документах [8] и [11].

Универсальная конфигурация предназначена для переноса настроек ViPNet Coordinator IG 5 с одного координатора на другой (между ПАК в одинаковых исполнениях). Экспорт универсальной конфигурации может быть выполнен по команде администратора ViPNet Coordinator IG 5 в папку компьютера, подключенного к ViPNet Coordinator IG 5 (АРМ администратора), и на USB-носитель. При экспорте файл универсальной конфигурации зашифровывается на пароле.

Подробно работа с копиями универсальной конфигурации ViPNet Coordinator IG 5 описана в документах [8] и [11].

Кроме того, в ViPNet Coordinator IG 5 реализовано локальное резервирование слепка СПО ViPNet Coordinator IG 5 с настройками продукта. Копии всех файлов, необходимых для функционирования ViPNet Coordinator IG 5, хранятся на резервном разделе накопителя ViPNet Coordinator IG 5 в открытом виде. Резервирование выполняется автоматически после каждой успешной проверки целостности при загрузке (перезагрузке) СПО (см. подраздел 5.5).

5.6.6 Восстановление работоспособности

Файловая система ViPNet Coordinator IG 5 организована таким образом, чтобы практически исключить необходимость вмешательства пользователя при сбоях (внезапное выключение питания, сопровождающееся порчей файловой системы), а также минимизировать последствия таких сбоев.

Восстановление работоспособности служб СПО ViPNet Coordinator IG 5 выполняется системой защиты от сбоев. Если контролируемая служба в течение периода оповещения не сообщила о своем состоянии или сообщила о внутреннем сбое, то система защиты от сбоев идентифицирует сбой службы и инициирует процедуру восстановления ее работоспособности. Для этого сначала делается попытка корректной остановки службы, в работе которой произошел сбой. Если эта попытка оказывается неудачной, то выполняется принудительная «некорректная» остановка службы. После этого система защиты от сбоев перезапускает остановленную службу.

В случае неисправностей, которые системе не удалось устранить автоматически, администратор ViPNet Coordinator IG 5 должен:

– удалить ключи;
– провести повторную инициализацию продукта и восстановить индивидуальные настройки ViPNet Coordinator IG 5 из резервной копии.

При возникновении неустранимых неисправностей ViPNet Coordinator IG 5 (кроме исполнения ViPNet Coordinator IG1000 Q1) администратором ViPNet Coordinator IG 5 может быть произведено восстановление работоспособности путем переустановки СПО ViPNet Coordinator IG 5 с последующей инициализацией (см. документ [9]) или восстановлением из резервной копии индивидуальной конфигурации (см. документы [8] и [11]). Подробное описание переустановки СПО ViPNet Coordinator IG 5 приведено в документе [8].

Если перечисленные действия не позволяют устранить неисправность, следует обратиться к изготовителю (см. п. 5.6.8).

Дополнительно в продукте реализована возможность работы в режиме кластера горячего резервирования. В случае выхода из строя ViPNet Coordinator IG 5, работающего в активном режиме, ViPNet Coordinator IG 5, работающий в пассивном режиме, автоматически переходит в активный режим и полностью восстанавливает работу сетевого узла.

Подробное описание процедуры восстановления работоспособности при сбоях и работы ViPNet Coordinator IG 5 в режиме кластера горячего резервирования приведено в документе [8].

5.6.7 Обновление ПО

Информация о выпуске обновлений ПО продукта (СПО и системного загрузчика U-Boot[22]) публикуется на сайте https://infotecs.ru.

[22] Системный загрузчик U-Boot не используется в ViPNet Coordinator IG 5 в исполнении ViPNet Coordinator IG1000 Q1.

Для своевременного получения информации о выпуске обновлений ПО продукта администратор сети ViPNet[23] должен подписаться на информационную рассылку «Поддержка» на сайте https://infotecs.ru.

Для получения обновления ПО продукта и информации по порядку его применения администратор сети ViPNet[23] должен обратиться к изготовителю ViPNet Coordinator IG 5. Администратор сети ViPNet[23] может получить обновления ПО ViPNet Coordinator IG 5 после предоставления сведений о сертификате технической поддержки.

В комплект обновления входит:

- файл обновления ПО ViPNet Coordinator IG 5, подписанный электронной подписью (для всех исполнений, кроме ViPNet Coordinator IG1000 Q1, файл обновления объединяет в одном архиве файлы СПО и системного загрузчика U-Boot);
- инструкция по обновлению;
- новый комплект эксплуатационной документации (при необходимости);
- бюллетень (при необходимости).

При получении комплекта обновления администратор сети ViPNet[23] должен убедиться в подлинности и целостности полученного файла обновления ПО продукта путем проверки его электронной подписи.

Дополнительно администратор сети ViPNet[23] может проверить целостность файла обновления ПО путем вычисления контрольной суммы и сравнения полученного значения с указанным в формуляре [7].

Контрольная сумма может быть вычислена:

- с использованием утилиты ViPNet HashCalc по алгоритму ГОСТ Р 34.11-2012, 256 бит;
- с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» версии 2.0.2 (разработчик АО «ЦБИ-сервис») по алгоритму «Уровень-3», программно.

Перед обновлением ПО рекомендуется экспортировать настройки ViPNet Coordinator IG 5 (см. п. 5.6.5), справочники, ключи, а также журнал IP-пакетов, журнал пакетов промышленных протоколов и системный журнал. Порядок экспорта приведен в документах [8], [11] и [18].

Реализовано два способа обновления ПО ViPNet Coordinator IG 5: с помощью ViPNet Prime и локально.

[23] Администратор ViPNet Coordinator IG 5 при условии выполнения им функций администратора сети ViPNet.

Обновление ПО ViPNet Coordinator IG 5 выполняется в соответствии с описанием, приведенным в документе [8].

На время обновления системного загрузчика U-Boot необходимо обеспечить гарантированное питание ViPNet Coordinator IG 5. Если обновление системного загрузчика U-Boot не пройдено успешно, то для восстановления ViPNet Coordinator IG 5 необходимо обратиться к изготовителю.

После успешного обновления ПО необходимо провести проверку настроек в соответствии с требованиями п. 4.3.3, а также проверку работоспособности в соответствии с требованиями п. 5.6.1.

Подробное описание процедуры установки и применения обновления ПО ViPNet Coordinator IG 5 приведено в документе [8].

Замена и (или) внесение соответствующих отметок в формуляр [7] при применении обновления производится администратором ViPNet Coordinator IG 5.

5.6.8 Порядок действий при выявлении уязвимостей в процессе эксплуатации

В случае выявления потенциальных уязвимостей, ошибок или несоответствий ViPNet Coordinator IG 5 документации на продукт, следует обратиться к изготовителю и сообщить о возникшей проблеме по электронной почте hotline@infotecs.ru, телефону, указанному на сайте https://infotecs.ru/, или заполнив форму на странице сайта: https://infotecs.ru/support. При обращении следует описать проблему, дату и условия возникновения и обнаружения.

Изготовитель, кроме того, выполняет регулярный поиск и устранение уязвимостей и других недостатков в ViPNet Coordinator IG 5 и выпуск соответствующих обновлений ПО.

Внеплановые обновления ПО для устранения обнаруженных уязвимостей ViPNet Coordinator IG 5 разрабатываются и выпускаются в срок не более 60 дней с момента выявления уязвимости и направляются пользователю (эксплуатирующей организации) в составе комплекта обновления (см. п. 5.6.7).

При получении от изготовителя информации о выявлении уязвимости необходимо в соответствии с полученными от изготовителя инструкциями реализовать компенсирующие меры по защите информации или временные ограничения по применению продукта, направленные на недопущение попыток эксплуатации выявленной уязвимости злоумышленниками (если на момент выявления информации об уязвимости нет доступных версий продукта с устраненной уязвимостью), либо выполнить обновление ПО продукта.

При получении от изготовителя информации о необходимости реализации ограничений по применению (разрабатываются изготовителем, если уязвимость невозможно устранить путем применения обновления) необходимо в соответствии с полученными от изготовителя инструкциями реализовать ограничения по применению продукта.

Если пользователь (эксплуатирующая организация) не может реализовать ограничение по применению продукта в соответствии с полученными от изготовителя инструкциями, эксплуатацию продукта следует прекратить.

При получении от изготовителя информации о невозможности устранения риска эксплуатации выявленной уязвимости с помощью компенсирующих мер и (или) путем обновления продукта эксплуатацию продукта следует прекратить.

6 Требования по обеспечению безопасности при выводе из эксплуатации и передаче в ремонт

При выводе из эксплуатации и утилизации ViPNet Coordinator IG 5 должны выполняться требования и рекомендации документа [12].

6.1 Порядок передачи в ремонт

Перед передачей ViPNet Coordinator IG 5 в ремонт администратор ViPNet Coordinator IG 5 должен:

- при наличии технической возможности:
  - выгрузить журналы регистрации событий на внешний носитель (см. подраздел 5.4);
  - выполнить резервирование настроек продукта (см. п. 5.6.5);
  - удалить введенную ключевую информацию (см. подраздел 2.3);
- поставить отметку о передаче в ремонт в разделе 12 «Особые отметки» формуляра [7].

Ремонт и техническое обслуживание ViPNet Coordinator IG 5 выполняется только предприятием-изготовителем. ViPNet Coordinator IG 5 подлежит передаче в ремонт только с формуляром [7].

При возврате ViPNet Coordinator IG 5 из ремонта необходимо заново ввести продукт в эксплуатацию в соответствии с требованиями подраздела 4.3 и проставить соответствующие отметки в формуляре [7].

6.2 Порядок вывода из эксплуатации

Вывод продукта из эксплуатации выполняет администратор ViPNet Coordinator IG 5.

При этом необходимо выполнить следующие действия:

1) отключить ViPNet Coordinator IG 5 от каналов связи;
2) удалить ключевую информацию, хранящуюся в ViPNet Coordinator IG 5 и на ключевых носителях, в соответствии с подразделом 2.3;
3) выключить ViPNet Coordinator IG 5;
4) поставить отметки о выводе ViPNet Coordinator IG 5 из эксплуатации в журнал поэкземплярного учета СКЗИ и в раздел 9 «Сведения о закреплении при эксплуатации» формуляра [7].

6.3 Утилизация

Решение об утилизации принимает владелец ViPNet Coordinator IG 5. Утилизация может быть проведена:

1. Владельцем продукта (либо эксплуатирующей организацией с разрешения владельца СКЗИ). Утилизация осуществляется комиссией в составе не менее двух человек из числа допущенных к эксплуатации СКЗИ. Получение специальной лицензии на уничтожение СКЗИ не требуется. При этом соблюдение требований к уничтожению СКЗИ, налагаемых данным разделом и документом [12] обязательно. При необходимости, определяемой порядком, действующим у владельца продукта (в эксплуатирующей организации), может потребоваться дополнительное согласование уничтожения СКЗИ с вышестоящей организацией, а также с органом криптографической защиты (при наличии).
2. Организацией-лицензиатом ФСБ или органом криптографической защиты на основании договора.

Утилизации подлежат:

– СПО ViPNet Coordinator IG 5, установленное на аппаратную платформу;
– ключевая информация и ключевые носители;
– оптический диск с дистрибутивом и эксплуатационной документацией из комплекта поставки ViPNet Coordinator IG 5;
– документация в бумажном виде;
– копии ключевой информации, дистрибутивов СПО, эксплуатационной документации в бумажном и электронном виде (при наличии копий).

Если требуется сохранение формуляра на ViPNet Coordinator IG 5 в бумажном виде, то в него должны быть внесены и заверены подписью уполномоченного лица следующие отметки:

– в раздел «Сведения о закреплении изделия при эксплуатации» внесены номер и дата приказа об освобождении за подписью ответственного лица;
– на титульный лист формуляра внесена запись «Не использовать при эксплуатации продукта».

Утилизацию необходимо выполнять с помощью сертифицированных средств гарантированного уничтожения информации. Если удаление информации невозможно без повреждения носителя, на котором она расположена, то необходимо уничтожить носитель любым способом, полностью исключающим возможность восстановления и использования информации.

После утилизации необходимо сделать соответствующую отметку в журнале поэкземплярного учета СКЗИ.

После выполнения вышеуказанных действий ограничения на дальнейшее использование аппаратной платформы не накладываются.

Список используемой литературы

1. ТС 26.2.001-2020 «Состав и содержание правил пользования средств криптографической защиты информации».
2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
4. Требования 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.
5. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.
6. Требования о защите информации, содержащейся в информационных системах общего пользования.
7. ViPNet Coordinator IG 5. Формуляр ФРКЕ.467759.003ФО.
8. ViPNet Coordinator IG 5. Настройка с помощью командного интерпретатора ФРКЕ.467759.003ИС2.
9. ViPNet Coordinator IG 5. Подготовка к работе ФРКЕ.467759.003ИС1.
10. ViPNet Prime. Руководство администратора организации ФРКЕ.00222-02 32 02.
11. ViPNet Coordinator IG 5. Настройка с помощью веб-интерфейса ФРКЕ.467759.003ИС4.
12. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.
13. ViPNet Coordinator IG 5. Сценарии работы ФРКЕ.467759.003ИС5.
14. ViPNet Coordinator IG 5. Справочник команд и конфигурационных файлов ФРКЕ.467759.003ИС6.
15. ViPNet Coordinator IG 5. Описание аппаратных платформ ФРКЕ.467759.003ИС7.
16. ViPNet Prime Key Center. Правила пользования ФРКЕ.00289-01 99 01.
17. ViPNet Prime. Руководство главного администратора ФРКЕ.00222-02 32 01.

18. ViPNet Coordinator IG 4. Настройка с помощью командного интерпретатора ФРКЕ.467759.001ИС2.

Настоящие правила пользования согласованы с ФСБ России

Приложение А

Пример формы протокола контрольной проверки ViPNet Coordinator IG 5

«___» _____ 20___ г.

ViPNet Coordinator IG 5 установлен

в_____

наименование подразделения

по адресу_____

в соответствии с эксплуатационной документацией и введен в эксплуатацию

в помещении №_____.

Акт о вводе в эксплуатацию №_____от _____.

Таблица А.1 – Состав и ожидаемые результаты проверок при регламентном контроле

№ п/п	Проверка	Ожидаемый результат	Результат (+/-)
1.	Провести проверку целостности аппаратной платформы на соответствие требованиям подраздела 5.5	Отсутствие внешних признаков НСД: – признаков вскрытия аппаратной платформы и нарушения целостности корпуса аппаратной платформы (например, нарушения целостности печатей или пломб); – признаков нарушения целостности и подлинности СЗЗ на корпусе аппаратной платформы; – подключенного дополнительного оборудования, не предусмотренного актом о вводе в эксплуатацию	
2.	Проверить механизм локальной аутентификации пользователя с ролью администратор по сертификату. Выполнить несколько попыток аутентификации с неправильным PIN-кодом, затем с правильным PIN-кодом	Механизм корректно реагирует на несколько попыток аутентификации с неправильным PIN-кодом: механизм препятствует аутентификации и каждый раз увеличивает время задержки перед возможностью следующей попытки аутентификации. Авторизация с правильным PIN-кодом проходит успешно	
3.	Проверить механизм аутентификации по протоколу SSH с защищенного узла, который имеет связь с ViPNet Coordinator IG 5. Для этого необходимо через SSH-клиент зайти на ViPNet Coordinator IG 5 и выполнить несколько попыток аутентификации пользователя с ролью администратор с	Механизм корректно реагирует на несколько попыток аутентификации с неправильным паролем. После каждой неудачной попытки аутентификации возникает задержка времени до следующей попытки аутентификации, величина задержки возрастает в зависимости от количества неудачных попыток аутентификации. Аутентификация с правильным паролем проходит успешно	

№ п/п	Проверка	Ожидаемый результат	Результат (+/-)
	неправильным паролем, затем с правильным паролем		
4.	Проверить механизм аутентификации средствами веб-интерфейса с любого защищенного узла, который имеет связь с ViPNet Coordinator IG 5[24]. Для этого необходимо через веб-браузер[25] зайти на ViPNet Coordinator IG 5 по его IP-адресу видимости на порт 8080 и выполнить аутентификацию пользователя с ролью администратор по паролю. Выполнить несколько попыток аутентификации с неправильным паролем, затем с правильным паролем	Механизм корректно реагирует на несколько попыток аутентификации с неправильным паролем. После каждой неудачной попытки аутентификации возникает задержка времени до следующей попытки аутентификации, величина задержки возрастает в зависимости от количества неудачных попыток аутентификации. Аутентификация с правильным паролем проходит успешно	
5.	Проверить целостность СПО продукта и файлов конфигурации с помощью команды machine self-test	Проверка прошла успешно. Наименования и контрольные суммы исполняемых файлов отображаются в полном объеме и соответствуют, указанным в формуляре [7]. Ошибок и нарушения контроля целостности не обнаружено	
6.	Проверить правильность настроек СПО продукта. Для этого необходимо сверить настройки в соответствии с п. 4.3.3	Настройки СПО ViPNet Coordinator IG 5 соответствуют настройкам, приведенным в п. 4.3.3	
7.	Проверить соединения с видимыми узлами сети ViPNet. Для этого необходимо в консоли ViPNet Coordinator IG 5 ввести команду iplir ping {id-узла, с которым нужно проверить соединение}	В консоли появляются сообщения о доступности сетевого узла	
8.	Проверить журналы регистрации событий	Отсутствуют события, свидетельствующие о проблемах безопасности или сбоях в работе	

[24] Проверка выполняется только для исполнений ViPNet Coordinator IG100 I1, ViPNet Coordinator IG100 I4, ViPNet Coordinator IG100 I5 и ViPNet Coordinator IG1000 Q1.
[25] Рекомендуется использовать браузеры Microsoft Edge, Google Chrome или Mozilla Firefox последних версий.

Приложение Б

Акт о вводе в эксплуатацию

АКТ №

ввода оборудования в эксплуатацию

г. _____ «___»_____ 20__ г.

Комиссия из представителей _____,

_____,

(иные лица)

назначенная распоряжением _____

(наименование заказчика)

№ _____ от "___"_____ 20__ г., ознакомившись с Продуктом ФРКЕ.467759.003 ViPNet Coordinator IG 5, изготовленным _____,

(наименование изготовителя)

размещенным по адресу: _____,

рассмотрев техническую документацию, представленную изготовителем,

и результаты эксплуатационных испытаний, проведенных в период с «___» _____ 20__ г. по «___»_____ 20__ г., установила:

1. Продукт ФРКЕ.467759.003 ViPNet Coordinator IG 5 соответствует заявленным требованиям, с учетом следующих замечаний: _____.

2. Установка, монтаж, пуско-наладочные работы выполнены в соответствии с проектом и с соблюдением Правил техники безопасности. Оборудование соответствует требованиям промышленной, пожарной и экологической безопасности.

3. Продукт ФРКЕ.467759.003 ViPNet Coordinator IG 5 выдержал испытания и может быть введено в эксплуатацию (или: только после устранения недостатков, отмеченных в Ведомости замечаний и предложений и препятствующих вводу в эксплуатацию).

Выводы:

Продукт ФРКЕ.467759.003 ViPNet Coordinator IG 5 ввести в эксплуатацию по адресу:

_____ с «___»_____ 20__ г.

(или: после устранения недостатков, отмеченных в Ведомости замечаний и предложений, препятствующих вводу оборудования в опытную эксплуатацию).

Приложения:

1. Протокол пуско-наладочных работ от «___»_____ 20__ г. № _____.
2. Ведомость замечаний и предложений от «___»_____ 20__ г. № _____.

Председатель комиссии _____

(подпись)

Члены комиссии _____

(подпись)

М. П.

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1	–	Все	–	–	–	ФРКЕ.467759.003.FK.1-2025		Андреева Н. В.	25.04.2025

© АО «ИнфоТеКС», 2023