

**ВРЕМЕННЫЙ РЕГЛАМЕНТ ОРГАНИЗАЦИИ
ПОДКЛЮЧЕНИЯ К ЗАЩИЩЕННОЙ СЕТИ
ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ
МУРМАНСКОЙ ОБЛАСТИ**

ВЕРСИЯ 1.1

На 14 листах

**Мурманск
2014**

1. Понятия и определения

1. Защищенная сеть образовательных организаций Мурманской области (далее – ЗСОО) – виртуальная, наложенная на физические каналы связи защищенная транспортная сеть, построенная с использованием технологий межсетевого экранирования и VPN и использующая для криптографической защиты алгоритм ГОСТ 28147-89, реализованная сертифицированными в установленном порядке средствами защиты информации

2. Администратор ЗСОО (далее – Администратор) – юридическое лицо, осуществляющее конфигурирование и управление ЗСОО, в соответствии с законодательством Российской Федерации, эксплуатационной документацией на средства защиты информации, на основании государственного контракта (договора)

3. Координатор ЗСОО (далее – Координатор) – орган государственной власти (Министерство образования и науки Мурманской области), осуществляющий координацию действий Участников ЗСОО, а так же разработку организационно-распорядительных документов, регламентирующих работу Участников в ЗСОО.

4. Оператор ЗСОО (далее – Оператор) – организация, подведомственная Министерству образования и науки Мурманской области, осуществляющая подготовительные работы по организации предоставления доступа к ресурсам ЗСОО на основании заявок и соглашений, одобренных Координатором.

5. Участник ЗСОО (далее – Участник) – государственная областная или муниципальная образовательная организация, подключенная к ЗСОО в установленном в настоящем временном регламенте порядке.

6. Ответственный пользователь СКЗИ Участника – сотрудник Участника, контролирующее эксплуатацию средства криптографической защиты информации, входящих в состав ЗСОО и находящихся в сегменте Участника.

7. Пользователь СКЗИ Участника – сотрудник Участника, использующее для выполнения своих служебных обязанностей информационные ресурсы, входящие в состав ЗСОО и эксплуатирующий средства криптографической защиты информации.

2. Общие положения

Организация подключения новых Участников включает в себя следующие этапы:

- заявительная процедура;
- процедура рассмотрение заявки Участника;
- процедура подключения Участника.

3. Заявительная процедура

3.1. При намерении подключения к ЗСОО, новый Участник направляет Координатору пакет документов для подключения к ЗСОО.

3.2. В комплект документов, передаваемый Участником, входят:

3.2.1. Оригинал заявки на подключение к ЗСОО (Приложение №1). В заявке обязательно указывается:

- адрес, по которому будет производиться подключение к ЗСОО;
- название средства криптографической защиты информации;
- контактные данные пользователей СКЗИ (ФИО, адрес электронная почта, телефон);
- реквизиты приказа о назначении пользователей СКЗИ.

3.2.2. Копия/скан-копия приказа о назначении ответственного пользователя СКЗИ (Приложение №2).

3.2.3. Копия/скан-копия приказа о назначении пользователей СКЗИ, в случае подключения к информационным ресурсам с использованием программного обеспечения ViPNet Клиент (Приложение №3).¹

3.2.4. Информация по выделению адресного пространства сегмента Участника, в случае подключения к информационным ресурсам с использованием программно-аппаратного комплекса ViPNet Coordinator HW (Приложение №4).

3.2.5. Два экземпляра акта приемки-передачи средств криптографической защиты информации, эксплуатационной и технической документации к ним²

3.3. Электронные сканированные копии документов необходимо направить Координатору, на адрес электронной почты evpyhtina@gov-murman.ru, оригинал заявки на бумажном носителе в обязательном порядке должен быть направлен в адрес Координатора.

4. Процедура рассмотрение заявки участника

4.1. Координатор, в течение 5 (пяти) рабочих дней с момента получения заявки, принимает решение о подключении нового Участника к ЗСОО.

4.2. В случае отрицательного результата рассмотрения заявки, Координатор уведомляет Участника об отказе в подключении к ЗСОО, с обоснованием причины отказа.

¹ В случае использования СКЗИ ViPNetCoordinator выполнять данный пункт не требуется. Допускать к самостоятельной работе с СКЗИ необходимо непосредственно тех сотрудников, которые работают на рабочем месте, на котором предполагается установка СКЗИ.

² В случае, если акты приемки-передачи были переданы ранее, данный пункт пропускается.

4.3. В случае отсутствия замечаний по представленным документам, не позднее установленного в п. 4.1 срока, Координатор передает пакет документов Оператору для осуществления процедуры оценки технической возможности и согласования схемы подключения нового Участника.

4.4. Оператор в течение 5 (пяти) рабочих дней со дня получения комплекта документов, проводит совместно с Участником оценку технической возможности для организации доступа к ЗСОО.

4.5. По результатам согласования схемы и технической возможности подключения Участника, Оператор передает комплект документов Администратору для формирования ключевой информации и осуществления подключения нового Участника.

4.6. В случае отсутствия технической возможности подключения Участника к ЗСОО, Участник совместно с Координатором и Оператором, принимают меры по устранению выявленных проблем.

5. Процедура подключения участника

5.1. Администратор в согласованные с новым Участником сроки:

- производит регистрацию сетевых узлов в Центре управления сетью и организует направления связи между сетевыми узлами, в соответствии с заявкой на подключение;
- формирует дистрибутивы ключей для компонентов Участника вместе с паролем доступа к нему;
- уведомляет Участника о возможности его подключения к ЗСОО (по контактной информации, указанной в заявке).

5.2. Участник для получения дистрибутива ключей и пароля доступа к нему должен направить к Администратору ответственного пользователя СКЗИ Участника, имеющего при себе документ удостоверяющий личность и доверенность на получение дистрибутива ключей (Приложение №5).

5.3. Администратор передает ключевой дистрибутив вместе с паролем доступа к нему и технической и эксплуатационной документацией ПО ViPNet лично Ответственному пользователю СКЗИ Участника по доверенности под роспись в журнале учета ключевой информации.

5.4. Ответственному пользователю СКЗИ выдаются:

5.4.1. Эксплуатационная документация:

- правила использования СКЗИ и проводится инструктаж по работе с СКЗИ в соответствии с приказом ФАПСИ от 13.06.2001 № 152 и эксплуатационной документацией на технические средства и программное обеспечение ViPNet.

- заключение о самостоятельном допуске к работе с СКЗИ.

5.4.2. На съемный носитель информации (флэш-носитель или гибкий магнитный диск Участника) записываются:

- эксплуатационно-техническая документация (инструкции) ПО ViPNet;

- дистрибутив ключей и резервный набор персональных ключей пользователя (в виде файлов *.dst и *.pk);

- парольная информация (пароль пользователя сетевого узла ViPNet в виде файла *.psw) и делается соответствующая запись в журнале учета ключевой информации.

5.5. Доверенность на получение СКЗИ подшивается в лицевой счет Участника и хранится у Администратора в соответствии с приказом ФАПСИ от 13.06.2001 № 152

5.6. Оригинал заявки подшивается в лицевой счет Участника и хранится у Координатора.

5.7. По завершении процедур установки и настройки программного или аппаратного обеспечения ViPNet, Участник производит проверку работоспособности данного обеспечения совместно с Администратором и в случае положительного результата осуществляет ввод СКЗИ в эксплуатацию:

- ввод в эксплуатацию осуществляется актом о вводе средств криптографической защиты информации в эксплуатацию (Приложение №6)

- результаты проверки оформляются протоколом проверки (Приложение №7)

- оригиналы акта и протокола хранятся у Ответственного пользователя СКЗИ Участника, а копии/скан-копии в обязательном порядке передаются Администратору и Координатору ЗСОО

5.8. По завершении процедуры подключения к ЗСОО, Участник обязан организовать учет, хранение и эксплуатацию СКЗИ в соответствии с «Инструкцией 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», утвержденной приказом ФАПСИ от 13.06.2001 №152

ЗАЯВЛЕНИЕ на подключение к ЗСОО

Наименование учреждения _____
ИНН _____

**В случае подключения нескольких средств СКЗИ – указывать информацию обо всех*

СКЗИ № _____

Адрес подключения	Указывается фактический адрес установки СКЗИ (Город, почтовый адрес)....
Наименование СКЗИ	Указывается СКЗИ, с использованием, которого будет производиться подключение к ЗСОО (Пример: ViPNet Client 3.2; ViPNet Coordinator HW100A; ViPNet Coordinator HW100B; ViPNet Coordinator HW100C; ViPNet Coordinator HW1000)
ФИО пользователя	Заполняется только при подключении с использованием СКЗИ ViPNetClient
Структурное подразделение	
Электронная почта	
Телефон	
Реквизиты приказа	

(*Все поля заполняются максимально полно. Фамилия, имя, отчество в печатываются **ВИМЕНИТЕЛЬНОМ ПАДЕЖЕ**, все поля заполняются исключительно в печатном виде, путем редактирования на компьютере с последующим распечатыванием на принтере. Заполнение «от руки» **НЕДОПУСТИМО**.)

Ответственным пользователем СКЗИ в _____
(наименование организации)

назначен _____

(ФИО)

(приказ от _____ № _____)

Поставщик СКЗИ _____
(наименование организации-поставщика СКЗИ)

Ответственный пользователь _____ / _____ /
Подпись

Руководитель учреждения _____ / _____ /
Подпись

" ____ " _____ 201_ г
М.П.

(наименование организации)

ПРИКАЗ

№ ____

(дата)

г. Мурманск

О назначении ответственного пользователя
средств криптографической защиты информации
и лиц их замещающих

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием средств криптографической защиты информации (далее – СКЗИ) информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, **п р и к а з ы в а ю**:

1. Назначить ответственным пользователем СКЗИ и возложить функции органа криптографической защиты по организации работ с СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности СКЗИ на следующего(-их) сотрудника(-ов):

(Ф.И.О., должность, подразделение, e-mail, телефон)_____
(Ф.И.О., должность, подразделение, e-mail, телефон)

2. Ответственному(-ым) пользователю(-ям) СКЗИ провести инструктаж и обучение пользователя(-ей) СКЗИ и ознакомить под роспись с правилами эксплуатации СКЗИ.

3. Ответственный пользователь обязан:

- контролировать соблюдения пользователями конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых компонентов ЗСОО и ключевых документах к ним;

- проводить ознакомление пользователей с правилами работы и требованиями безопасности ЗСОО;

- осуществлять хранение эксплуатационной и технической документации, ключевых документов, носителей информации ограниченного распространения относящихся к компонентам ЗСОО, в соответствии с требованиями законодательства;

- соблюдать правила эксплуатации СКЗИ;
- принимать меры по препятствованию несанкционированного доступа к компонентам ЗСОО со стороны пользователей и иных посторонних лиц;
- немедленно принимать меры по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

4. Назначенные в соответствии с п. 1 настоящего приказа сотрудник(-и) несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе обмена информацией;
- сохранение в тайне закрытых ключей шифрования и иной ключевой информации;
- соблюдение правил эксплуатации программно-аппаратных средств ViPNet.

5. Контроль за исполнением настоящего приказа оставляю за

_____.

Руководитель учреждения

Подпись

(наименование организации)

ПРИКАЗ

№ ____

(дата)

г. Мурманск

О назначении пользователей
средств криптографической защиты информации

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений составляющих государственную тайну, с использованием информационных систем ЗСОО **п р и к а з ы в а ю :**

1. Допустить к самостоятельной работе с СКЗИ следующих работников:

№	ФИО пользователя	Структурное подразделение	Должность

2. В своей работе пользователям СКЗИ руководствоваться нормативно-правовыми актами РФ в сфере защиты информации.

3. Контроль за исполнением настоящего приказа оставляю за _____.

Руководитель учреждения

Подпись

Требования по выделению адресного пространства участника при подключении программно-аппаратного комплекса к ЗСОО

Для подключения программно-аппаратного комплекса ViPNet на территории Участника должен:

1. Обеспечить подключение к сети Интернет (любые провайдеры, доступные в регионе).

2. При подключении через сеть Интернет обеспечение доступности внешнего интерфейса криптошлюза (IP внеш.) из сети Интернет одним из следующих способов:

2.1. Обеспечение NAT-трансляции частного IP-адреса в публичный IP-адрес (трафик по протоколу UDP, порт 55777).

2.2. Выделение для интерфейса публичного IP-адреса.

3. Обеспечить маршрутизацию в локальной сети Участника таким образом, чтобы трафик с адресов серверов или автоматизированных рабочих мест Участника, отправляемый на серверы ЗСОО, направлялся на внутренний интерфейс криптомаршрутизатора.

4. Для организации подключения ПАК ViPNet в необходимо обеспечить выделение в следующих IP адресов:

п/п	IP адрес/маска	Назначение
1	IP внеш./маска	IP-адрес и маска сети внешнего интерфейса ПАК ViPNet. Может быть как из частного, так и из публичного адресного пространства.
2	IPgw внеш.	Адрес шлюза по умолчанию в сети, в которую включается внешний интерфейс ПАК ViPNet .
3	IPfw (NAT)	Публичный Интернет адрес NAT-трансляции, через который осуществляется доступ к внешнему интерфейсу ПАК ViPNet . Указывается в случае использования частного адреса на внешнем интерфейсе ПАК ViPNet при подключении через сеть Интернет. При подключении ПАК ViPNet в сеть Интернет напрямую IP fw совпадает с IP внеш./маска.
4	IPвнут./маска	Адрес и маска сети внутреннего(-их) интерфейса(-ов) ПАК ViPNet. IP внеш. и IP внут. обязательно должны принадлежать разным подсетям.
5	IPgwвнут.	Адрес шлюза для доступа к внутренним ресурсам организации. Указывается в случае нахождения ресурсов организации и внутреннего интерфейса ПАК ViPNet в разных сетях.
6	IPтунн.	Адрес сервера или АРМ (диапазон адресов), которые будут взаимодействовать с серверами ЗСОО.

**Доверенность № _____
на получение средств криптографической защиты информации
и электронно-цифровой подписи**

Дата выдачи: _____
(дата прописью)

(наименование организации)

в лице _____
(должность и ФИО руководителя - полностью)

действующего на основании _____

настоящей доверенностью уполномочивает _____

(должность и ФИО – полностью)
(паспорт серии _____ № _____, выдан “ ____ ” _____

_____ года _____) представлять интересы
(кем выдан)

_____ и получить
(наименование организации)

средства криптографической защиты информации (СКЗИ), а так же дистрибутивы ключей для первичного запуска прикладной программы сети ViPNet и выполнить все необходимые действия, связанные с исполнением настоящего поручения.

Ответственным пользователем в _____
(наименование организации)

за эксплуатацию СКЗИ назначен _____
(Ф.И.О., занимаемая должность)

Доверенность действительна до “ ____ ” _____ 20__ года и дана без права передоверия.

Подпись лица, получившего доверенность _____.
(подпись)

Руководитель _____ (_____)
(подпись) (инициалы и фамилия)

М.П.

“ ____ ” _____ 20__ г.

**Акт
о вводе СКЗИ в эксплуатацию**

« ___ » _____ 20__ г.

Комиссия в составе: председателя комиссии _____
_____, членов комиссии _____
_____ и

Ответственного пользователя СКЗИ _____
составила акт о том, что (наименование СКЗИ) установлен в
_____ по
адресу _____

в помещении № _____, в соответствии с технической и эксплуатационной документацией
и введен в эксплуатацию.

Состав (наименование СКЗИ):

Системный блок № _____

Программный комплекс:

(наименование СКЗИ) версия _____ сборка _____

Версия операционной системы: _____

Дополнительно установленное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного
администрирования и т. д.):

Дополнительно установленное оборудование (наименование, назначение, серийный номер
и т. д.) _____

Председатель комиссии:

Должность	Ф.И.О.	Подпись
-----------	--------	---------

Члены комиссии:

Должность	Ф.И.О.	Подпись
-----------	--------	---------

Должность	Ф.И.О.	Подпись
-----------	--------	---------

Протокол контрольной проверки СКЗИ

«___» _____ 20__ г.

(наименование СКЗИ) установлен в _____

по адресу _____

в помещении №_____, в соответствии с технической и эксплуатационной документацией.

Состав (наименование СКЗИ):

Системный блок № _____

Программный комплекс:

(наименование СКЗИ) версия: _____

Версия операционной системы: _____

Дополнительно установленное оборудование (наименование, назначение, серийный номер и т.д.) _____

Дополнительно установленное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного администрирования и т. д.): _____

Состав и результаты проверок и контрольных тестов

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
1.	Загрузка ОС с отказом от ввода пароля ViPNet	Отказ в загрузке ОС		
2.	Загрузка ОС с аутентификацией пользователя ³	Загрузка ОС и старт ПО ViPNet		
3.	Проверка установленных режимов безопасности ⁴	Режимы безопасности соответствуют назначению СУ		
4.	Проверка настроек ПО	Настройки ПО соответствуют требованиям ⁵		
5.	Аутентификация с паролем администратора СУ	Переход ПО в режим работы администратора СУ		
6.	Контроль журнала событий ПО ViPNet Координатор [Монитор]	Отсутствие попыток несанкционированного изменения режимов, настроек фильтров, аварийных завершений ПО		
7.	Контроль журнала регистрации IP-	Отсутствие признаков		

³ Указать тип аутентификации

⁴ Для координаторов на каждом из сетевых интерфейсов

⁵ Пункт 5.3.1, Регламент информационной безопасности при использовании программно-аппаратных средств комплекса ViPNet (ФРКЕ. 00029-04 90 01)

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
	пакетов	сетевых атак, отсутствие информации о пропуске пакетов на запрещенные режимом (фильтрами) адреса (протоколы)		
8.	Проверка связи с видимыми СУ защищенной сети	Наличие сообщений о доступности СУ		
9.	Проверка связи с видимым СУ защищенной сети, для которого включен фильтр блокировки пакетов	Наличие сообщений о недоступности СУ, информация в журнале о блокировании пакетов		
10.	Проверка связи (ping _____) с открытым не зарегистрированным адресом (во 2 режиме)	Отсутствие ответа от узла. Информация в журнале о блокировке пакетов для данного адреса		
11.	Настройка фильтра, блокирующего отдельный протокол (например, ICMP) для отдельного СУ защищенной сети, проверка соединения с СУ по данному протоколу	Отсутствие ответа от СУ, информация о блокировании пакетов по выбранному протоколу		
12.	Настройка фильтра, запрещающего отдельный протокол (например, UDP) для всех СУ защищенной сети, проверка связи с СУ по данному протоколу (например, проверка соединения)	Наличие сообщений о недоступности СУ. Информация в журнале о блокировании пакетов		
13.	Настройка фильтра, разрешающего отдельный протокол (например, ICMP) для всех узлов открытой сети, проверка связи с любым открытым узлом по данному протоколу (например, ping)	Наличие ответа от узла. Информация в журнале о пропуске пакетов для данного адреса		
14.	Проверка связи по разрешенному протоколу для зарегистрированных открытых адресов ⁶	Наличие соединения по данному протоколу		
15.	Проверка связи по запрещенному протоколу для зарегистрированных открытых адресов	Отсутствие соединения по данному протоколу		
16.	Отправка зашифрованного и подписанного письма адресатам ДП ⁷	Отправка письма, получение квитанций о доставке (прочтении)		
17.	Контроль журналов автопроцессинга ДП ⁸	Отсутствие сбоев в работе правил		

ОТВЕТСТВЕННЫЙ ПОЛЬЗОВАТЕЛЬ
СКЗИ

ФИО _____

Дата: «__» _____ 20__ г.

Подпись: _____

М.П.

⁶ Только для 2 режима безопасности

⁷ При наличии установленного ПО ViPNet Клиент [Деловая Почта]

⁸ При наличии данного функционала на СУ