18.12.2018 П9-1-04-200-29542

УТВЕРЖДАЮ:
Директор Департамента
проектов по информатизации
Минкомсвязи России

О.Ю. Качанов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00C4750D5B11E4DA80E811D87D2044760C
Владелец: Качанов Олег Юрьевич
Действителен с 02.07.2018 до 02.07.2019

Регламент

по организации межсетевого взаимодействия между Сторонней ViPNet-сетью и Защищённой ViPNet-сетью ФГИС «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации»

Москва 2018

1. СПИСОК СОКРАЩЕНИЙ И ТЕРМИНОВ

VPN	Виртуальная частная сеть. Обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет)
VipNet	Защищённая VPN сеть.
АРМ	Автоматизированное рабочее место
Администратор	сотрудник, отвечающий за работу компьютерной сети предприятия в штатном режиме
Единая система	Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации
ЕИСУКС	Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации
ИСММК	Индивидуальный симметричный межсетевой мастер-ключ

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Регламент определяет порядок организации межсетевого взаимодействия между VipNet-сетями (№ 1274 (КС2) и № 4318 (КС3)) Федеральной государственной информационной системы «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации» (далее – Защищённая сеть) и сторонними VipNet-сетями (далее – Сторонняя сеть) через соответствующие VipNet-координаторы.

2.2. Регламент об организации межсетевого взаимодействия Защищённой сети разработан в соответствии с:

- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.3. Регламент определяет и устанавливает:

- порядок организации межсетевого взаимодействия Сторонней сети с Защищённой сетью;
- порядок работы а случае смены Администратора Сторонней сети;
- порядок работы в случае плановой смены межсетевого мастер-ключа;
- порядок работы в случае компрометации ключей;
- порядок разрешения конфликтных ситуаций.

3. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ СО СТОРОННИМИ СЕТЯМИ

3.1. Организация подключения Сторонних сетей к Защищённой сети включает в себя следующие стадии:

- подача заявки;
- рассмотрение заявки;
- настройка межсетевого взаимодействия.

3.2. Подача заявки.

3.2.1. Для организации межсетевого взаимодействия между Защищённой сетью и Сторонней сетью, Администратор Сторонней сети формирует заявку в виде информационного письма, в котором указывает:

– контакты лиц, ответственных за организацию межсетевого взаимодействия (ФИО, должность, контактный телефон, электронная почта);

- часы работы ответственных лиц за организацию межсетевого взаимодействия относительно московского времени;
- номер подключаемой сторонней VipNet-сети;
- класс используемого для организации межсетевого взаимодействия СКЗИ VipNet (КС2, КС3);
- используемая версия программного комплекса VipNet Administrator сторонней VipNet-сети;
- используемая версия прошивки программно-аппаратного комплекса VipNet Coordinator HW (или версия программного комплекса ViPNet Coordinator Software) сторонней VipNet-сети;
- акт соответствия требованиям безопасности информации, предъявляемым к сегменту сторонней ViPNet-сети и к автоматизированным рабочим станциям, подключаемым к ЕИСУКС (Приложение №1);
- копия аттестата соответствия требованиям безопасности информации, предъявляемым к государственным информационным системам класса защищенности К3, выданный на сегмент сторонней VipNet-сети, включающий в себя автоматизированное рабочее место Администратора и программно-аппаратный комплекс VipNet Coordinator сторонней VipNet-сети, посредством которого строится межсетевое взаимодействие;
- наименование АРМ пользователя подключённого к Сторонней сети, ФИО пользователя, на которого оформлен Абонентский пункт, с указанием версии используемого программного обеспечения (в случае установленного ПО «VipNet Client»), статический ip-адрес АРМ (в случае не установленного ПО «VipNet Client»), должность, контактный телефон, адрес служебной электронной почты, роль пользователя в Единой

системе (уполномоченный сотрудник, уполномоченное должностное лицо);

- копия приказа (распоряжения) о закреплении АРМ за сотрудником подразделения;
- наименование Координатора, на котором зарегистрирован подключаемый Абонентский пункт, с указанием версии используемого программного обеспечения;
- наименование АРМ Администратора Сторонней сети с указанием версии используемого программного обеспечения.

3.2.2. Информационное письмо о межсетевом взаимодействии, составленное в соответствии с подпунктом 3.2.1 настоящего документа, отправляется в Минкомсвязь России в бумажном виде, электронная копия информационного письма высылается на электронную почту rezerv@minsvyaz.ru (официальный электронный адрес «горячей линии» Единой системы).

3.3. Рассмотрение заявки.

3.3.1. Техническая поддержка Единой системы (уполномоченная Минкомсвязью России организация) в течение 5-ти рабочих дней со дня получения информационного письма по электронной почте от Минкомсвязи России проводит предварительный анализ заявки, включая оценку технической возможности для организации межсетевого взаимодействия. В случае принятия решения о технической возможности организации межсетевого взаимодействия Техническая поддержка Единой системы уведомляет по электронной почте Минкомсвязь России и орган государственной власти, инициирующий заявку, о принятии такого решения, назначает дату передачи ИСММК на АРМ Администратора сторонней VipNet-сети для установления межсетевого взаимодействия.

3.3.2. Техническая поддержка Единой системы имеет право отказать в организации межсетевого взаимодействия. Причины для отказа могут быть следующими:

- сведения, запрашиваемые в соответствии с п. 3.2.1, предоставлены не в полном объеме, с указанием недостающих сведений;
- класс используемого для организации межсетевого взаимодействия СКЗИ Сторонней сети отличный от класса КС2 или КС3;
- акт соответствия требованиям безопасности информации, предъявляемым к сегменту сторонней ViPNet-сети и к автоматизированным рабочим станциям, подключаемым к ЕИСУКС не предоставлен;
- копия аттестата соответствия требованиям безопасности информации на сегмент сторонней ViPNet-сети не предоставлен и (или) не соответствует предъявленным требованиям безопасности информации к государственным информационным системам класса защищенности К3;
- отсутствует закрепление АРМ за сотрудником соответствующего подразделения.

3.4. В соответствии с «Инструкцией для подключения пользователей объединенных сетей» формирование и передачу ИСММК осуществляют Администратор безопасности Единой системы и Администратор Сторонней сети:

- Администратор безопасности Единой системы осуществляет формирование ИСММК для Сторонней сети;

- Администратору Сторонней сети по защищенному каналу передаются экспортные файлы, в состав которых входят экспортные справочники, ИСММК, пароль на ИСММК, а также форма подтверждения, любым способом, исключающим несанкционированный доступ (далее – НСД) к пересылаемой информации;

- после получения экспортных файлов Администратор Сторонней сети осуществляет настройку межсетевого канала, настройку типов коллектива;

- после получения ответного экспорта от Администратора Сторонней -сети по защищенному каналу, Администратор безопасности Единой системы осуществляет установку ответного экспорта из Сторонней сети.

После выполнения всех действий, указанных в подпункте 3.4 Администратор безопасности Единой системы и Администратор Сторонней сети осуществляют проверку межсетевого взаимодействия.

По итогам организованного межсетевого взаимодействия обе стороны подписывают Протокол установления межсетевого взаимодействия (Приложение №2) в 2-х экземплярах и обмениваются подписанными экземплярами документа по фельдъегерской почте (в том числе в электронном виде, подписав электронные копии документа квалифицированной электронной подписью).

4. ПОРЯДОК РАБОТЫ В СЛУЧАЕ СМЕНЫ АДМИНИСТРАТОРА СТОРОННЕЙ СЕТИ

4.1. В случае смены Администратора Сторонней сети (его контактных данных), ответственные за организацию межсетевого взаимодействия лица Сторонней сети обязаны в течение 1-го рабочего дня выслать контактную информацию на адрес rezerv@minsvyaz.ru (официальный электронный адрес «горячей линии» Единой системы).

5. ПОРЯДОК РАБОТЫ В СЛУЧАЕ ПЛАНОВОЙ СМЕНЫ МЕЖСЕТЕВОГО МАСТЕР-КЛЮЧА.

5.1. Порядок работы в случае плановой смены ИСММК предполагает выполнение ряда технологических и организационных мероприятий, включающих следующие стадии:

- предварительные организационные мероприятия;
- формирование нового ИСММК;
- процедура создания экспорта и приёма импорта;
- обновление ключевой информации.

5.2. Предварительные организационные мероприятия

Перед тем как осуществить плановую смену ИСММК, Администратор безопасности Единой системы и Администратор Сторонней сети, с которой установлено межсетевое взаимодействие должны выбрать и согласовать время проведения смены ИСММК и последующего обновления ключей шифрования для Абонентских пунктов сетей.

5.3. Формирование нового ИСММК

Формирование нового ИСММК производится в соответствии с «Инструкцией для подключения пользователей объединенных сетей».

5.4. Процедура создания экспорта и приёма импорта

После смены ИСММК производится процедура создания экспортных данных и приём импортированных данных в соответствии с «Инструкцией для подключения пользователей объединенных сетей».

5.5. Обновление ключевой информации

После смены ИСММК, связь между взаимодействующими Абонентскими пунктами сети Единой системы и Сторонней сети, с которой установлено межсетевое взаимодействие, возможна только после прохождения обновления ключевой информации на всех соответствующих Абонентских пунктах. Обновленная ключевая информация через Центр управления сетью Единой системы отправляется на Абонентские пункты, участвующие в межсетевом взаимодействии.

6. ПОРЯДОК РАБОТЫ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

6.1. К событиям компрометации ключей относятся следующие случаи:

- посторонним лицам стал доступен съёмный носитель с ИСММК;
- посторонние лица получили несанкционированный доступ к ИСММК;

- посторонним лицам мог стать доступен пароль ИСММК, и эти лица могли иметь доступ к рабочему месту, на котором хранится ИСММК.

6.2. Компрометация ИСММК.

При наступлении любого из перечисленных в п. 6.1 настоящего Регламента событий Администратор Сторонней сети обязан сообщить о факте компрометации Администратору безопасности Единой системы.

6.3. Администратор безопасности Единой системы при получении сообщения о компрометации ИСММК в течение 1-го рабочего дня должен:

- удалить межсетевое взаимодействие со Сторонней сетью;
- в соответствии с «Инструкцией для подключения пользователей объединенных сетей» создать новый мастер ключ, задать новый пароль и отправить любым способом, исключающим несанкционированный доступ (далее – НСД) к пересылаемой информации, Администратору Сторонней сети.

6.4. Возобновление межсетевого взаимодействия возможно только после прохождения обновления ключевой информации на всех взаимодействующих Абонентских пунктах.

7. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

7.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения или компрометацией электронных документов и/или получение доступа к Единой системе пользователями сторонних сетей, не входящих в межсетевое взаимодействие.

7.2. Разрешение конфликтных ситуаций осуществляется путём взаимодействия Администраторов участников межсетевого взаимодействия, у которых возникли претензии.

7.3. В случае выявления нарушений законодательства в части защиты персональных данных, разрешение конфликта производится в юридическом порядке.

Приложение №1

Типовая форма Акта соответствия требованиям безопасности информации, предъявляемым к сегменту сторонней ViPNet-сети и к автоматизированным рабочим станциям, подключаемым к ФГИС «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации»

г. Москва «___» _____ 20__ г.

Проверки системы защиты информации автоматизированного рабочего места _____ проводились в рамках выполнения работ по подключению к ФГИС «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации» (далее – ЕИСУ КС) посредством организации межсетевого взаимодействия между защищенной ViPNet-сетью № 1274 (4318), владельцем которой является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, и ViPNet-сетью № ____, владельцем которой является _____.

1. Объект проверки

Система защиты информации (далее – СЗИ) автоматизированного рабочего места (далее – АРМ) _____.

Номер АРМ сети №_____	**IP-адрес АРМ**	**ФИО пользователя сети №_____ _____**
№ _____		_____

2. Место проведения проверки

Испытания СЗИ АРМ проводились в _____ по адресу: _____.

3. Цели проверки

Проверка проводится для достижения следующих целей:

– подтверждение соответствия сегмента сети _____, в котором размещается программно-аппаратный комплекс ViPNet Coordinator и автоматизированное рабочее место администратора ViPNet-сети № _____, требованиям по безопасности информации, предъявляемым к государственным информационным системам класса **К3**;

– проверка наличия действующих сертификатов соответствия на средства защиты информации, установленные на АРМ и подтверждение соответствия СЗИ требованиям, предъявляемым к АРМ, подключаемым к ЕИСУ КС;

– проверка реализации в СЗИ функций по защите информации;

– проверка соответствия содержания эксплуатационной документации фактической реализации функций.

4. Проверка наличия действующих сертификатов соответствия на средства защиты информации

Проведена проверка используемых средств защиты информации и действующих сертификатов на них по следующему перечню.

Проведена проверка наличия следующих средств защиты информации.

Наименование средства защиты информации	**Количество**	**Место установки**	**Номер сертификата соответствия, срок действия**	**Подтверждение соответствия требованиям, предъявляемым к АРМ, подключаемым к ЕИСУ КС**
Модуль защиты от НСД и контроля устройств Средства защиты информации Secret Net Studio 8	1	АРМ № _____		Является средством защиты от несанкционированного доступа, прошедшим проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей и соответствует требованиям руководящих документов по 5 классу

Наименование средства защиты информации	**Количество**	**Место установки**	**Номер сертификата соответствия, срок действия**	**Подтверждение соответствия требованиям, предъявляемым к АРМ, подключаемым к ЕИСУ КС**
				защищенности средств вычислительной техники
Антивирусное средство защиты	1	АРМ № _____		Является средством антивирусной защиты информации 5 класса
ViPNet Administrator 4	1	АРМ № _____		
Программный комплекс ViPNet Client 4	1	АРМ № _____		
Программно-аппаратный комплекс ViPNet Coordinator 4	1			

5. Подтверждение соответствия сегмента сети _____ требованиям по безопасности информации

Наименование сегмента	Наименование объекта	Место установки	Аттестат соответствия требованиям по безопасности	Результат
Сегмент сети _____, в котором размещается программно-аппаратный комплекс ViPNet Coordinator и автоматизированное рабочее место администратора ViPNet-сети № _____	ПАК ViPNet Coordinator		Номер: _____ Кем выдан: _____ Срок действия: _____ Класс защищенности информационной системы: _____	Соответствует требованиям по безопасности информации
	АРМ Администратора ViPNet Coordinator			

6. Проверка реализации в СЗИ АРМ функций по защите информации

6.1. Идентификация и аутентификация субъектов доступа и объектов доступа

Объект проверки	Результат
Проверка реализации управления идентификацией и аутентификацией субъектов доступа и объектов доступа включает в себя: - проверку реализации механизмов идентификации и аутентификации пользователей, являющихся работниками оператора; - проверку реализации механизмов управления идентификаторами, в том числе, создания, присвоения, уничтожения идентификаторов; - проверку реализации механизмов управления средствами аутентификации, в том числе, хранения, выдачи, инициализации, блокирования средств аутентификации и принятия мер в случае утраты или компрометации средств аутентификации; - проверку реализации защиты обратной связи при вводе аутентификационной информации.	Соответствует Используются механизмы средств защиты информации: - Средство защиты информации «Secret Net Studio 8».

6.2. Управление доступом субъектов доступа к объектам доступа

Объект проверки	Результат
Проверка реализации мер по управлению доступом субъектов доступа к объектам доступа включают в себя: - проверку управления (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей; - проверку реализации необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; - проверку управления (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные	Соответствует Используются механизмы средств защиты информации: - Средство защиты информации «Secret Net Studio 8»; - Программный комплекс ViPNet Client 4; - Программно-аппаратный комплекс ViPNet Coordinator 4

Объект проверки	Результат
способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами; - проверку разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; - проверку назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; - проверку ограничения неуспешных попыток входа в информационную систему (доступа к информационной системе); - проверку реализации защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети; - проверку обеспечения управления взаимодействием с информационными системами сторонних организаций (внешние информационные системы).	

6.3. Ограничение программной среды

Объект проверки	Результат
Проверка реализации мер по ограничению программной среды включает в себя: - Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Соответствует - Принят ряд организационных мер по ограничению программной среды. *Подтвердить приказом.*

6.4. Защита машинных носителей информации

Объект проверки	Результат
Проверка реализации мер по защите машинных носителей информации включает в себя: - учет машинных носителей информации; - управление доступом к машинным	Соответствует - Принят ряд организационных мер по защите машинных носителей. *Подтвердить приказом.*

Объект проверки	Результат
носителям информации; - уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	

6.5. Регистрация событий безопасности

Объект проверки	Результат
Проверка реализации мер по регистрации событий безопасности включают в себя: - проверку определения событий безопасности, подлежащих регистрации, и сроков их хранения; - проверку определения состава и содержания информации о событиях безопасности, подлежащих регистрации; - проверку сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения; - проверку защиты информации о событиях безопасности.	Соответствует Используются механизмы средств защиты информации: - Средство защиты информации «Secret Net Studio 8».

6.6. Антивирусная защита

Объект проверки	Результат
Проверка реализации мер по антивирусной защите включает в себя: - проверку реализации антивирусной защиты; - проверку обновления баз данных признаков вредоносных компьютерных программ (вирусов).	Соответствует Используется антивирусный пакет «Kaspersky Endpoint Security 10 для Windows»
Наличие сертифицированного комплекта на средства антивирусной защиты	Соответствует

6.7. Контроль (анализ) защищенности информации

Объект проверки	Результат
Проверка реализации мер по контролю (анализу) защищенности информации включают в себя проверку обеспечения: - выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; - контроля установки обновлений	Соответствует Принят ряд организационных мер по проведению работ по контролю (анализу) защищенности информации. *Подтвердить приказом и регламентом.*

программного обеспечения, включая обновление программного обеспечения средств защиты информации; - контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации; - контроль состава технических средств, программного обеспечения и средств защиты информации; - контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	

6.8. Защита технических средств

Объект проверки	Результат
Проверка реализации мер по защите технических средств включает в себя: − проверку реализации организации контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования; − проверку функционирования системы контроля и управления физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены; − проверку обеспечения размещения устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.	Соответствует Принят ряд организационных мер по защите технических средств. *Подтвердить приказом*

6.9. Защита информационной системы, ее средств, систем связи и передачи данных

Объект проверки	Результат
Проверка реализации мер по защите информационной системы, ее средств, систем связи и передачи данных включает в себя проверку реализации обеспечения защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны	Соответствует Используются ПАК ViPNet Coordinator HW1000 D 4.x
Класс средств криптографической защиты информации	КС3

7. Заключение по результатам проверки

Система защиты информации АРМ _____ соответствует требованиям безопасности информации, предъявляемым к АРМ, подключаемым к ЕИСУ КС, а также сегмент сети _____, в котором размещается программно-аппаратный комплекс ViPNet Coordinator, используемый для организации межсетевого взаимодействия и автоматизированное рабочее место администратора ViPNet-сети № _____, требованиям по безопасности информации, предъявляемым к государственным информационным системам класса **К3**.

Проверка показала работоспособность СЗИ АРМ №_____ _____ и готовность к организации межсетевого взаимодействия и подключения его к ЕИСУ КС.

Приложение № 2

ПРОТОКОЛ
установления межсетевого взаимодействия
« » _____ 20__ г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Класс СКЗИ	Владелец сети	Пользователь сети
№ _____		_____ полное наименование организации, ОГРН	_____ полное наименование организации, ОГРН
№ _____		_____ полное наименование организации, ОГРН	_____ полное наименование организации, ОГРН

2. Подключаемые автоматизированные рабочие места сторонней сети:

Номер АРМ сети (доменное имя подключаемого АРМ) №_____	ФИО пользователя сторонней сети
№ _____	_____

3. Целью установления межсетевого взаимодействия является организация доступа перечисленных в пункте 2 пользователей VipNet-сети №_____ к защищенной части Единой системы.
4. Процедуру установления межсетевого взаимодействия осуществляли (ответственные сотрудники):

Номер сети	Должность	ФИО	Контактные данные (e-mail, номер телефона)
№_____			
№_____			

5. Передача начального и ответного экспорта между сетями № ____ и № ____ осуществлялась через специалиста, уполномоченного Сторонами на данные действия.
6. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети Минкомсвязи России № _____.
7. Для установления межсетевого взаимодействия были назначены серверы-маршрутизаторы для организации шлюза:
   - в сети _____№ _____ - "_____",
   - в сети _____№ _____ - "_____".
8. Смена межсетевых ключей, изменение состава Абонентского пункта, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с указанием производимых изменений.
9. Стороны обязуются без предварительного согласования не производить изменений в настройках и структуре защищенных сетей, способных привести к нарушению межсетевого взаимодействия.

От _____	От _____
(Пользователь сети № _____)	(Пользователь сети № _____)
_____ (должность, подпись, инициалы, фамилия)	_____ (должность, подпись, инициалы, фамилия)
«___» _____ 20 __ г.	«___» _____ 20 __ г.
От _____	От _____
(Владелец сети № _____)	(Владелец сети № _____)
_____ (должность, подпись, инициалы, фамилия)	_____ (должность, подпись, инициалы, фамилия)
«___» _____ 20 __ г.	«___» _____ 20 __ г.