Государственное бюджетное учреждение дополнительного
профессионального образования Воронежской области
«Институт развития образования имени Н. Ф. Бунакова»

СОГЛАСОВАНО

Директор Центра цифровой
трансформации образования
ГБУ ДПО ВО «ВИРО им. Н.Ф.
Бунакова»

_____Д. Г. Плотников

м.п.

«22» 11 2020 г.

УТВЕРЖДАЮ

Ректор
ГБУ ДПО
«ВИРО им. Н. Ф. Бунакова»

_____А. Ю. Митрофанов

м.п.

«22» 11 2020 г.

ПОРЯДОК

подключения автоматизированных рабочих мест
внешних пользователей к
Государственной информационной системе
«Образование Воронежской области»

Воронеж, 2020

Содержание

1 Общие положения 3
2 Требования по защите информации 4
3 Рекомендации по исполнению требований 6
3.1 Установка и настройка средств защиты информации 6
3.1.1 SecretNet Studio 6
3.1.2 Континент TLS клиент 7
3.1.3 ScanOVAL 9
3.2 Реализация организационных мер 10
3.2.1 Назначение лица, ответственного за защиту информации 10
3.2.2 Определение перечня лиц, имеющих право доступа к АРМ 10
3.2.3 Контроль доступа в помещения, в которых расположены АРМ 11
3.2.4 Обеспечение безопасности машинных носителей информации 11
3.3 Контроль за реализацией мер 12
3.4 Рекомендации по повышению квалификации сотрудников 12
Приложение 1 Должностная инструкция лица, ответственного за защиту информации 13
Приложение 2 Перечень лиц, доступ которых к информации ограниченного доступа (в том числе персональным данным), обрабатываемой в АРМ, необходим им для выполнения ими служебных (трудовых) обязанностей ... 16
Приложение 3 Журнал ознакомления работников 17
Приложение 4 Перечень помещений, в которых расположены АРМ и/или хранятся машинные носители информации ограниченного доступа, а также лиц, имеющих право доступа в них 20
Приложение 5 Журнал открытия/закрытия помещений 21
Приложение 6 Журнал учета машинных носителей информации 23
Приложение 7 Перечень мест хранения съемных машинных носителей информации ограниченного доступа (в том числе персональных данных) ... 25
Приложение 8 Заключение по результатам оценки соответствия 26

1 Общие положения

1.1 Данный документ разработан во исполнение требований пунктов:

– УПД.16 «Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)»;

– ЗИС.3 «Обеспечение 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»

приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2 Данный документ содержит требования по защите информации, предъявляемые к автоматизированным рабочим местам, подключаемым к государственной информационной системе «Образование Воронежской области» (далее – АРМ, ГИС «Образование ВО»), а также методические рекомендации по их исполнению.

1.3 Выполнение положений данного документа является обязательным для всех организаций, планирующих подключение АРМ к ГИС «Образование ВО».

2 Требования по защите информации

2.1 Подключение АРМ к ГИС «Образование ВО» может осуществляться с использованием следующих каналов связи:

– закрытой сети связи RSNet 2517;

– информационно-телекоммуникационной сети «Интернет».

В случае использования закрытой сети связи RSNet 2517 требования по защите информации предъявляются провайдером данной сети связи.

В случае использования информационной-телекоммуникационной сети «Интернет», должны быть выполнены требования по защите информации, указанные ниже.

2.2 АРМ, подключаемые к ГИС «Образование ВО» должны отвечать минимальным системным требованиям, указанным в таблице ниже.

Таблица 1 – Минимальные системные требования

№ п/п	Показатель	Значение
1	Операционная система	Windows 10 (версии 1903 – 2009) Windows 8.1 Rollup Update KB2919355 Windows 7 SP1 Windows Server 2019 Windows Server 2016 Windows Server 2012/Server 2012 R2 Rollup Update KB2919355 Windows Server 2008 R2 SP1
2	Оперативная память	Минимально – 2 Гб Рекомендуется – 4 Гб
3	Свободное дисковое пространство	4 Гб
4	Дополнительные требования	Подключение к Интернет

2.3 На каждом из АРМ, подключаемых к ГИС «Образование ВО», должны быть установлены средства защиты информации, указанные в таблице ниже.

Таблица 2 – Средства защиты информации

№ п/п	Средство	Порядок получения
1	Система защиты информации от несанкционированного доступа SecretNet Studio с модулями межсетевого экранирования, обнаружения вторжений и антивирусной защиты	У официальных дистрибьюторов ООО «Код Безопасности» по каталожному артикулу «SNS-8.x-BL3-NS-BK4-SB-VIRO-SP1Y»
2	Средство криптографической защиты информации Континент TLS клиент	Бесплатно предоставляется ГБУ ДПО «ВИРО им. Н. Ф. Бунакова» при поступлении заявки на подключение

№ п/п	Средство	Порядок получения
3	Средство анализа уязвимостей ScanOVAL	Бесплатно доступно для загрузки по адресу: https://bdu.fstec.ru/site/scanoval

2.4 В отношении АРМ должны быть реализованы следующие организационные меры защиты информации, перечень которых представлен в таблице ниже.

Таблица 3 – Организационные меры защиты информации

№ п/п	Меры защиты информации
1	Назначение лица, ответственного за защиту информации
2	Определение перечня лиц, имеющих право доступа к АРМ
3	Контроль доступа в помещения, в которых расположены АРМ
4	Обеспечение безопасности машинных носителей информации

3 Рекомендации по исполнению требований

3.1 Установка и настройка средств защиты информации

В данном разделе представлен порядок установки и настройки средств защиты информации, указанных в п. 2.3 требований.

3.1.1 SecretNet Studio

3.1.1.1 Установка

Пользователь, устанавливающий ПО Secret Net Studio, должен обладать правами администратора компьютера.

Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.10) и запустите установку с помощью команды "Защитные компоненты". Примечание. Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните следующее действие:

– при установке на компьютер с 64-разрядной версией Windows запустите с установочного диска файл \Setup\Client\x64\SnSetup.ru-RU.exe;

– при установке на компьютер с 32-разрядной версией Windows запустите с установочного диска файл \Setup\Client\Win32\SnSetup.ru-RU.exe.

На экране появится диалог принятия лицензионного соглашения.

Ознакомьтесь с содержанием лицензионного соглашения и нажмите кнопку «Принимаю». На экране появится диалог для выбора режима работы компонента.

В поле «Режим работы» укажите нужный режим функционирования клиента — автономный («Автономный режим»).

Нажмите кнопку «Далее». На экране появится диалог для выбора лицензий и формирования списка устанавливаемых защитных подсистем.

Нажмите кнопку «Загрузить» и выберите из раскрывающегося списка метод получения лицензий: укажите «Из файла», а затем выберите нужный файл в появившемся диалоге. После загрузки данных в диалоге появятся сведения о лицензиях.

Отметьте в списке устанавливаемые подсистемы:

– Базовая защита;

– Контроль устройств;

– Персональный межсетевой экран;

– Обнаружение и предотвращение вторжений;

– Антивирус.

По окончании настройки параметров нажмите кнопку "Готово". Начнется процесс установки защитных подсистем в соответствии с заданными параметрами.

3.1.1.2 Настройка

Перейдите во вкладку настройки Центра управления Secret Net Studio. В разделе вход в систему необходимо указать следующие параметры:

– Максимальный период неактивности до входа в систему – 10 минут;

– Количество неудачных попыток аутентификации – 3 попытки;

– Парольная политика – Установить флаг «Свои значения»;

– Минимальная длинна пароля – 8 символов;

– Срок действия пароля - 30 дней.

В разделе Персональный межсетевой экран переведите флаг в положение «включить».

В разделе Антивирус переведите флаг в положение «включить».

Установите следующие флаги:

– Оптимальная защита;

– Сканировать подключаемые носители.

В разделе Обнаружение вторжений переведите флаг в положение «включить».

Установите следующие флаги:

– Включить детекторы атак;

– Блокировка атакующего хоста при обнаружении атак – 30 минут;

– Использовать черный список адресов.

В раздел белый список адресов добавить адрес: 195.98.66.130.

3.1.2 Континент TLS клиент

3.1.2.1 Установка

Пользователь, устанавливающий ПО TLS-клиент, должен обладать правами администратора компьютера.

Поместите установочный диск в устройство чтения компакт- дисков и запустите на исполнение файл Континент TLS-клиент.exe, находящийся в каталоге с дистрибутивом ПО.

На экране появится окно выбора устанавливаемых компонентов.

Выберите компонент «Континент TLS Клиент КС1». На экране появится стартовое окно мастера установки компонента.

Программа установки выполнит диагностику системы, после чего начнется установка ПО. После ее успешного завершения на экране появится сообщение о необходимости перезагрузки компьютера.

Нажмите кнопку «Перезагрузить» в окне сообщения. Начнется перезагрузка компьютера.

После установки TLS-клиента на рабочем столе появится ярлык запуска графического приложения TLS-клиента, а в главном меню Windows появится раздел «Код Безопасности».

3.1.2.2 Регистрация

При первом запуске TLS- клиента пользователю будет предложено зарегистрировать программу на сервере регистрации компании «Код Безопасности».

Доступна онлайн- и офлайн-регистрация. Срок работы без регистрации TLS-клиента ограничен и составляет 14 дней. Количество дней, оставшихся до окончания регистрации, отображается в разделе «О программе». Если в течение этого срока TLS-клиент не зарегистрировать, то при каждом следующем запуске он будет предлагать зарегистрироваться в системе и, в случае отказа, прекращать свою работу.

Для онлайн-регистрации TLS-клиента нажмите кнопку «Да» в открывшемся автоматически окне регистрации или выберите в меню настроек TLS-клиента пункт «Регистрация» и нажмите кнопку «Начать».

Введите требуемые параметры и нажмите кнопку «Готово». Начнется процесс регистрации и подключения к указанному серверу. При его успешном завершении на экране появится соответствующее информационное окно.

После регистрации TLS- клиента в разделе «О программе» вместо текста «Программа не зарегистрирована» появится регистрационный номер программы.

3.1.2.3 Установка сертификатов

Для импорта серверного сертификата выберите в главном меню TLS-клиента пункт «Управление сертификатами». В области отображения информации появится список установленных сертификатов.

На панели инструментов выберите категорию «Серверные сертификаты» и нажмите кнопку «Импортировать». На экране появится стандартное окно открытия файла.

Укажите файл загружаемого сертификата «vrnds.crt» и нажмите кнопку «Открыть». Начнется загрузка и установка сертификата. После успешного

завершения операции на экране появится соответствующее информационное сообщение.

Нажмите кнопку «ОК».

Для установки пользовательского сертификата выберите в главном меню TLS-клиента пункт «Управление сертификатами». В области отображения информации появится список установленных сертификатов.

На панели инструментов выберите категорию «Пользовательские сертификаты» и нажмите кнопку «Импортировать». На экране появится диалог настройки параметров импорта.

В поле «Имя файла» укажите полный путь к файлу user_vrnds(xxxx).cer, содержащему нужный сертификат, и нажмите кнопку «Далее». При импорте пользовательского сертификата появится окно запроса контейнера закрытого ключа сертификата. Выберите требуемый контейнер и нажмите кнопку «Далее».

Проверьте корректность введенных параметров импорта и нажмите кнопку «Готово».

3.1.2.4 Настройка

В основном меню TLS-клиента выберите пункт «Главная». В области отображения информации откроется список имеющихся защищенных ресурсов и TLS-серверов (соединений).

Выберите закладку «Добавить» на панели инструментов, а затем «Ресурс» в раскрывшемся списке. В правой части области отображения информации основного окна появится соответствующий список настроек.

В поле «Адрес» введите имя ресурса:

– dou.vrnds.ru – для работы с базой дошкольных образовательных учреждений;

– oo.vrnds.ru – для работы с базой общеобразовательных учреждений;

– prof.vrnds.ru – для работы с базой профессиональных образовательных учреждений.

3.1.3 ScanOVAL

3.1.3.1 Установка

Установка программы осуществляется с помощью инсталляционного пакета ScanOVAL.msi. Запустите исполняемый файл ScanOVAL.msi. Дождитесь появления окна приветствия и нажмите кнопку «Далее». Далее в появившемся окне будет предложено ознакомиться с лицензионным соглашением. После ознакомления с содержимым выберете пункт «Я

принимаю условия данного лицензионного соглашения» и нажмите кнопку «Далее».

Укажите каталог, в который будут установлены файлы программы. По умолчанию используются следующие каталоги:

– для 32-х битных систем: «C:\Program Files\ScanOVAL»;

– для 64-х битных систем: «C:\Program Files (x86)\ScanOVAL».

В результате нажатия кнопки «Далее» появится окно «Все готово к установке ScanOVAL». В следующем окне необходимо нажать кнопку «Установить», в результате чего появится статусная строка установочного процесса. О завершении процесса установки будет свидетельствовать сообщение «Установка ScanOVAL завершена», при этом на рабочем столе появится ярлык программы.

3.1.3.2 Настройка

Загрузите с сайта https://bdu.fstec.ru/site/scanoval файл базы уязвимостей и укажите его расположение в программе. После этого можно запустить сканирование ПК на наличие уязвимостей, подлежащих устранению.

3.2 Реализация организационных мер

В данном разделе представлен порядок реализации мер, указанных в п. 2.4 требований.

3.2.1 Назначение лица, ответственного за защиту информации

Мероприятия по защите информации, обрабатываемой на АРМ, должны быть возложены на лицо, ответственное на защиту информации.

В случаях, когда на момент реализации указанных мер в организации отсутствует лицо, ответственное за защиту информации, оно должно быть назначено приказом руководителя.

Проект Должностной инструкции лица, ответственного за защиту информации, представлен в Приложении 1 к настоящему документу.

3.2.2 Определение перечня лиц, имеющих право доступа к АРМ

В организации должен быть определен ***Перечень лиц, доступ которых к информации ограниченного доступа (в том числе персональным данным), обрабатываемой в АРМ, необходим им для выполнения ими служебных (трудовых) обязанностей***.

Проект «Перечня лиц…» представлен в Приложении 2 к настоящему документу. Доступ к АРМ лиц, не указанных в данном перечне, должен быть запрещен.

Все лица, включенные в указанный перечень, должны быть ознакомлены с положениями законодательства РФ по вопросам обработки и защиты информации ограниченного доступа, в том числе:

– Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технология и о защите информации»;

– Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– настоящим документом.

По результатам ознакомления работников Оператора с указанными требованиями должна быть создана соответствующая запись в ***Журнале ознакомления работников, непосредственно осуществляющих обработку информации ограниченного доступа (в том числе ПДн) с положениями законодательства РФ и локальными актами по вопросам обработки и защиты информации***.

Проект «Журнала ознакомления…» представлен в Приложении 3 к настоящему документу.

3.2.3 Контроль доступа в помещения, в которых расположены АРМ

В организации должен быть определен ***Перечень помещений, в которых располагаются АРМ, используемые для подключения к ГИС «Образование ВО», или хранятся машинные носители, подключаемые к таким АРМ, а также лиц, имеющих право доступа в них***.

Проект «Перечня помещений…» представлен в Приложении 4 к настоящему документу.

Пребывание в таких помещения лиц, не имеющих право доступа в них, не допускается.

Открытие и закрытие Помещений должны фиксироваться в специальном ***Журнале открытия и закрытия помещений, в которых ведется обработка информации ограниченного доступа***, с указанием лица, осуществившего открытие и закрытие Помещения.

Проект «Журнала открытия и закрытия помещений…» представлен в Приложении 5 к настоящему документу.

3.2.4 Обеспечение безопасности машинных носителей информации

Все машинные носители информации, используемые с АРМ (как встроенные, так и съемные) подлежат учету в специальном ***Журнале учета***

машинных носителей информации ограниченного доступа (в том числе персональных данных).

Проект «Журнала учета…» представлен в Приложении 6 к настоящему документу.

Машинные носители информации, используемые с АРМ, должны храниться только в помещениях/сейфах/шкафах, определенных в ***Перечне мест хранения съемных машинных носителей информации ограниченного доступа (в том числе персональных данных)***.

Проект «Перечня мест хранения…» представлен в Приложении 7 к настоящему документу.

В случаях, когда в помещении отсутствуют сейфы/шкафы, позволяющие исключить бесконтрольный доступ к машинным носителям, такие носители подлежат передаче ответственному за защиту информации по окончании рабочего дня.

3.3 Контроль за реализацией мер

После выполнения всех мероприятий, указанных в разделе 3, ответственным за защиту информации в АРМ должно быть составлено заключение о выполнении организацией всех требований по защите информации, представленных в разделе 2, подписанное руководителем организации.

Копия данного заключения подлежит передаче в ГБУ ДПО «ВИРО им. Н. Ф. Бунакова» в целях предоставления организации учетных данных для подключения к ГИС «Образование ВО».

Проект «Заключения…» представлен в Приложении 8 к настоящему документу.

3.4 Рекомендации по повышению квалификации сотрудников

Сотрудникам, назначенным ответственными за защиту информации, рекомендуется пройти курсы повышения квалификации по направлению XXX

Приложение 1
Должностная инструкция лица, ответственного за защиту информации

1 Общие положения

1.1 Настоящая Должностная инструкция лица, ответственного за защиту информации, **НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ** (далее – Инструкция, Оператор, Ответственный за защиту информации) разработана в соответствии с требованиями пункта:

– пункта 9 Приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– пункта 14 Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2 Инструкция определяет требования к квалификации, ответственность, права и обязанности Ответственного за защиту информации.

1.3 Инструкция вступает в силу с момента ее утверждения руководителем Оператора и действует бессрочно, до ее замены новой Инструкцией или ее отмены на основании приказа руководителя Оператора.

2 Требования к квалификации должностного лица

2.1 Ответственный за защиту информации должен знать и понимать положения следующих документов:

– нормативных правовых актов и методических документов, действующих на территории Российской Федерации, в том числе:

- Федерального закона от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Методического документа «Меры защиты информации в государственных информационных системах», утвержденного ФСТЭК России 11.02.2014 г.;

– внутренних организационно-распорядительных документов по защите информации.

3 Обязанности должностного лица

Ответственный за защиту информации обязан выполнять нижеследующее.

3.1 Участвовать в работах по обеспечению защиты информации ограниченного доступа, обрабатываемой в АРМ Оператора.

3.2 Осуществлять управление (администрирование) системой защиты информации в целях поддержания установленного уровня защищенности информации ограниченного доступа при ее обработке в АРМ Оператора.

3.3 Выполнять периодический анализ сведений об известных угрозах безопасности информации и уязвимостях средств вычислительной техники, и принимать своевременные меры по нейтрализации вновь возникающих актуальных угроз безопасности информации при ее обработке в АРМ Оператора.

3.4 Осуществлять информирование и обучение работников Оператора, задействованных в обработке информации ограниченного доступа в информационных системах Оператора, правилам работы с защищаемой информацией и требованиям нормативных правовых актов Российской Федерации и внутренних организационно-распорядительных документов Оператора в области защиты информации.

4 Права должностного лица

Ответственный за защиту информации имеет право на нижеследующее.

4.1 Запрашивать у руководства и работников Оператора информацию, необходимую для исполнения своих должностных обязанностей.

4.2 Прекращать доступ работников Оператора к АРМ в случаях нарушения этими работниками требований по защите информации, установленных законодательством Российской Федерации, внутренними организационно-распорядительными документами Оператора, эксплуатационной и технической документацией на средства защиты информации, а также вносить руководству Оператора предложения о привлечении к дисциплинарной ответственности таких работников.

4.3 Вносить руководству Оператора предложения о совершенствовании процессов защиты информации в информационных системах Оператора.

5 Ответственность должностного лица

Ответственный за защиту информации несет ответственность за нижеследующее.

5.1 Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией.

5.3 За нарушение конфиденциальности информации, ставшей известной ему в рамках исполнения своих должностных обязанностей.

Приложение 2
Перечень лиц, доступ которых к информации ограниченного доступа (в том числе персональным данным), обрабатываемой в АРМ, необходим им для выполнения ими служебных (трудовых) обязанностей

№ п/п	Наименование должности	Наименование АРМ*
1	Подразделение 1	
1.1	Должность 1.1	АРМ № 1
1.2	Должность 1.2	АРМ № 1
1.3	Должность 1.3	АРМ № 1
1.4	Должность 1.4	АРМ № 1
1.5	Должность 1.5	АРМ № 1
1.6	Должность 1.6	АРМ № 1
2	Подразделение 2	
2.1	Должность 2.1	АРМ № 1
2.2	Должность 2.2	АРМ № 1
2.3	Должность 2.3	АРМ № 1
2.4	Должность 2.4	АРМ № 1
2.5	Должность 2.5	АРМ № 1
2.6	Должность 2.6	АРМ № 1
* указать при использовании в организации одновременно нескольких АРМ для доступа к ГИС «Образование ВО»		

Приложение 3
Журнал ознакомления работников

Журнал
ознакомления работников, непосредственно осуществляющих обработку информации ограниченного доступа (в том числе персональных данных) с положениями законодательства Российской Федерации и локальными актами по вопросам обработки и защиты информации

Начат «____» _____ 202_ г. Окончен «____» _____ 202_ г.

_____ _____

_____ / _____ / _____ / _____ /

На _____ листах

Указанные ниже работники Государственного бюджетного учреждения дополнительного профессионального образования Воронежской области «Институт развития образования имени Н. Ф. Бунакова» ознакомлены со следующими нормативными правовыми актами и организационно-распорядительными документами в области обработки и обеспечения безопасности информации ограниченного доступа (в том числе персональных данных):

– нормативными правовыми актами, действующими на территории Российской Федерации, в том числе:

- Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технология и о защите информации»;
- Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– внутренними организационно-распорядительными документами в области обработки ПД.:

Дата	ФИО ознакомившего	Подпись ознакомившего	ФИО работника	Подпись работника	Примечание

Приложение 4
Перечень помещений, в которых расположены АРМ и/или хранятся машинные носители информации ограниченного доступа, а также лиц, имеющих право доступа в них

№ п/п	Номер помещения	Перечень допущенных лиц

Приложение 5
Журнал открытия/закрытия помещений

Журнал
учета открытия/закрытия помещений, в которых ведется обработка информации ограниченного доступа (в том числе персональных данных)

Начат «____» _____ 202_ г.

_____
_____ / _____ /

Окончен «____» _____ 202_ г.

_____
_____ / _____ /

На _____ листах

Дата	Помещение №	Время открытия помещения	ФИО сотрудника, подпись	Время закрытия помещения	ФИО сотрудника, подпись

Приложение 6
Журнал учета машинных носителей информации

Журнал
учета машинных носителей информации ограниченного доступа
(в том числе персональных данных)

Начат «____» _____ 202_ г.

_____

_____ / _____ /

Окончен «____» _____ 202_ г.

_____

_____ / _____ /

На _____ листах

№ п/п	Заводской/ учетный номер	Тип носителя	Место установки (для несъемных)	ФИО ответственного (для съемных)	Расписка в получении, дата (для съемных)	Расписка в обратном приеме, дата (для съемных)	Место хранения	Сведения об уничтожении, номер акта
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								

Приложение 7
Перечень мест хранения съемных машинных носителей информации ограниченного доступа (в том числе персональных данных)

№ п/п	Наименование должности	Номер помещения/сейфа/шкафа
3	Подразделение 1	
3.1	Должность 1.1	Помещение 101, сейф 0001
3.2	Должность 1.2	Помещение 102, сейф 0002
3.3	Должность 1.3	Помещение 103, сейф 0003
3.4	Должность 1.4	Помещение 104, сейф 0004
3.5	Должность 1.5	Помещение 105, сейф 0005
3.6	Должность 1.6	Помещение 106, сейф 0006
4	Подразделение 2	
4.1	Должность 2.1	Помещение 201, сейф 0007
4.2	Должность 2.2	Помещение 202, сейф 0008
4.3	Должность 2.3	Помещение 203, сейф 0009
4.4	Должность 2.4	Помещение 204, сейф 0010
4.5	Должность 2.5	Помещение 205, сейф 0011
4.6	Должность 2.6	Помещение 206, сейф 0012

Приложение 8 Заключение по результатам оценки соответствия

УТВЕРЖДАЮ

Руководитель организации

_____ФИО

м.п.

«___»_____ 202_ г.

Заключение
по результатам оценки соответствия реализованных мер защиты информации, реализованных **НАЗВАНИЕ ОРГАНИЗАЦИИ**, требованиям по защите информации, предъявляемым к автоматизированным рабочим местам, используемым для подключения к государственной информационной системе «Образование Воронежской области»

В ходе проведенной оценки соответствия установлено, что:

– используемые средства защиты информации установлены и настроены в соответствии с требованиями Порядка подключения автоматизированных рабочих мест внешних пользователей к Государственной информационной системе «Образование Воронежской области»;

– назначено лицо ответственное за защиту информации;

– доступ к автоматизированным рабочим местам имеют доступ только сотрудники, определенные специальным перечнем;

– обеспечивается контроль доступа в помещения с автоматизированными рабочими местами, исключающий неправомерный доступ к ним со стороны лиц, не допущенных к обработке информации;

– ведется учет используемых машинных носителей информации ограниченного доступа (в том числе персональных данных).

Ответственный за защиту информации, должность	_____ (дата, подпись)	ФИО