Министерство образования и науки Нижегородской области

П Р И К А З

21.09.2023 № 316-01-63-2593/23

г. Нижний Новгород

Об утверждении Технических условий подключения к объекту информатизации модуль «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа»

В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», п р и к а з ы в а ю:

1. Утвердить прилагаемые к настоящему приказу «Технические условия подключения к объекту информатизации модуль «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа».

2. Контроль за исполнением настоящего приказа оставляю за собой.

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 037298B5E7892DD35AC4C4B547D9DAF3
Кому выдан: Пучков Михаил Юрьевич
Действителен: с 26.07.2023 до 18.10.2024

И.о министра М.Ю. Пучков

УТВЕРЖДЕНО
приказом министерства образования
и науки Нижегородской области

от 21.09.2023 № 316-01-63-2593/23

Технические условия подключения к объекту информатизации модуль «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа»

Нижний Новгород
2023

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Администратор ИБ	Администратор информационной безопасности
АРМ	Автоматизированное рабочее место
ГИС	Государственная информационная система
АИС	Автоматизированная информационная система
ИБ	Информационная безопасность
КСЗ	Комплекс средств защиты информации
НСД	Несанкционированный доступ
ОС	Операционная система
ОТСС	Основные технические средства и системы
ПДн	Персональные данные
ПО	Программное обеспечение
РГИС НОП	Государственная информационная система Региональная государственная информационная система «Нижегородская образовательная платформа»
САВЗ	Средство антивирусной защиты информации
СЗИ НСД	Средство (система) защиты информации от несанкционированного доступа
СКЗИ	Средство криптографической защиты информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие «Технические условия подключения к объекту информатизации модуль «Учет контингента обучающихся» РГИС НОП» (далее – Технические условия) определяют требования и условия, а также устанавливают порядок подключения автоматизированных информационных систем общеобразовательных организаций, организаций среднего профессионального образования, органов управления в сфере образования муниципальных и городских округов Нижегородской области и иных уполномоченных организаций (далее — внешние АИС) к РГИС НОП.

Настоящие технические условия разработаны в соответствии с:

– Федеральным законом Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных»,

– Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",

– нормативными правовыми актами, техническими и методическими документами ФСТЭК России и ФСБ России в области обеспечения информационной безопасности и защиты персональных данных.

Требования технических условий устанавливают порядок выполнения работ по подключению внешних АИС к РГИС НОП, а также состав программно-технических средств, в том числе средств защиты информации, необходимых для организации защищенного взаимодействия внешних АИС и РГИС НОП, как информационных систем персональных данных.

Основной целью настоящих технических условий является определение необходимых требований и условий по обеспечению безопасности и защите персональных данных в РГИС НОП.

2. ХАРАКТЕРИСТИКА РГИС НОП

Цель РГИС НОП – оказание государственных и муниципальных услуг в электронном виде, в том числе:

– предоставление информации о текущей успеваемости обучающегося, ведения электронного дневника и электронного журнала успеваемости;

– приема обучающихся в образовательные организации для получения основного общего и среднего профессионального образования;

– автоматизации работы образовательной организации, создание цифровой образовательной среды посредством государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа»

– выполнении иных требований законодательства Российской Федерации.

Внешние АИС функционируют с РГИС НОП и ведут обработку следующих сведений:

– фамилия, имя, отчество;

– пол;

– дата рождения;

– контактный телефон (при наличии);

– гражданство;

– СНИЛС (при наличии);

– реквизиты документа, удостоверяющего личность;

– наименование образовательной организации, в которой осваивает образовательные программы основного общего, среднего профессионального образования;

– номер класса/группы (при наличии).

Внешними АИС являются АИС образовательных учреждений, органов управления образованием муниципальных и городских округов Нижегородской области, иных уполномоченных организаций. В качестве данных АИС рассматриваются как локальные информационные системы, развернутые на единственном автоматизированном рабочем месте, так и распределенные информационные системы, функционирующие на базе локальной или распределенной вычислительной сети.

3. ПОРЯДОК ПОДКЛЮЧЕНИЯ К РГИС НОП

3.1. Порядок подключения внешнего АИС к РГИС НОП включает в себя следующие этапы:

3.1.1. Приобретение технических средств, программного обеспечения и средств защиты информации, необходимых для обеспечения безопасности информации в РГИС НОП с установленными в пункте 6 настоящих Технических условий Требований к составу средств защиты информации.

3.1.2. Определить границы контролируемой зоны где расположен объект информатизации.

3.1.3. Ограничить доступ в помещение, в котором размещаются ОТСС объекта информатизации.

3.1.4. Назначение лиц, ответственных за обеспечение безопасности информации, обрабатываемой в РГИС НОП.

3.1.5. Назначение лиц, допущенных к работе в РГИС НОП.

3.1.6. Установка и конфигурация технических и программных средств, а также средств средств защиты информации в соответствии с Требованиями.

3.1.7. Выполнение иных организационных мероприятий по защите информации.

3.1.8. Направление акта о готовности подключения АИС к РГИС НОП по утвержденной форме в соответствии с настоящими Техническими условиями.

3.2. Для проведения работ по защите информации в ходе создания/эксплуатации АИС в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие:

– лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации;

– проектирования в защищенном исполнении средств и систем информатизации, установки, монтажа, средств защиты информации;

– лицензию ФСБ России на деятельность по распространению шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации.

4. ТРЕБОВАНИЯ К СОСТАВУ ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

4.1. В ходе подготовки подключения внешней АИС к РГИС НОП оператором подключаемых объектов должны быть реализованы следующие организационные мероприятия:

4.1.1. Реализация организационных мер, направленных на ограничение физического доступа в помещение, в котором размещается подключенная АИС к РГИС НОП (утверждение списка лиц, допущенных в помещение, в котором размещаются ОТСС АРМ, реализация мероприятий по ограничению физического доступа в соответствии с утвержденными правилами пропускного и внутриобъектового режимов).

4.1.2. Ознакомление пользователей АИС с требованиями эксплуатационной документации на систему защиты информации РГИС НОП и используемых в ее составе средств защиты информации.

4.1.3. Определение перечня работников, допущенных к работе с СКЗИ (утверждение списка лиц).

4.1.4. Определение мест хранения СКЗИ и ключевых носителей.

4.1.5. Обеспечение поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним.

4.1.6. Выполнение требований к эксплуатации и правил пользования средствами защиты информации, используемыми в составе КСЗ, в т.ч. СКЗИ.

5. ТРЕБОВАНИЯ К СОСТАВУ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АРМ

5.1. С учетом необходимости обеспечения соответствия требованиям «Технического задания на создание системы защиты информации объекта информатизации РГИС НОП» к АРМ предъявляются следующие дополнительные требования:

5.1.1. На АРМ запрещается использование технологий беспроводной передачи информации (Wi-Fi, Bluetooth, IrDa и т.п.).

5.1.2. На АРМ запрещается установка средств разработки и отладки программного обеспечения. Необходимо исключить попадание в систему средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

5.1.3. Используемое системное и прикладное программное обеспечение должно быть лицензионным и иметь поддержку производителя, включающую выпуск обновлений.

5.1.4. На АРМ должно быть исключено использование пакетов программного обеспечения:

– позволяющего удаленно управлять АРМ;

– средств аудио- и видеоконференцсвязи;

– веб-конференций, веб-чатов и т.п.;

– не участвующего в технологическом процессе обработки информации и не требующееся для выполнения должностных обязанностей работника, являющегося пользователем АИС.

6. ТРЕБОВАНИЯ К СОСТАВУ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. В соответствии с требованиями Технического задание необходимо обеспечить использование в составе АРМ отечественных средств защиты информации, сертифицированных в установленном законодательством РФ порядке по требованиям безопасности информации ФСТЭК России и ФСБ России:

- СЗИ НСД,

- САВЗ,

- программный комплекс «VipNet Client 4.X» с подключением к защищенной сети передачи данных № 6526.

7. ТРЕБОВАНИЯ К КОНФИГУРАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

7.1. Доступ к BIOS/UEFI АРМ должен быть ограничен путем установки пароля на доступ, соответствующего требованиям парольной политики объекта информатизации, в том числе ГИС.

7.2. Дополнительные требования к конфигурации технических средств не предъявляются.

7.3. Перед установкой системного и прикладного программного обеспечения требуется произвести с помощью отдельного АРМ проверку дистрибутивных носителей на отсутствие вредоносного кода с помощью средств антивирусной защиты информации, имеющих актуальные базы сигнатур.

7.4. Установленное системное программное обеспечение должно соответствовать следующим требованиям:

– Должно быть настроено обновление программного обеспечения САВЗ в автоматическом режиме.

– Встроенный брэндмауэр операционной системы должен быть отключен, включен брэндмауэр СКЗИ.

– АРМ не должен быть включен в состав домена службы каталогов Active Directory и администрироваться исключительно локально;

– Учетная запись «Гость» должна быть отключена.

– Рекомендуется исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек, системного реестра, для всех, включая группу Administrators.

7.5. На АРМ должна быть установлена только одна ОС.

7.6. На АРМ необходимо использовать исключительно отечественное лицензионное программное обеспечение СЗИ с его регулярным обновлением.

7.7. Необходимо ограничить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из недоверенных источников, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносных программ.

8. ТРЕБОВАНИЯ К КОНФИГУРАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. Администратор ИБ производит установку средств защиты информации исключительно в следующем порядке:

8.1.1. Установка средств межсетевого экранирования и криптографической защиты информации «VipNet Client 4.X».

8.1.2. Установка СЗИ НСД.

8.1.3. Установка САВЗ.

8.2. Установка вышеперечисленных средств защиты информации должна производиться администратором информационной безопасности в соответствии с требованиями эксплуатационной документации на указанные средства защиты информации и утвержденной инструкцией администратора информационной безопасности АИС.

8.3. В целях обеспечения безопасности информации в РГИС НОП к АИС предъявляются требования к третьему классу защищенности по обеспечению безопасности информации (К-3) и поддержания третьего уровня защищенности обрабатываемой информации (УЗ-3) в соответствии с приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

8.4. Каждый пользователь АИС обеспечивается персональной учетной записью с использованием механизмов СЗИ НСД.

8.5. После установки и конфигурации системного, прикладного программного обеспечения и средств защиты информации, системный блок АРМ должен быть опечатан.

9. УПРАВЛЕНИЕ ДОСТУПОМ К РЕСУРСАМ СЕГМЕНТА РГИС НОП

9.1. Процедуры управления доступом к модулю «Учет контингента обучающихся» РГИС НОП реализуются администраторами информационной безопасности оператора подключаемых объектов и ГБОУ ДПО НИРО на основании акта о готовности к подключению АИС/АРМ оператора подключаемых объектов к РГИС НОП (форма акта приведена в Приложении 1 к настоящим Техническим условиям), с приложением копии акта/аттестата соответствия УЗ-3, подписанные лицензиатом ФСТЭК России.

9.2. Ежегодно, не позднее 31 сентября направление в ГБОУ ДПО НИРО подтверждения соответствия АРМ к предъявляемым настоящими Техническими условиями требованиям (форма акта приведена в Приложении 2 к настоящим Техническим условиям), с приложением копии акта/аттестата соответствия УЗ-3, подписанные лицензиатом ФСТЭК России.

9.3. Хранение одного экземпляра утвержденного акта о готовности и подтверждения соответствия осуществляется Администратором безопасности информации ГБОУ ДПО НИРО в деле.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Работники ГБОУ ДПО НИРО и операторы подключаемых АИС несут персональную ответственность за реализацию мероприятий, связанных с управлением доступом и обеспечением информационной безопасности, предусмотренных настоящими Техническими условиями.

10.2. Контроль выполнения мероприятий, предусмотренных настоящими Техническими условиями, реализуется администраторами информационной безопасности ГБОУ ДПО НИРО.

ПРИЛОЖЕНИЕ 1
к «Техническим условиям...»

Для служебного пользования

Экз.№____

«У Т В Е Р Ж Д А Ю»

Должность руководителя оператора
внешних АИС, подключаемых к
модулю «Учет контингента
обучающихся» РГИС НОП

_____ Ф.И.О. руководителя

«____»_____20__ г.

АКТ

**о готовности к подключению к модулю «Учет контингента обучающихся»
государственной информационной системы
Региональная государственная информационная система
«Нижегородская образовательная платформа»**

_____
(указывается наименование оператора подключаемых АИС)

Настоящий акт составлен по результатам проверки готовности к подключению автоматизированного рабочего места *Наименование оператора подключаемых объектов* (далее – *АРМ,* объект информатизации*)* к модулю «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа» (далее – РГИС НОП).

В ходе проверки установлено, что требования и условия по обеспечению информационной безопасности, установленные «Техническими условиями подключения к объекту информатизации модуль «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа» в *Наименование оператора подключаемых объектов* выполняются, в частности:

1. Определены границы контролируемой зоны в соответствии с _____.
2. Назначение ответственные лица за обеспечение безопасности информации, обрабатываемой в РГИС НОП в соответствии с _____.
3. Назначены лица, допущенные к работе в РГИС НОП в соответствии с _____.
4. Все ОТСС объекта информатизации расположены в пределах контролируемой зоны. Доступ в помещение, в котором размещаются ОТСС объекта информатизации, ограничен и предоставляется согласно «Перечня лиц, допущенных в помещение №____».
5. Приказом *Руководителя оператора подключаемых объектов №___ от _____20__ г.* администратором информационной безопасности назначен *Должность Ф.И.О.*

6. В составе системы защиты информации АИС обеспечивается использование следующих сертифицированных по требованиям безопасности информации средств защиты информации:

п/п	Наименование и тип средства защиты информации	Сведения о лицензиях	Зав. номер СЗЗ

7. Все технические и программные средства, в том числе средства защиты информации работоспособны, комплектны, функционируют в штатном режиме. Системный блок АРМ опечатан.

8. Конфигурация технических и программных средств, в том числе средств защиты информации, соответствует установленным требованиям и условиям по защите информации.

9. В *Наименование оператора подключаемых объектов* в отношении АИС обеспечивается ведение «Журнала учета съемных машинных носителей информации», разработаны и утверждены:

– Перечень защищаемых информационных ресурсов.
– Матрица доступа (включая правила фильтрации сетевого трафика).

10. Фактические структурно-функциональные характеристики объекта информатизации, состав ОТСС, программного обеспечения, средств защиты информации, субъектов и объектов доступа, а также реализованные правила разграничения доступа соответствует документированным сведениям.

11. Пользователи объекта информатизации ознакомлены с требованиями эксплуатационной документации на систему защиты информации, а также используемое программное обеспечение и средства защиты информации.

12. Сведения об акте/аттестате соответствия: выдан *Наименование лицензиата ФСТЭК России*, № ____ от «__» _____20__г. Срок действия до «___»_____20___г.

АИС/АРМ *Наименование оператора подключаемых объектов* соответствует требованиям защиты информации по УЗ-3.

АИС/АРМ *Наименование оператора подключаемых объектов* готово к подключению к модулю «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа».

Разработано:
Администратор информационной безопасности *Наименование оператора подключаемых объектов*

«____» _____ 20___ г. _____ _____
(подпись) *(фамилия, имя, отчество)*

Согласовано:
Администратор информационной безопасности ГБОУ ДПО НИРО

«____» _____ 20___ г. _____ _____
(подпись) *(фамилия, имя, отчество)*

Согласовано:
Администратор информационной безопасности министерства образования и науки Нижегородской области

«____» _____ 20___ г. _____ _____
(подпись) *(фамилия, имя, отчество)*

ПРИЛОЖЕНИЕ 2
к «Техническим условиям...»

Для служебного пользования

Экз.№____

«У Т В Е Р Ж Д А Ю»

Должность руководителя оператора
внешних АИС, подключаемых к
модулю «Учет контингента
обучающихся» РГИС НОП

_____ Ф.И.О. руководителя

«____»_____20__ г.

АКТ

проверки подключенной внешней АИС/АРМ
к модулю «Учет контингента обучающихся»
государственной информационной системы
Региональная государственная информационная система
«Нижегородская образовательная платформа»

_____
(указывается наименование оператора подключаемых объектов)

Настоящий акт составлен по результатам проверки подключенной внешней АИС/АРМ *Наименование оператора подключаемых объектов* (далее – *АИС/АРМ,* объект информатизации*)* к модулю «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа» (далее – РГИС НОП).

В ходе проверки установлено, что требования по обеспечению информационной безопасности, установленные «Техническими условиями подключения к объекту информатизации модуль «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа» в *Наименование оператора подключаемых объектов* выполняются, в частности:

1. Все ОТСС объекта информатизации расположены в пределах контролируемой зоны. Доступ в помещение, в котором размещаются ОТСС объекта информатизации, ограничен.

2. В составе системы защиты информации АИС обеспечивается использование следующих сертифицированных по требованиям безопасности информации средств защиты информации:

п/п	Наименование и тип средства защиты информации	Сведения о лицензиях	Зав. номер СЗЗ

3. Все технические и программные средства, в том числе средства защиты информации работоспособны, комплектны, функционируют в штатном режиме. Системный блок АРМ опечатан.

4. Конфигурация технических и программных средств, в том числе средств защиты информации, соответствует установленным требованиям и условиям по защите информации.

5. Сведения об акте/аттестате соответствия: выдан *Наименование лицензиата ФСТЭК России, №_____ от «___» _____20__г. Срок действия до «___»_____20___г.*

АИС/АРМ *Наименование оператора подключаемых объектов,* подключенный к модулю «Учет контингента обучающихся» государственной информационной системы Региональная государственная информационная система «Нижегородская образовательная платформа», соответствует требованиям защиты информации по УЗ-3.

Разработано:
Администратор информационной безопасности *Наименование оператора подключаемых объектов*

«____» _____ 20___ г. _____ _____
(подпись) *(фамилия, имя, отчество)*

Согласовано:
Администратор информационной безопасности ГБОУ ДПО НИРО

«____» _____ 20___ г. _____ _____
(подпись) *(фамилия, имя, отчество)*

Согласовано:
Администратор информационной безопасности министерства образования и науки Нижегородской области

«____» _____ 20___ г. _____ _____
(подпись) *(фамилия, имя, отчество)*