Министерство цифрового развития и связи Нижегородской области

Министерство спорта Нижегородской области

ПРИКАЗ

от 02.09.2025 № 324-128-од

от 02.09.2025 № 339

г. Нижний Новгород

Об утверждении «Правил подключения участников информационного взаимодействия к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области»

В целях обеспечения защиты информации, обрабатываемой в региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области»

п р и к а з ы в а е м:

1. Утвердить прилагаемые «Правила подключения участников информационного взаимодействия к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области» (далее – «Правила подключения»).

2. Участникам информационного взаимодействия, осуществляющим полномочия в сфере «Физическая культура и спорт» и получающим доступ к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области», обеспечить выполнение требований «Правил подключения».

3. Оператору региональной государственной информационной системы «Единый агрегатор физкультурно-спортивных организаций Нижегородской области» обеспечивать подключение участников информационного

взаимодействия, осуществляющих полномочия в сфере «Физическая культура и спорт» при выполнении требований «Правил подключения».

Министр

_____ А.А.Синелобов

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

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00FF6AE557F0C086E1076027D2648ED688
Владелец: Синелобов Александр Анатольевич
Действителен: с 26.05.2025 по 19.08.2026

Министр

_____ Д.С.Кабайло

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

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 6548D18CD3B100B929F3A681AA36580A
Владелец: Кабайло Дмитрий Сергеевич
Действителен: с 19.06.2025 по 12.09.2026

УТВЕРЖДЕНЫ

приказом министерства цифрового развития и связи Нижегородской области и министерства спорта Нижегородской области от 02.09.2025 № 324-128-од/339

Правила
подключения участников информационного взаимодействия к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области»

1. Общие положения

Настоящие Правила устанавливают требования и условия предоставления доступа к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области» (далее – РГИС ЕАФСО НО) участникам информационного взаимодействия:

- министерству спорта Нижегородской области и подведомственным ему государственным учреждениям, осуществляющим полномочия в сфере «Физическая культура и спорт»;

- органам местного самоуправления Нижегородской области и подведомственным им муниципальным учреждениям, осуществляющим полномочия в сфере «Физическая культура и спорт».

РГИС ЕАФСО НО является государственной информационной системой (далее – ГИС) регионального масштаба.

В РГИС ЕАФСО НО осуществляется обработка персональных данных субъектов, не являющихся сотрудниками оператора системы (обработка иных категорий персональных данных, общедоступных персональных данных).

В отношении РГИС ЕАФСО НО выдан аттестат соответствия требованиям о защите информации (от 19.12.2024 №3950.00018.2024), не составляющей государственную тайну, содержащейся в ГИС, утвержденным приказом ФСТЭК России от 11.02.2013 № 17, предъявляемым к ГИС третьего класса защищенности (К3).

Обладатель информации, содержащейся в РГИС ЕАФСО НО – министерство спорта Нижегородской области.

Обладатель информации в части формирования требований к защите информации, содержащейся в РГИС ЕАФСО НО – министерство цифрового развития и связи Нижегородской области.

Оператор РГИС ЕАФСО НО – государственное автономное учреждение Нижегородской области «Центр координации проектов цифровой экономики».

Выполнение настоящих Правил является обязательным для подключения участника информационного взаимодействия к ресурсам РГИС ЕАФСО НО.

2. Порядок подключения к ресурсам РГИС ЕАФСО НО

В целях подключения к ресурсам РГИС ЕАФСО НО участник информационного взаимодействия выполняет комплекс организационных и технических мероприятий:

- выделяет автоматизированное рабочее место (далее – АРМ), соответствующее требованиям, установленным настоящими Правилами;

- проводит оснащение, установку и настройку на АРМ комплекса средств защиты информации;

- организует защиту помещения, в котором расположен АРМ;

- назначает персонал, ответственный за работу на АРМ;

- утверждает комплект организационно-распорядительных документов (далее – ОРД) для работы на АРМ;

- подтверждает Оператору РГИС ЕАФСО НО выполнение требований по защите информации предоставлением акта, подтверждающего проведение необходимых мероприятий на АРМ для подключения к РГИС ЕАФСО НО.

3. Требования к вариантам подключения

<table>
<tr><th colspan="6">Вариант подключения № 1</th></tr>
<tr><td>1</td><td>Операционная система</td><td colspan="4">ОС Windows 10, 11
(лицензия для Бизнеса)</td></tr>
<tr><td>2</td><td>Прикладное программное обеспечение</td><td colspan="4">Веб-браузер</td></tr>
<tr><td>3</td><td colspan="5">Средства антивирусной защиты, имеющие действующие сертификаты соответствия ФСТЭК России. Соответствует требованиям документов: Требования к средствам антивирусной защиты (ФСТЭК России, 2012), Требования по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, по 4 уровню (ФСТЭК России, 2020).</td></tr>
<tr><td>4</td><td>Программный или программно-аппаратный комплекс (далее-ПАК), сертифицированный по требованиям ФСБ России к средствам криптографической защиты информации (далее -СКЗИ) класса минимум КС1 и имеющий действующие сертификаты соответствия ФСБ России</td><td>ПАК ViPNet Coordinator</td><td>АПКШ Континент</td><td>ПК ViPNet Client 4</td><td>Континент АП</td></tr>
<tr><th colspan="5">Вариант подключения № 2</th><th></th></tr>
</table>

1	Операционные системы, имеющие действующие сертификаты соответствия ФСТЭК России. Соответствует требованиям документов: Требования по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, по 4 уровню (ФСТЭК России, 2020).				
2	Прикладное программное обеспечение	Веб-браузер			
3	Средства антивирусной защиты, имеющие действующие сертификаты соответствия ФСТЭК России. Соответствует требованиям документов: Требования к средствам антивирусной защиты (ФСТЭК России, 2012), Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, по 4 уровню (ФСТЭК России, 2020).				
4	Программный или ПАК, сертифицированный по требованиям ФСБ России к СКЗИ минимум КС1 и имеющий действующие сертификаты соответствия ФСБ России	ПАК ViPNet Coordinator	АПКШ Континент	ПК ViPNet Client 4U	Континент АП
Вариант подключения № 3					
1	Операционные системы российского производства, не имеющие действующие сертификаты соответствия ФСТЭК России				
2	Прикладное программное обеспечение	Веб-браузер			
3	Средства антивирусной защиты, имеющие действующие сертификаты соответствия ФСТЭК России. Соответствует требованиям документов: Требования к средствам антивирусной защиты (ФСТЭК России, 2012), Требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, по 4 уровню (ФСТЭК России, 2020)				
4	Программный или ПАК, сертифицированный по требованиям ФСБ России к СКЗИ класса минимум КС1 и имеющий действующие сертификаты соответствия ФСБ России	ПАК ViPNet Coordinator	АПКШ Континент	ПК ViPNet Client 4U	Континент АП

3.1. Организационные требования к АРМ

АРМ должен располагаться в границах контролируемой зоны участника информационного взаимодействия (границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории).

Корпус АРМ должен быть опечатан способом, обеспечивающим контроль за его несанкционированным вскрытием.

Применению на АРМ подлежат только учтенные установленным порядком съемные носители информации, разрешенные политиками средств защиты информации к использованию на данном АРМ.

На АРМ не допускается подключение мобильных устройств (смартфонов, планшетов, и т.п.) как в целях использования в качестве съемных носителей информации, так и с целью подзарядки устройства.

Программное обеспечение АРМ должно состоять из комплекса программных средств, обеспечивающих непосредственное выполнение технологического процесса обработки информации в РГИС ЕАФСО НО.

При использовании программного обеспечения (далее – ПО) на АРМ должны быть соблюдены условия лицензионных соглашений с разработчиками ПО. В операционной системе должны быть выполнены корректные настройки часового пояса, даты и времени.

На АРМ не допускается использование технологий виртуализации, программных средств разработки и отладки приложений. Средства беспроводных технологий доступа (при их наличии) должны быть отключены/ извлечены.

Все оборудование АРМ должно находиться в технически исправном состоянии.

3.2.Общие требования к составу средств защиты информации АРМ

На АРМ должны использоваться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании» и имеющие техническую поддержку разработчика.

Состав средств защиты информации АРМ должен включать:

- средство антивирусной защиты информации. Антивирусное ПО на АРМ должно быть сертифицировано ФСТЭК России (а при наличии ПО средства криптографической защиты информации – сертифицировано ФСБ России в соответствии с требованиями эксплуатационной документации СКЗИ (при наличии требования));

- АРМ должен иметь подключение к корпоративной сети передачи данных (далее – и КСПД) через программное СКЗИ или программно-аппаратное СКЗИ, совместимое с оборудованием КСПД, сертифицированное ФСБ России;

- подключение АРМ к внешним каналам связи должно быть обеспечено с применением сертифицированного ФСТЭК России средства межсетевого экранирования.

Необходимо проводить анализ защищенности АРМ не реже чем 1 раз в полгода (6 месяцев).

Для установки и настройки средств защиты информации могут быть привлечены:

- организация, имеющая лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации;

- в случае поставки, установки или обслуживания СКЗИ – организация, имеющая лицензию ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Параметры настроек установленных на АРМ средств защиты информации должны быть выполнены в соответствии с эксплуатационной документацией и обеспечивать реализацию базового набора мер защиты информации в соответствии с приложением № 2 к приказу Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для третьего класса защищенности, адаптированного к структурно-функциональным характеристикам АРМ, информационным технологиям, особенностям функционирования АРМ.

3.3. Настройки антивирусного ПО

На АРМ должно использоваться антивирусное ПО, входящее в реестр отечественного ПО и имеющее сертификат ФСТЭК/ ФСБ России.

Настройки антивирусного ПО должны обеспечить:

- актуальность антивирусных сигнатурных баз;
- антивирусную защиту АРМ в постоянном режиме;
- автоматическую проверку подключаемых USB-устройств.

3.4. Организация защиты помещений

В помещении с размещенным АРМ должны соблюдаться следующие условия:

- ограничение и контроль доступа посторонних лиц в помещение с размещенным АРМ;

- при нахождении в рабочем помещении посторонних лиц должен проводиться визуальный контроль их действий и исключаться возможность просмотра ведущихся работ;

- расположение монитора АРМ должно исключать случайный просмотр информации на нем посторонними лицами и другими сотрудниками в том числе через окна помещения.

Мероприятия по ограничению и контролю доступа в помещение с расположенным АРМ включают:

- утверждение перечня лиц, допущенных в помещение;

- помещение, в котором размещен АРМ, имеет прочную входную дверь с замком, гарантирующим надежное закрытие в нерабочее время;

- окна помещения, в котором размещен АРМ, оборудованы металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения (в случае, если помещения расположены на первых и (или) последних этажах зданий, а также окна помещений находятся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц).

3.5. Требования к квалификации персонала участника информационного взаимодействия

Пользователи, допущенные к работе на АРМ участника информационного взаимодействия, подключенном к РГИС ЕАФСО НО, должны владеть навыками работы с персональным компьютером.

Лица, ответственные за обеспечение защиты информации, обрабатываемой с использованием АРМ, за внесение изменений в конфигурацию АРМ и средств защиты информации АРМ, за выявление инцидентов и реагирование на них, должны обладать достаточными для выполнения своих обязанностей знаниями и умениями.

3.6. Состав ОРД

Участник информационного взаимодействия должен разработать и утвердить в соответствии с установленным порядком комплект ОРД, включающий документы:

- о назначении:

1) структурного подразделения или должностного лица (работника), ответственного за защиту информации, обрабатываемой в РГИС ЕАФСО НО с использованием АРМ;

2) лица, ответственного за выявление инцидентов и реагирование на них;

3) лица, ответственного за планирование и контроль мероприятий по защите информации, обрабатываемой в РГИС ЕАФСО НО с использованием АРМ;

4) лиц, которым разрешены действия по внесению изменений в конфигурацию АРМ и средств защиты информации АРМ, и их полномочий;

5) лиц, доступ которых к РГИС ЕАФСО НО необходим в целях выполнения должностных обязанностей;

6) лиц, допущенных к работе с СКЗИ на АРМ;

7) лиц, допущенных в помещение, где размещен АРМ.

- определяющие:

1) границы контролируемой зоны, в пределах которой постоянно размещается АРМ;

2) права и обязанности пользователя АРМ;

3) права и обязанности назначенных ответственных лиц;

4) порядок администрирования и использования средств защиты АРМ;

5) парольную политику при работе с АРМ;

6) правила доступа в помещение с размещенным АРМ в рабочее и нерабочее время, а также в нештатных ситуациях (реализация мероприятий по ограничению физического доступа в соответствии с утвержденными правилами пропускного и внутриобъектового режимов);

7) порядок учета машинных носителей информации;

8) порядок внесения изменений в конфигурацию АРМ и средств защиты информации АРМ;

9) порядок обнаружения и реагирования на инциденты, которые могут привести к сбоям или нарушению функционирования АРМ и РГИС ЕАФСО НО и (или) к возникновению угроз безопасности информации.

При разработке ОРД необходимо руководствоваться:

- Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

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

- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- методическим документом ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах»;

- формулярами, эксплуатационной и технической документацией на средства защиты информации, настоящими Правилами.

Разрабатываемые ОРД должны содержать требования о защите информации, предъявляемые к защите персональных данных при их обработке в информационных системах персональных данных не ниже третьего уровня защищенности персональных данных и в государственных информационных системах третьего класса защищенности, адаптированные к структурно-функциональным характеристикам АРМ, информационным технологиям, особенностям функционирования АРМ.

Работники участника информационного взаимодействия, допущенные к работе на АРМ, должны быть ознакомлены с положениями утвержденных ОРД и с требованиями эксплуатационной документации на средства защиты информации, установленные на АРМ, под подпись.

4. Подтверждение выполнения требований по защите информации

После реализации участником информационного взаимодействия всех требований по защите информации, указанных в настоящих Правилах, участник информационного взаимодействия проводит мероприятия по оценке и подтверждению выполнения мероприятий

по защите информации на АРМ участника информационного взаимодействия для подключения к РГИС ЕАФСО НО:

- приказом участника информационного взаимодействия создается комиссия по проведению приемочных испытаний АРМ, подключаемого к РГИС ЕАФСО НО;

- комиссия проверяет выполнение всех требований, указанных в настоящих Правилах, в т.ч. наличие указанных средств защиты информации, оформленных актов установки и настройки средств защиты информации (включая акт установки на АРМ СКЗИ, подписанный организацией-лицензиатом ФСБ России);

- комиссия оформляет акт оценки выполнения мероприятий по защите информации на АРМ участника информационного взаимодействия для подключения к РГИС ЕАФСО НО по форме, приведенной в приложении 1 к настоящим Правилам. Акт оценки подписывается всеми членами комиссии, утверждается председателем комиссии;

- участник информационного взаимодействия направляет официальным письмом в адрес оператора РГИС ЕАФСО НО копию акта оценки с письмом – подтверждением проведения необходимых мероприятий по форме, приведенной в приложении 2 к настоящим Правилам;

Оператор РГИС ЕАФСО НО вправе запросить у участника информационного взаимодействия копии документов, указанных в акте оценки.

5. **Активация учетной записи пользователя РГИС ЕАФСО НО**

После успешного подтверждения выполнения требований по защите информации, Оператор РГИС ЕАФСО НО активирует учетную запись пользователя РГИС ЕАФСО НО, зарегистрированную за пользователем подключаемого АРМ.

ПРИЛОЖЕНИЕ 1
к Правилам подключения участников
информационного взаимодействия
к региональной государственной
информационной системе «Единый агрегатор
физкультурно-спортивных организаций
Нижегородской области»

Форма акта оценки выполнения мероприятий по защите информации на АРМ Участника информационного взаимодействия для подключения к РГИС ЕАФСО НО

УТВЕРЖДАЮ

Должность

ФИО

_____
(подпись)

«_____» _____ 20 ___ г.

АКТ оценки выполнения мероприятий по защите информации в

_____

_____
(наименование участника информационного взаимодействия)

для подключения к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области»

Комиссия в составе:

Председатель комиссии:

_____
(должность) (ФИО)

Члены комиссии:

_____
(должность) (ФИО)

_____
(должность) (ФИО)

_____
(должность) (ФИО)

назначенная приказом от «_____» _____ 20 __ г. № ___, провела оценку выполнения мероприятий по защите информации для подключения к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области» (далее – РГИС ЕАФСО НО), организованного в:

_____

_____

(полное наименование участника информационного взаимодействия, ИНН)

Оценка мероприятий по защите информации проводилась на соответствие требованиям, изложенным в «Правилах подключения участников информационного взаимодействия к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области», утвержденных приказом министерства цифрового развития и связи Нижегородской области от «___» _____ 20 ___ г. № ___ (далее – Правила).

Таблица 1 – Сведения об АРМ

№ п/п	Наименование АРМ (например: АРМ отдела кадров)	Характеристики
1.	Инв. №, зав. № АРМ	
2.	Тип АРМ (сист. блок/ моноблок)	
3.	Операционная система (версия, билд (номер сборки)	
4.	Адрес расположения АРМ (населенный пункт, ул., д., этаж, № помещения, наименование помещения)	

Таблица 2 – Ответственные лица

№ п/п	Зона ответственности	Должность	ФИО	Телефон
1.	Ответственный за защиту информации, обрабатываемой с использованием АРМ			
2.	Ответственный за выявление инцидентов и реагирование на них			

Таблица 3 – Мероприятия по ограничению и контролю доступа в помещение, с расположенным АРМ

№ п/п	Наименование мероприятий	Статус реализации (ДА/ НЕТ/ Иное[1])	Дополнительные сведения
1.	Обеспечивается режим, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в помещения, где размещается АРМ		
2.	Правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях утверждены		
3.	Перечень лиц, имеющих право доступа в помещения утвержден		
4.	Помещение имеет прочную входную дверь с замком, гарантирующим надежное закрытие в нерабочее время		
5.	Окна помещений оборудованы металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения[2].		

[1] В случае выбора варианта ответа «Иное», необходимо описать реализацию в столбце «Дополнительные сведения».

[2] Указывается в случае если помещения расположены на первых и (или) последних этажах зданий, а также окна помещений, находятся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц.

Таблица 4 – Перечень средств защиты информации, отметка о установке

№ п/п	Тип СрЗИ	Наименование	Производитель	Версия	Сведения о сертификате соответствия (рег. №, № сертификата соответствия, действует до)	Кем установлено/ настроено СрЗИ (Организация, должность, ФИО)	№ лицензии ФСТЭК/ФСБ (на осуществление работ)[3]	Дата установки/ настройки СрЗИ	Акт установки/ настройки СрЗИ
1.	ОС (вариант подключения №2)								
2.	САВЗИ								
3.	СКЗИ								

[3] В случае привлечения организации – лицензиата ФСТЭК/ ФСБ

Таблица 5 – Перечень утвержденных организационно-распорядительных документов

№ п//п	Документ определяет	Реквизиты документа (название, дата утверждения, кем утвержден, реквизиты приказа об утверждении)
1.	Структурное подразделение или должностное лицо (работник), ответственное за защиту информации, обрабатываемой с использованием АРМ	
2.	Лицо, ответственное за выявление инцидентов и реагирование на них	
3.	Лицо, ответственное за планирование и контроль мероприятий по защите информации, обрабатываемой с использованием АРМ	
4.	Лица, которым разрешены действия по внесению изменений в конфигурацию АРМ и СрЗИ АРМ, и их полномочий	
5.	Лица, доступ которых к РГИС ЕАФСО НО необходим в целях выполнения должностных обязанностей	
6.	Лица, допущенные к работе с СКЗИ	
7.	Лица, допущенные в помещение, где размещен АРМ	
8.	Границы контролируемой зоны, в пределах которой постоянно размещается АРМ	
9.	Права и обязанности пользователя АРМ	
10.	Права и обязанности лиц, ответственных: – за защиту информации, обрабатываемой с использованием АРМ; – за выявление инцидентов и реагирование на них; – за планирование и контроль мероприятий по защите информации, обрабатываемой с использованием АРМ; – за внесение изменений в конфигурацию АРМ и СрЗИ АРМ.	
11.	Порядок администрирования и использования СрЗИ АРМ	
12.	Парольная политика при работе с АРМ	
13.	Правил доступа в помещение с размещенным АРМ в рабочее и нерабочее время, а также в нештатных ситуациях	
14.	Порядок учета машинных носителей информации	
15.	Порядок внесения изменений в конфигурацию АРМ и СрЗИ АРМ	
16.	Порядок обнаружения и реагирования на инциденты, которые могут привести к сбоям или нарушению функционирования АРМ и РГИС ЕАФСО НО и (или) к возникновению угроз безопасности информации	

ЗАКЛЮЧЕНИЕ КОМИССИИ

В результате оценки выполнения мероприятий по защите информации в

_____

(наименование участника информационного взаимодействия)

для подключения к РГИС ЕАФСО НО, комиссия установила, что:

1) АРМ находится в технически исправном состоянии;

2) на АРМ установлены и настроены средства защиты информации в соответствии с разделом 3 Правил (вариант подключения №__);

3) утвержден комплект ОРД для подключения к РГИС ЕАФСО НО в соответствии с разделом 3.7 Правил;

4) работники, допущенные работе на АРМ, ознакомлены с ОРД и с требованиями эксплуатационной документации на средства защиты информации, установленные на АРМ, под подпись. Уровень квалификации указанных лиц позволяет выполнять возложенные на них обязанности по обработке информации в РГИС ЕАФСО НО.

ВЫВОД

Мероприятия по защите информации на АРМ для подключения к РГИС ЕАФСО НО проведены и соответствуют требованиям Правил.

Комиссия в составе:

Председатель комиссии:

_____

(должность) (ФИО) (подпись)

Члены комиссии:

_____

(должность) (ФИО) (подпись)

_____

(должность) (ФИО) (подпись)

_____

(должность) (ФИО) (подпись)

ПРИЛОЖЕНИЕ 2
к Правилам подключения участников
информационного взаимодействия
к региональной государственной
информационной системе «Единый агрегатор
физкультурно-спортивных организаций
Нижегородской области»

(оформляется на официальном бланке Организации)

В адрес
государственного автономного учреждения
Нижегородской области
«Центр координации проектов цифровой экономики»

Заявка на подключение
к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области» (РГИС ЕАФСО НО)

от _____ № _____

Направляем информацию для подключения к РГИС ЕАФСО НО _____.
(указывается наименование Организации)

Автоматизированное рабочее место пользователя РГИС ЕАФСО НО по своему назначению и техническим характеристикам удовлетворяет требованиям, предъявляемым к подключению, указанным в Приложении №1 к «Правилам подключения участников информационного взаимодействия к региональной государственной информационной системе «Единый агрегатор физкультурно-спортивных организаций Нижегородской области», утвержденным приказом министерства цифрового развития и связи Нижегородской области от «___» _____ 20 ___ г. № ___, вариант подключения №____ (указать номер варианта подключения).

Приложение: копия акта оценки, на __ л.

Руководитель организации _____ _____
(ФИО) (Подпись)