**АГЕНТСТВО ПО РАЗВИТИЮ ЧЕЛОВЕЧЕСКОГО ПОТЕНЦИАЛА И ТРУДОВЫХ РЕСУРСОВ УЛЬЯНОВСКОЙ ОБЛАСТИ**

# Р А С П О Р Я Ж Е Н И Е

22 января 2026 года № 10-р

г. Ульяновск

## Об утверждении Порядка передачи информации из государственных информационных систем Агентства по развитию человеческого потенциала и трудовых ресурсов Ульяновской области в иные информационные системы

В целях совершенствования использования информационной инфраструктуры Агентства по развитию человеческого потенциала и трудовых ресурсов Ульяновской области:

Утвердить прилагаемый Порядок передачи информации из государственных информационных систем Агентства по развитию человеческого потенциала и трудовых ресурсов Ульяновской области в иные информационные системы.

Руководитель Агентства П.Н. Калашников

УТВЕРЖДЁН
распоряжением Агентства по
развитию человеческого
потенциала и трудовых
ресурсов Ульяновской области
от 22.01.2026 № 10-л

# ПОРЯДОК
## передачи информации из государственных информационных систем Агентства по развитию человеческого потенциала и трудовых ресурсов Ульяновской области в иные информационные системы

### 1. Общие положения

1.1. Настоящий Порядок устанавливает правила и процедуры передачи информации, содержащейся в государственных информационных системах (далее – ГИС) Агентства по развитию человеческого потенциала и трудовых ресурсов Ульяновской области (далее – Агентство, оператор ГИС), в иные информационные системы (далее – ИИС).

1.2. Порядок разработан в соответствии с положениями следующих нормативных правовых актов Российской Федерации:

-Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

-Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

-Иные нормативные правовые акты, регулирующие отношения в сфере обработки информации ограниченного доступа, её защиты, а также обеспечения информационной безопасности.

1.3. Передача информации из ГИС Агентства в ИИС запрещается в случае, если такая ИИС не соответствует установленным законодательством Российской Федерации требованиям о защите информации, предусмотренным частью 8.1 статьи 14 Федерального закона от 27 июля 2006 г. № 149-ФЗ. Ответственность за оценку соответствия принимающей ИИС указанным требованиям возлагается на оператора ГИС Агентства в соответствии с разделом 2 настоящего Порядка.

### 2. Реализация организационных мер

2.1. Обязательные документы:

1) соглашение о взаимодействии между оператором государственной информационной системы (ГИС) и оператором информационной системы организации (ИИС), содержащее раздел, регламентирующий порядок обеспечения защиты информации в процессе информационного взаимодействия;

2) распорядительный документ оператора о назначении лиц, ответственных за организацию и осуществление передачи информации ограниченного доступа;

3) внутренний организационно-распорядительный документ оператора, определяющий порядок (регламент) передачи информации, включая процедуры контроля её передачи, а также порядок выявления, регистрации и реагирования на инциденты информационной безопасности, связанные с передачей информации.

2.2. Обязанности оператора ГИС:

1) определить номенклатуру (состав) и цели передачи в ИИС информации ограниченного доступа;

2) установить требуемый уровень защищённости передаваемой информации в соответствии с законодательством Российской Федерации и действующими нормативными правовыми актами в области защиты информации;

3) осуществить оценку соответствия принимающей информационной системы (ИИС) следующим требованиям:

а) наличие действующего аттестата соответствия требованиям по защите информации или акта оценки соответствия требованиям по защите информации, оформленного в установленном порядке;

б) оснащённости сертифицированными в системе сертификации средств защиты информации (СЗИ), соответствующими установленному классу защищённости;

в) наличию и реализации комплекса организационных и технических мер защиты информации, адекватных уровню защищённости передаваемой информации.

2.3. Обязанности оператора ИИС:

1) обеспечить конфиденциальность полученной информации ограниченного доступа, исключив её разглашение и неправомерный доступ;

2) реализовать право на доступ к информации исключительно в пределах полномочий, предоставленных уполномоченным лицам;

3) предотвратить несанкционированный доступ (далее – НСД) к информации, а также её передачу (распространение) неуполномоченным физическим и/или юридическим лицам;

4) обеспечить своевременное обнаружение фактов НСД, уничтожения, модифицирования, блокирования, копирования информации;

5) предупреждать и минимизировать последствия нарушений установленного порядка доступа к информации;

6) исключить возможность несанкционированного воздействия на технические средства, приводящего к нарушению их функционирования;

7) обеспечить возможность восстановления информации, подвергшейся модификации или уничтожению, в установленные сроки;

8) осуществлять регулярный контроль уровня защищённости информации, включая проведение оценки защищённости:

а) с периодичностью не реже одного раза в три года;

б) в обязательном порядке после каждого инцидента информационной безопасности (компьютерного инцидента);

в) в порядке, предусмотренном внутренним регламентом оператора ИИС.

2.4. Требования к размещению и условиям хранения (обработки) информации:

1) информация, содержащая персональные данные граждан Российской Федерации, подлежит размещению (хранению) исключительно на территории Российской Федерации, что должно быть подтверждено соответствующими организационно-техническими решениями.

2) обеспечение физической защиты помещений и технологического оборудования, предназначенных для обработки указанной информации, включая:

а) систему контроля и управления доступом в помещения;

б) организацию охраны.

## 3. Реализация технических мер

3.1. Требования к защите каналов передачи данных:

1) передача информации по каналам связи должна осуществляться с обязательным применением средств криптографической защиты информации (СКЗИ), сертифицированных в соответствии с законодательством Российской Федерации и требованиями Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Эксплуатация СКЗИ должна проводиться в соответствии с их эксплуатационной документацией и утверждёнными регламентами;

2) при организации удалённого доступа к информационным ресурсам ГИС и ИИС доступ разрешается исключительно через сети связи общего пользования и (или) выделенные сети связи, технические средства которых размещены на территории Российской Федерации;

3) должна быть реализована процедура строгой аутентификации пользователей, обеспечивающая однозначную идентификацию и подтверждение подлинности субъекта доступа перед предоставлением прав на работу с информацией;

4) средства защиты информации (СЗИ), обеспечивающие безопасность каналов передачи данных, должны быть настроены (сконфигурированы) в соответствии с требованиями нормативной и эксплуатационной документации к используемому программному обеспечению (ПО) и программно-аппаратным комплексам.

3.2. Требования к управлению уязвимостями:

Организация и проведение мероприятий по управлению уязвимостями информационных систем, включающих в себя:

– выявление (идентификацию) уязвимостей программного обеспечения и конфигураций средств вычислительной техники;

– оценку критичности выявленных уязвимостей и связанных с ними рисков для безопасности информации;

– своевременное устранение (нейтрализацию) выявленных уязвимостей путём установки обновлений безопасности, полученных от производителей ПО, их последующего тестирования и применения в установленном порядке.

3.3. Требования к программно-аппаратной защите:

1) на всех узлах информационных систем должно быть установлено и функционировать антивирусное программное обеспечение отечественного производства. Необходимо обеспечить поддержание актуальности антивирусных баз и регулярное продление лицензий на использование данного ПО.

2) при назначении прав доступа должен неукоснительно соблюдаться принцип наименьших привилегий, согласно которому пользователям и процессам предоставляется минимальный набор прав, необходимый для выполнения возложенных на них законных функциональных задач.

3) для защиты от несанкционированного доступа (НСД) к информации должны применяться сертифицированные средства защиты информации от НСД.

4) на границах сетевого периметра информационных систем и между их сегментами должны быть установлены и корректно настроены межсетевые экраны (брандмауэры) отечественного производства, имеющие соответствующие сертификаты соответствия.

## 4. Контроль исполнения

4.1. Ответственность за соблюдение установленных настоящим Порядком требований возлагается:

- на оператора государственной информационной системы (ГИС) – в части организации, подготовки, проверки корректности и осуществления передачи информации, а также подтверждения соответствия принимающей стороны установленным требованиям.

- на оператора иной информационной системы (ИИС) – в части корректного приёма, обеспечения безопасного хранения, обработки и защиты переданной информации на протяжении всего её жизненного цикла в соответствии с целями передачи и условиями соглашения.

4.2. Оператор ИИС обязан обеспечить проведение ежемесячной проверки актуальности и действенности ключевой документации и компонентов СКЗИ, включая сертификаты ключей проверки электронной подписи, сертификаты удостоверяющих центров, а также сроков действия лицензий на использование криптосредств.

4.3. Порядок реагирования на инциденты информационной безопасности:

1) в случае выявления факта несанкционированного доступа (НСД), утечки информации или иного инцидента, угрожающего безопасности передаваемой информации, оператор ГИС обязан немедленно инициировать процедуру блокировки дальнейшей передачи данных в соответствующую ИИС;

2) об обнаруженном инциденте производится уведомление уполномоченных государственных органов в срок, не превышающий 24 (двадцати четырёх) часов с момента его обнаружения, в соответствии с установленными данными органами форматами и регламентами;

3) расследование причин и последствий инцидента осуществляется с обязательным участием сотрудников отдела информационной безопасности или иного ответственного структурного подразделения (уполномоченного

специалиста по информационной безопасности) оператора, в системе которого произошёл инцидент, с составлением соответствующего акта.

## 5. Заключительные положения

5.1. Действие настоящего Порядка подлежит прекращению или приостановлению в следующих случаях:

1) при вступлении в силу изменений в законодательство Российской Федерации, требующих пересмотра установленных настоящим документом процедур и регламентов;

2) в случае утраты юридической силы (отзыва) аттестата соответствия требованиям по защите информации или акта оценки соответствия, выданного в отношении принимающей ИИС, а также при выявлении несоответствия уровня её защищённости установленным на момент передачи информации требованиям.

3) в случае прекращения действия Соглашения о взаимодействии между оператором ГИС и оператором ИИС.