ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 28. 10. 2021 № 1371

г. Курган

Об утверждении регламента информационного взаимодействия внешних информационных систем персональных данных с информационными системами Департамента образования и науки Курганской области

В соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» ПРИКАЗЫВАЮ:

1. Утвердить регламент информационного взаимодействия внешних информационных систем персональных данных с информационными системами Департамента образования и науки Курганской области (приложение).

2. Контроль за исполнением настоящего приказа возложить на заместителя директора Департамента образования и науки Курганской области Хлебникова И.Н.

Директор Департамента образования и науки Курганской области А.Б. Кочеров

Моторин Григорий Павлович
8(3522)462829

УТВЕРЖДАЮ
Директор
Департамента образования и науки
Курганской области

_____ А.Б. Кочеров

м.п.

«28» октября 2021 г.

РЕГЛАМЕНТ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

внешних информационных систем персональных данных с информационными системами Департамента образования и науки Курганской области

2021

Перечень используемых сокращений

Участники взаимодействия	Организации, осуществляющие деятельность в сфере образования на территории Курганской области
Департамент	Департамент образования и науки Курганской области
Регламент	Настоящий Регламент информационного взаимодействия внешних информационных систем персональных данных с информационными системами Департамента образования и науки Курганской области
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ФСБ России	Федеральная служба безопасности Российской Федерации
ИСПДн	Информационные системы персональных данных участников взаимодействия
ЗСПД	Защищенная сеть передачи данных
ПДн	Персональные данные
СЗИ	Средства защиты информации
ОС	Операционная система
АРМ	Автоматизированные рабочие места
ПО	Программное обеспечение
СКЗИ	Средства криптографической защиты информации
Спецпомещение	Помещения, где установлены средства криптографической защиты информации из состава информационных систем персональных данных и хранятся ключевые документы к ним
СЗПДн	Система защиты персональных данных

История изменений документа

Версия	Дата	Изменения
1.0	26.10.2021	Создание документа

1 Общие положения

1.1 Настоящий регламент (далее – Регламент) устанавливает перечень требований к информационным системам персональных данных (далее – ИСПДн), функционирующим на территории Курганской области в организациях сферы образования (далее – участники взаимодействия), и определяет порядок их подключения к информационными системам Департамента образования и науки Курганской области (далее – Департамент) с целью безопасного обмена информацией и документами.

1.2 Регламент разработан согласно действующим нормативно правовым актам, методическим документам и национальным стандартам в области защиты информации:

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

[2] Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

[3] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

[4] Постановление Правительства Курганской области от 8 сентября 2015 г. № 285 «О защищенной сети передачи данных Правительства Курганской области»

[5] Приказ ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

[6] Приказ ФСТЭК России № 77 от 29 апреля 2021 г. «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

[7] Приказ ФСТЭК России № 55 от 3 апреля 2018 г. «Положение о системе сертификации средств защиты информации»;

[8] Приказ ФСБ России от 10 июля 2014 г. № 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»;

[9] Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

[10] ГОСТ Р 51583. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;

[11] ГОСТ Р 51624. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

1.3 Департамент является оператором региональных информационных систем, обрабатывающим персональные денные (далее – ПДн), доступ к которым осуществляется посредством защищенной сети передачи данных (далее – ЗСПД) ViPNet № 3335 Правительства Курганской области.

1.4 Согласно постановлению [4] ЗСПД является защищенной виртуальной сетью, созданной для обеспечения взаимодействия информационных систем органов исполнительной власти Курганской области, органов местного самоуправления муниципальных образований Курганской области, подведомственных им государственных и муниципальных учреждений через единое защищенное информационное пространство. Посредством ЗСПД ViPNet № 3335 участники взаимодействия также могут получить доступ к сторонним информационным системам, функционирующим на территории Курганской области, операторами которых являются иные органы власти и учреждения, в частности:

- «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» Федеральной службы по надзору в сфере образования и науки;
- «Единый социальный регистр населения» Главного управления социальной защиты населения Курганской области;
- «Навигатор дополнительного образования детей Курганской области» Государственного автономного нетипового образовательного учреждения Курганской области «Центр развития современных компетенций»;
- «Региональная система учета государственных и муниципальных платежей» Финансового управления Курганской области».

1.5 Участники взаимодействия при организации информационного взаимодействия с информационными системами Департамента в обязательном порядке должны выполнить организационные и технические меры по защите ПДн, предусмотренные Регламентом.

1.6 Для выполнения работ по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридические лица или индивидуальные предприниматели, имеющие лицензию на деятельность по технической защите конфиденциальной информации ФСТЭК России и лицензию ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

2 Порядок подключения участников взаимодействия

2.1 Организация информационного взаимодействия ИСПДн участников взаимодействия с информационными системами Департамента проводится в соответствии с порядком подключения участников взаимодействия, включающего следующий перечень работ и мероприятий:

1) подготовка технического и программного обеспечения ИСПДн в соответствии с требованиями, приведенными в п. 3.1 Регламента;

2) выполнение мероприятий по защите ПДн в соответствии с требованиями, приведенными в п. 3.2 Регламента, а также получение парольно-ключевой информации на средства ЗСПД ViPNet № 3335 у Департамента информационных технологий и цифрового развития Курганской области, являющегося оператором ЗСПД;

3) направление уведомления на адрес электронной почты Департамента don@kurganobl.ru о выполнении требований Регламента по форме, приведенной в Приложении к Регламенту;

4) получение доступа к ресурсам информационных систем Департамента в порядке, установленном Департаментом;

5) поддержание уровня защищенности ПДн в ходе эксплуатации ИСПДн в соответствии с требованиями, приведенными в п 3.3 Регламента.

2.2 Схема информационного взаимодействия ИСПДн участников взаимодействия с информационными системами Департамента приведена на рисунке 1.

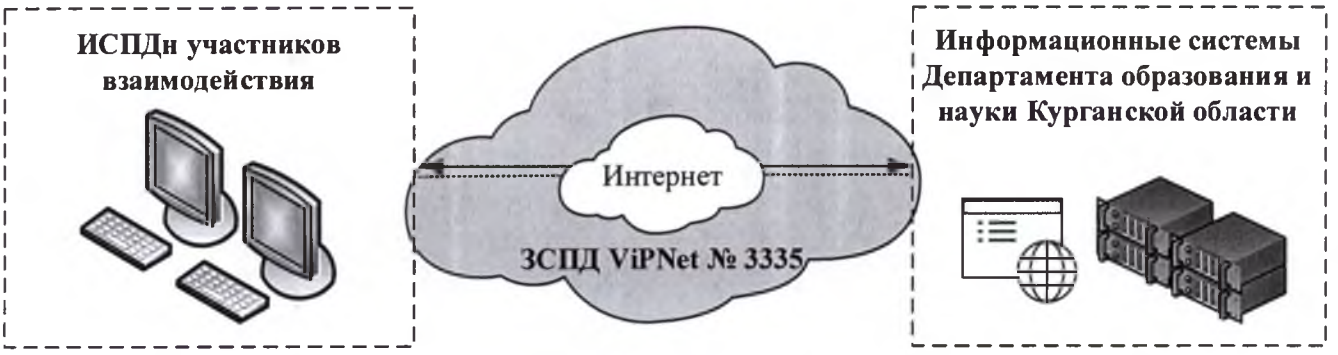

Рисунок 1 – Схема информационного взаимодействия

3 Требования к ИСПДн участников взаимодействия

3.1 Требования к техническому и программному обеспечению

3.1.1 Программные, программно-технические средства и средства защиты информации (далее – СЗИ), входящие в состав ИСПДн участников взаимодействия, должны быть полностью исправны и принадлежать участникам взаимодействия на любом законном основании.

3.1.2 Не допускается использование устаревших и не поддерживаемых производителями операционных систем (далее – ОС), в частности Windows XP, Windows Vista, Windows 7.

3.1.3 Автоматизированные рабочие места (далее – АРМ) должны соответствовать минимальным техническим требованиям:

- процессор:
  - 64-битная архитектура (x64);
  - количество ядер ≥ 2 шт.;
  - количество потоков ≥ 4 шт.;
  - базовая частота ≥ 1.8 ГГц.
- оперативная память:
  - объем ≥ 4 Гб;
  - частота ≥ 2133 МГц.
- накопитель HDD/SSD объемом ≥ 120 Гб;
- наличие порта Gigabit Ethernet 8P8C (RJ-45);
- ОС Windows 10 Pro x64 либо ОС семейства Linux* из Единого реестра российских программ для электронных вычислительных машин и баз данных.

  ** При использовании ОС семейства Linux возможны проблемы совместимости и ограничения функциональных возможностей в работе средств системы*

Внимание! *Выбор «устаревших» и «слабых» АРМ ведет к невозможности обеспечения стабильной работы ИСПДн и принятия необходимых мер защиты информации, вследствие чего могут возникнуть дополнительные финансовые издержки*

3.1.4 Для стабильной работы рекомендуется использовать АРМ, соответствующие следующим техническим требованиям:

- процессор Intel Core i3/i5, либо AMD Ryzen 3/5;
- оперативная память DDR4 объемом 8 Гб с частотой 2400 – 3200 МГц;
- SSD объемом 120 – 480 Гб;
- наличие порта Gigabit Ethernet 8P8C (RJ-45);
- ОС Windows 10 Pro x64.

3.1.5 На АРМ должно использоваться только лицензионное программное обеспечение (далее – ПО), установлены критические обновления безопасности.

3.1.6 На АРМ не должно быть установлено и использоваться ПО, цели функционирования которого заведомо не соответствуют целям функционирования ИСПДн. Например, приложения социальных сетей и игры.

3.2 Требования к защите ПДн

3.2.1 Участники взаимодействия должны выполнить организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с требованиями по защите ПДн [5], [8] для установленного уровня защищенности ПДн, определенного согласно требованиям [3].

3.2.2 При выполнении организационных мер защиты ПДн участниками взаимодействия должны быть назначены в установленном порядке ответственные лица:

– за организацию обработки ПДн в ИСПДн;

– за обеспечение безопасности ПДн (администратор безопасности) в ходе создания, ввода в эксплуатацию и эксплуатации ИСПДн и её системы защиты;

– за поддержание функционирования ИСПДн в установленном штатном режиме работы (администратор системы);

– за эксплуатацию помещений, где установлены средства криптографической защиты информации (далее – СКЗИ) из состава ИСПДн и хранятся ключевые документы к ним (далее – спецпомещения).

3.2.3 Назначенные ответственные лица должны знать документы по защите информации участников взаимодействия и обладать достаточным уровнем знаний для выполнения требований по защите ПДн при их обработке в ИСПДн.

3.2.4 Создание системы защиты персональных данных (далее – СЗПДн) для ИСПДн должно осуществляться с учетом государственных стандартов [10], [11] и предусматривать следующий комплекс работ:

1) формирование требование к СЗПДн;
2) разработка СЗПДн;
3) внедрение СЗПДн;
4) оценка эффективности (аттестация) ИСПДн на соответствие требованиям по защите информации;
5) сопровождение СЗПДн в ходе эксплуатации ИСПДн.

3.2.5 Выбор СЗИ для реализации технических мер защиты ПДн должен осуществляться при создании СЗПДн для ИСПДн, при этом СЗИ должны выбираться с учетом их стоимости, совместимости с техническими средствами и структурно-функциональными особенностями функционирования ИСПДн.

3.2.6 Для реализации функций СЗПДн рекомендуется использовать сертифицированные ФСТЭК и (или) ФСБ России СЗИ, а именно:

– защиты канала связи сети ViPNet № 3335:
  – СКЗИ «Программный комплекс ViPNet Client 4»;
  – СКЗИ «Программно-аппаратный комплекс ViPNet Coordinator HW 4».
– защиты от несанкционированного доступа;
– межсетевого экранирования;
– антивирусной защиты.

3.2.7 При использовании СКЗИ участники взаимодействия в соответствии с требованиями [8] обеспечивают:

– организацию режима обеспечения безопасности спецпомещений, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения в соответствии с п.6 требований [8];

– сохранность носителей ПДн в соответствии с п.7 требований [8];

– определение лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей в соответствии с п.8 требований [8];

– использование СКЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в

случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, в соответствии с п.9 требований [8].

3.2.8 По результатам внедрения СЗПДн участники взаимодействия организуют проведение оценки эффективности (аттестации) ИСПДн на соответствие требованиям по защите ПДн [5] согласно порядку [6].

3.3 Требования к эксплуатации

3.3.1 Участники взаимодействия в ходе эксплуатации ИСПДн обеспечивают поддержку их безопасности в соответствии с условиями, установленными в документах по защите информации и документах по оценке эффективности (аттестации) ИСПДн, а также проводят периодический контроль уровня защищенности ПДн.

3.3.2 При эксплуатации ИСПДн участники взаимодействия осуществляют своевременное продление применяемых СЗИ и СКЗИ в рамках реализации СЗПДн, а также вносят соответствующие отметки в эксплуатационную документацию.

3.3.3 В случае развития (модернизации) ИСПДн, в ходе которого изменяется конфигурация (параметры настройки) программных, программно-технических средств и СЗИ, исключены программные, программно-технические средства и СЗИ, дополнительно включены аналогичные средства или заменены на аналогичные средства проводятся дополнительные испытания в соответствии с порядком [6]. Сведения об изменениях ИСПДн и проведенных при этом испытаниях включаются в технический паспорт.

3.3.4 В случае развития (модернизации) ИСПДн, приводящего к повышению уровня защищенности ПДн и (или) к изменению архитектуры СЗПДн в части изменения видов и типов программных, программно-технических средств и СЗИ, изменения структуры СЗПДн, состава и мест расположения ИСПДн и её компонентов, проводится повторная оценка эффективности (аттестация) ИСПДн на соответствие требованиям по защите ПДн [5] согласно порядку [6].

3.3.5 При эксплуатации ИСПДн не допускается:

- вносить несанкционированные изменения в конфигурацию программных, программно-технических средств, СЗИ;
- осуществлять несанкционированную замену программных, программно-технических средств, СЗИ на аналогичные средства;
- проводить обработку информации в случае обнаружения неисправностей в СЗПДн;
- проводить обработку информации в случае обнаружения инцидента безопасности.

4 Заключительные положения

4.1 Уполномоченные лица (руководители) участников взаимодействия обеспечивают принятие необходимых мер, направленных на выполнение требований Регламента.

4.2 Ответственность за выполнение требований по защите ПДн в ходе эксплуатации ИСПДн участников взаимодействия лежит исключительно на участниках взаимодействия.

4.3 Ответственные лица участников взаимодействия при нарушении закона о защите ПДн [2] и иных нормативно-правовых актов, приведенных в п. 1.2 Регламента, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном законодательством Российской Федерации.

4.4 В случае нарушения участниками взаимодействия требований Регламента, а также законодательства Российской Федерации по защите ПДн и установленного порядка эксплуатации СКЗИ, Департамент имеет право в одностороннем порядке ограничить доступ (отключить) таких участников взаимодействия от информационных систем Департамента и ЗСПД. При этом, участники взаимодействия не освобождаются от выполнения возложенных на них задач, связанных с необходимостью обмена информацией и документами, в связи с чем они самостоятельно изыскивают иные законные способы и средства обмена информацией и документами, в том числе без использования средств автоматизации.

Приложение.

Форма уведомления

(на официальном бланке участника взаимодействия)

Директору
Департамента образования и
науки Курганской области
Кочерову А.Б.
don@kurganobl.ru

Об информационном взаимодействии

Уважаемый Андрей Борисович!

[Участник взаимодействия] (далее – участник взаимодействия) сообщает о выполнении требований Регламента информационного взаимодействия внешних информационных систем персональных данных (далее – ИСПДн) с информационными системами Департамента образования и науки Курганской области (далее – Департамент) и подтверждает выполнение требований по защите персональных данных при их обработке в ИСПДн в соответствии с действующим законодательством Российской Федерации.

Сведения об ИСПДн участника взаимодействия:

Наименование ИСПДн	*«Ведение образовательной деятельности»*
Реквизиты документа, подтверждающего выполнение требований по защите ПДн при их обработке в ИСПДн	*Аттестат соответствия требованиям по защите информации №XXXX.XXXXX.XXXX выдан «__» ____202_г.*
Ответственное лицо за организацию обработки ПДн в ИСПДн	*Директор Иванова Лидия Ивановна*
Количество автоматизированных рабочих мест, входящих в состав ИСПДн	*1 (одно)*
Применяемые средства защиты каналов связи сети ViPNet № 3335	*Программный комплекс ViPNet Client 4*
Наименование информационных систем Департамента, с которыми необходимо обеспечить взаимодействие	*Мониторинг образования Курганской области», «Государственная итоговая аттестация»*

Участник взаимодействия гарантирует принятие необходимых мер по обеспечению защиты ПДн в ходе эксплуатации ИСПДн, в том числе своевременное продление применяемых средств защиты информации.

(наименование должности руководителя участника взаимодействия)	*(подпись)*	*(инициалы, фамилия)*