



**АДМИНИСТРАЦИЯ ГОРОДА КОВРОВА
ВЛАДИМИРСКОЙ ОБЛАСТИ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ**

П Р И К А З

«30» мая 2023 г.

Ковров

№ 394

**О назначении администраторов информационной безопасности в
управлении образования администрации города Коврова**

В соответствии с пп.1 п.1 ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в целях создания и поддержания необходимо уровня безопасности информации и в связи с кадровыми изменения в управлении образования администрации города Коврова (далее – управление образования) **приказываю:**

1. Назначить ответственными администраторами информационной безопасности (далее - АИБ):

1.1. _____, заместителя начальника, начальника отдела организационной и кадровой работы управления образования;

1.2. _____ методиста информационно-методического центра при управлении образования;

1.3. _____, ведущего инженера – системного администратора информационно-методического центра при управлении образования.

2. Утвердить обязанности АИБ управления образования для следующих работников:

2.1. _____

– знать действующие законодательные акты в области защиты информации и ПДн и положения внутренней организационно-распорядительной документации управления образования;

– проводить мониторинг и анализ законодательной базы Российской Федерации в области защиты информации и ПДн и информационной безопасности в целом;

– создавать новые и редактировать уже существующие внутренние документы по защите информации и ПДн, на основании анализа законодательной базы;

– изучать все стороны деятельности управления образования и выработать рекомендации по организации обработки ПДн при решении следующих основных вопросов:

- организация доступа к ПДн и учет сотрудников управления образования, допущенных к обработке ПДн, как в программных комплексах, так и на бумажных носителях;
- контроль поддержания в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;
- контроль обеспечения соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
- организация работы по заключению договоров на работы по защите ПДн;
- контроль изменений в процессах обработки ПДн и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных (Роскомнадзор) с целью актуализации уведомления управления образования в реестре операторов ПДн;
- подготовка предложений по совершенствованию действующей системы защиты ПДн;
- знать цели обработки ПДн в управлении образования и перечень обрабатываемых ПДн;
- периодически представлять руководству отчеты о состоянии защиты информационных систем и о нештатных ситуациях на объектах информационных систем и допущенных пользователями нарушениях установленных требований по защите информации и ПДн;
- разрабатывать планы мероприятий по обеспечению безопасности информации управления образования; обеспечивать выполнение мероприятий плана;
- участвовать в расследовании нарушений по вопросам защиты ПДн, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;
- обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно действующему законодательству.

2.2.

- знать действующие законодательные акты в области защиты информации и ПДн и положения внутренней организационно-распорядительной документации управления образования;
- проводить мониторинг и анализ законодательной базы Российской Федерации в области защиты информации и ПДн и информационной безопасности в целом;
- создавать новые и редактировать уже существующие внутренние документы по защите информации и ПДн, на основании анализа законодательной базы;
- изучать все стороны деятельности управления образования и выработать рекомендации по организации обработки ПДн при решении следующих основных вопросов:

- организация доступа к ПДн и учет сотрудников управления образования, допущенных к обработке ПДн, как в программных комплексах, так и на бумажных носителях;
- контроль поддержания в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;
- контроль обеспечения соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
- организация работы по заключению договоров на работы по защите ПДн;
- контроль изменений в процессах обработки ПДн и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных (Роскомнадзор) с целью актуализации уведомления управления образования в реестре операторов ПДн;
- подготовка предложений по совершенствованию действующей системы защиты ПДн;
- знать цели обработки ПДн в управлении образования и перечень обрабатываемых ПДн;
- вести учетные Журналы и хранить организационно-распорядительную документацию управления образования в отведенном для этого месте;
- осуществлять инструктаж сотрудников управления образования, занимающихся обработкой информации и ПДн в информационных системах, по вопросам обеспечения безопасности и работе с информацией и ПДн;
- создавать новые и редактировать уже существующие внутренние документы по защите информации и ПДн, на основании анализа законодательной базы;
- разрабатывать планы мероприятий по обеспечению безопасности информации управления образования; обеспечивать выполнение мероприятий плана;
- осуществлять периодические проверки соблюдения пользователями информационных систем установленных в организации норм безопасности информации и ПДн и вести Журнал учета мероприятий по контролю над соблюдением режима защиты ПДн (совместно с Мельниковым А.А.);
- участвовать в расследовании нарушений по вопросам защиты ПДн, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;

2.3.

- участвовать в установке и настройке средств защиты, в контрольных и тестовых испытаниях и проверках элементов информационных систем и вести Журнал учета средств защиты информации и эксплуатационной документации;
- участвовать в приемке новых программных;
- обеспечивать доступ к защищаемой информации и ПДн пользователям информационных систем согласно их правам, в соответствии с Разрешительной системой (матрицей) доступа к ПДн, обрабатываемым в управлении образования;
- осуществлять резервное копирование баз данных с информацией и ПДн, а также программного обеспечения и вести Журнал учета процедур резервного копирования;

- анализировать состояния системы защиты информационных систем и ее отдельных подсистем;
 - контролировать неизменность состояния средств защиты их параметров и режимов защиты;
 - контролировать физическую сохранность средств и оборудования информационных систем;
 - обеспечивать своевременный анализ журналов учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;
 - оказывать помощь пользователям информационных систем в части применения средств защиты и консультировать по вопросам введенного режима защиты;
 - периодически представлять руководству отчеты о состоянии защиты информационных систем и о нештатных ситуациях на объектах информационных систем и допущенных пользователями нарушениях установленных требований по защите информации и ПДн;
 - подготовка предложений по совершенствованию действующей системы защиты ПДн;
 - в случае отказа работоспособности технических средств и программного обеспечения информационных систем, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;
 - участвовать в расследовании нарушений по вопросам защиты ПДн, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;
 - обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно действующему законодательству;
 - принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий (совместно с ведущими инженерами информационно-методического центра при управлении образования).
3. Утвердить права и ответственность АИБ управления образования:
- 3.1. АИБ управления образования имеют право:
- на выделение необходимого количества рабочего времени для выполнения функций, указанных в п.2. настоящего приказа;
 - беспрепятственного доступа ко всем элементам ИС;
 - знакомиться со всеми документами и материалами, необходимыми для выполнения возложенных задач;
 - проводить проверки соблюдения режима обеспечения безопасности информации и ПДн данных управления образования;
 - требовать от сотрудников управления образования соблюдения требования действующего законодательства и локальных актов управления образования по вопросам защиты информации и ПДн;
 - сообщать начальнику Управления об отказе того или иного пользователя ИС пройти проверку его знаний.

3.2. Ответственность за неисполнение обязанностей АИБ.

АИБ должен понимать в полной мере ответственность, возложенную на него, так как именно его действия влияют на достаточность устанавливаемых норм безопасности информации и ПДн Управления.

При не выполнении своих функций или халатном отношении к своим функциям, АИБ может спровоцировать реальную угрозу утечки информации и ПДн, что повлечет за собой ущерб для Управления, выражающийся в штрафных санкциях, административной и уголовной ответственности.

За ненадлежащее исполнение своих функций к АИБу могут быть применены административные санкции в соответствии с действующим законодательством.

4. В своей работе по выполнению функций АИБ руководствоваться документами:

- обязанностями АИБ, утвержденными п. 2 настоящего приказа;
- организационно- распорядительными документами по защите информации управления образования;
- законодательными актами Российской Федерации в области защиты информации и персональных данных;
- нормативными документами ФСТЭК России по защите информации и персональных данных.

5. Консультанту отдела организационной и кадровой работы управления образования Курловой Ю.В. внести дополнение в должностные инструкции вышеуказанных работников.

6. Признать утратившим силу приказ управления образования от 11.11.2022 № 733 «О назначении администраторов информационной безопасности в управлении образования администрации города Коврова».

7. Контроль исполнения приказа оставляю за собой.

8. Приказ вступает в силу со дня его подписания.

Начальник управления



С.Г. Павлюк