

ПРИКАЗ №7

О назначении Администратора безопасности информационных систем
персональных данных ООО «Цифровые решения «Айдиком»»

г. Набережные Челны

5 мая 2026

В целях выполнения требований законодательства, в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», приказываю:

1. Назначить Администратором безопасности информационных систем персональных данных ООО «Цифровые решения «Айдиком»» Генерального директора Шакирова И.Ф.

2. Администратору безопасности информационных систем персональных данных обеспечить ознакомление работников Общества, допущенных к обработке персональных данных, с настоящим Приказом под подпись.

3. Утвердить Инструкцию Администратора безопасности информационных систем персональных данных ООО «Цифровые решения «Айдиком»» (приложение № 1 к настоящему приказу).

4. Контроль за исполнением настоящего Приказа оставляю за собой.

Генеральный директор



И.Ф. Шакиров



Инструкция Администратора безопасности информационных систем
персональных данных ООО «Цифровые решения «Айдиком»»

1. Общие положения.

1.1. Администратор безопасности информационных систем персональных данных ООО «Цифровые решения «Айдиком»» (далее – Администратор безопасности ИСПДн) назначается приказом ООО «Цифровые решения «Айдиком»» (далее – Общество) и отвечает за обеспечение соблюдения требований законодательства в области защиты персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Общества.

1.2. Администратор безопасности ИСПДн должен знать нормы действующего законодательства Российской Федерации в области обработки и обеспечения безопасности ПДн.

1.3. В своей деятельности Администратор безопасности ИСПДн руководствуется нормами действующего законодательства РФ, Политикой Общества и настоящей Инструкцией.

2. Основные функции и обязанности.

Функции Администратора безопасности ИСПДн:

2.1. Администратор безопасности ИСПДн анализирует процессы обработки ПДн в информационных системах персональных данных (ИСПДн) Общества и вырабатывает рекомендации по их защите при решении следующих основных вопросов:

- проведение аналитической работы по комплексной защите и предупреждению утечки ПДн из ИСПДн;
- подготовка решений в отношении сведений о работах, выполняемых Обществом, подлежащих защите;
- контроль за внедрением и эксплуатацией систем защиты информации, обрабатываемой техническими средствами;
- проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки ПДн;
- подготовка предложений по совершенствованию действующей системы защиты ПДн в ИСПДн;
- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей ПДн;
- осуществления в пределах своей компетенции иных функций в соответствии с целями и задачами Общества.

Администратор безопасности ИСПДн обязан:

2.2. Соблюдать требования действующего законодательства Российской Федерации в области обработки и обеспечения безопасности ПДн.

2.3. Знать состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн в ИСПДн.

2.4. Осуществлять общий контроль за техническим сопровождением ИСПДн:

- контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;

- контролировать использование съёмных машинных носителей информации, в том числе запрещать использование неучтённых носителей информации;

- проводить инструктаж для работников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Общества (далее – Пользователи ИСПДн) по вопросам защиты ПДн.

2.5. Осуществлять контроль над настройкой и сопровождением подсистемы регистрации и учёта ИСПДн:

- согласовывать реализацию полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утверждённого списка лиц, допущенных к работе в ИСПДн;

- контролировать надёжность и частоту смены паролей доступа;

- контролировать своевременное ограничение или удаление учётной записи Пользователя ИСПДн при увольнении или переводе работника;

- регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа (далее – НСД) к ИСПДн;

- фиксировать факты попыток несанкционированного доступа или инцидентов информационной безопасности в Журнале регистрации выявленных нарушений в сфере защиты персональных данных и иной конфиденциальной информации (далее – Журнал учета инцидентов);

- согласовывать список лиц, допущенных к работе в ИСПДн.

2.6. Контролировать сопровождение подсистемы обеспечения целостности рабочего программного обеспечения ИСПДн:

- контролировать регулярное и своевременное обновление средств антивирусной защиты Общества;

- контролировать регулярное и своевременное создание резервных копий ИСПДн Общества;

- контролировать настройку и сопровождение систем защиты от НСД в ИСПДн.

2.7. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследований фактов НСД.

2.8. Участвовать при проведении внутреннего контроля соответствия обработки и защиты ПДн.

2.9. Контролировать выполнение Пользователями ИСПДн, установленных в ООО «Цифровые решения «АйдиКом»» требований по обеспечению безопасности ПДн.

2.10. В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своей компетенции.

2.11. Контролировать функционирование и работоспособность средств антивирусной защиты на автоматизированных рабочих местах ИСПДн.

2.12. Организовывать расследования попыток НСД и ИСПДн.

3. Права.

Администратор безопасности ИСПДн имеет право:

3.1. Знакомится с локальными актами Общества, регламентирующими процессы обработки и защиты ПДн.

3.2. Вносить предложения по совершенствованию существующей системы защиты информации.

3.3. При необходимости привлекать специализированные организации или квалифицированных специалистов на основании гражданско-правовых договоров для оказания услуг по защите информации.

3.4. Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных ООО «Цифровые решения «АйдиКом»», а также соблюдения требований действующего законодательства Российской Федерации в области обработки и защиты ПДн.

3.5. Участвовать в работе по совершенствованию мероприятий, направленных на обеспечение безопасности ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн.

4. Ответственность.

Администратор безопасности ИСПДн несёт ответственность за:

4.1. Несоблюдение требований локальных актов Общества и законодательства РФ в области защиты ПДн.

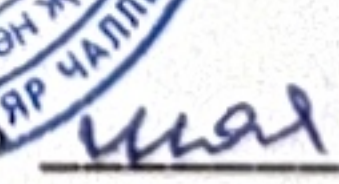
4.2. Разглашение ПДн в пределах, установленных действующим законодательством Российской Федерации.

Генеральный директор



И.Ф. Шакиров

С Положением (Инструкцией) ознакомлен, правила и процедуры понятны, обязуюсь исполнять.

Генеральный директор  /И.Ф. Шакиров/  2026 г.

