



МАУ ДО «СШ № 10», 423803, г. Набережные Челны, улица им. Комарова, дом 23
тел./факс: (8552) 49-36-23; ИНН 1650081908,
Отделение-НБ РТ банка России/УФК по РТ г. Казань, р/с 03234643927300001100
ЛАГ 30800125-ДЮСШ10 (бюджет) ЛАВ 30800126-ДЮСШ10 (вне бюджет) БИК(Казань) 019205400

ПРИКАЗ

от 17 июня 2026 г.

№ 105

О назначении ответственного за обеспечение безопасности ПДн в ИСПДн

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

ПРИКАЗЫВАЮ:

1. Ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных МАУ ДО "СШ №10" назначается и.о. заместителя директора Самохвалова И.А...
2. Утвердить Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МАУ ДО "СШ №10".
3. Самохвалова И.А обеспечивает:
 - соблюдение требований законодательства Российской Федерации в области персональных данных при их обработке в информационных системах персональных данных;
 - выполнение требований по защите персональных данных в соответствии с установленным уровнем защищённости УЗ-3;
 - контроль за обеспечением конфиденциальности персональных данных;
 - взаимодействие с уполномоченным органом по защите прав субъектов персональных данных при проведении мероприятий по контролю.
4. Самохвалова И.А несёт персональную ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.
5. Канунниковой М.Е. довести содержание настоящего приказа до сведения работников МАУ ДО "СШ №10", непосредственно осуществляющих обработку персональных данных.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор:

С приказом ознакомлены:



О.В.Зайнеева

И.А.Самохвалова
М.Е.Канунникова



УТВЕРЖДЕНА

ПРИКАЗОМ

МАУ ДО "СШ №10"

от «17» июня 2026 г. № 105

ИНСТРУКЦИЯ

ответственного за обеспечение безопасности ПДн в ИСПДн

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее — ИСПДн) МАУ ДО "СШ №10" (далее — Организация).

1.2. Инструкция разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Составы 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 защищённости»;
- иными нормативными правовыми актами Российской Федерации в области персональных данных и защиты информации.

1.3. Ответственным за обеспечение безопасности персональных данных в ИСПДн Организации является заместитель директора (далее — Ответственный за безопасность ПДн).

1.4. Ответственный за безопасность ПДн назначается приказом Директора Организации и подчиняется непосредственно Директору Организации.

1.5. Ответственный за безопасность ПДн в своей деятельности руководствуется законодательством Российской Федерации в области персональных данных и защиты информации, локальными нормативными актами Организации и настоящей Инструкцией.

1.6. Для ИСПДн Организации установлен УЗ-3.

1.7. Требования настоящей Инструкции являются обязательными для исполнения лицом, назначенным ответственным за обеспечение безопасности персональных данных в ИСПДн Организации.

ИНСТРУКЦИЯ **ответственного за обеспечение безопасности ПДн в ИСПДн**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее — ИСПДн) МАУ ДО "СШ №10" (далее — Организация).

1.2. Инструкция разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Составы 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 защищённости»;
- иными нормативными правовыми актами Российской Федерации в области персональных данных и защиты информации.

1.3. Ответственным за обеспечение безопасности персональных данных в ИСПДн Организации является заместитель директора (далее — Ответственный за безопасность ПДн).

1.4. Ответственный за безопасность ПДн назначается приказом Директора Организации и подчиняется непосредственно Директору Организации.

1.5. Ответственный за безопасность ПДн в своей деятельности руководствуется законодательством Российской Федерации в области персональных данных и защиты информации, локальными нормативными актами Организации и настоящей Инструкцией.

1.6. Для ИСПДн Организации установлен УЗ-3.

1.7. Требования настоящей Инструкции являются обязательными для исполнения лицом, назначенным ответственным за обеспечение безопасности персональных данных в ИСПДн Организации.

2. ЗАДАЧИ

2.1. Основными задачами Ответственного за безопасность ПДн являются:

- обеспечение безопасности персональных данных при их обработке в ИСПДн Организации в соответствии с требованиями законодательства Российской Федерации;
- планирование и реализация организационных и технических мер по обеспечению безопасности персональных данных в ИСПДн;
- организация применения средств защиты информации в ИСПДн и контроль за соблюдением условий их использования, предусмотренных эксплуатационной и технической документацией;
- контроль за выполнением работниками Организации требований по обеспечению безопасности персональных данных при их обработке в ИСПДн;
- предотвращение несанкционированного доступа к персональным данным, обрабатываемым в ИСПДн;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по реагированию на инциденты информационной безопасности;
- обеспечение функционирования средств криптографической защиты информации (СКЗИ) в соответствии с условиями сертификатов и эксплуатационной документацией;
- поддержание уровня защищённости персональных данных в ИСПДн на уровне не ниже УЗ-3.

3. ФУНКЦИИ И ОБЯЗАННОСТИ

3.1. Ответственный за безопасность ПДн выполняет следующие функции и обязанности.

В части планирования и организации защиты:

3.2. Разрабатывает и представляет на утверждение Директору Организации проекты организационно-распорядительных документов, регламентирующих обеспечение безопасности персональных данных в ИСПДн.

3.3. Участвует в определении актуальных угроз безопасности персональных данных при их обработке в ИСПДн, в подготовке модели угроз безопасности и акта определения уровня защищённости персональных данных.

3.4. Разрабатывает план мероприятий по обеспечению безопасности персональных данных в ИСПДн и обеспечивает его выполнение.

3.5. Определяет совместно с Директором порядок реагирования на инциденты информационной безопасности, связанные с персональными данными.

В части управления доступом:

3.6. Ведёт учёт лиц, допущенных к работе с персональными данными в ИСПДн, и поддерживает перечень лиц, допущенных к обработке персональных данных, в актуальном состоянии.

3.7. Осуществляет управление учётными записями пользователей ИСПДн: создание, изменение, блокирование, удаление учётных записей при приёме, переводе и увольнении работников в срок не позднее одного рабочего дня с даты соответствующего кадрового события.

3.8. Обеспечивает разграничение прав доступа пользователей к персональным данным в ИСПДн в соответствии с матрицей доступа, утверждённой Директором Организации.

3.9. Обеспечивает назначение, смену и контроль паролей пользователей ИСПДн. Минимальная длина пароля — 8 символов, включая буквы в верхнем и нижнем регистре, цифры и специальные символы. Смена паролей осуществляется не реже одного раза в 90 дней.

3.10. Осуществляет блокирование учётной записи пользователя при выявлении фактов нарушения требований по обеспечению безопасности персональных данных незамедлительно до выяснения обстоятельств.

В части эксплуатации средств защиты информации:

3.11. Осуществляет установку, настройку и администрирование средств защиты информации (СЗИ) в ИСПДн в соответствии с эксплуатационной и технической документацией.

3.12. Обеспечивает обновление программного обеспечения СЗИ, антивирусных баз и баз сигнатур средств обнаружения вторжений своевременно по мере выпуска обновлений производителем.

3.13. Ведёт журнал учёта средств защиты информации, эксплуатационной и технической документации к ним.

3.14. Обеспечивает контроль целостности программного обеспечения СЗИ. При обнаружении нарушения целостности СЗИ работа ИСПДн приостанавливается до восстановления целостности.

В части защиты при подключении к сети Интернет:

3.15. Осуществляет контроль за использованием межсетевых экранов, обеспечивающих фильтрацию сетевого трафика при взаимодействии ИСПДн с информационно-телекоммуникационными сетями общего пользования, в том числе сетью Интернет.

3.16. Обеспечивает контроль за соблюдением работниками Организации правил работы в сети Интернет, исключающих несанкционированную передачу персональных данных по незащищённым каналам связи.

В части эксплуатации СКЗИ:

3.17. Обеспечивает функционирование СКЗИ в соответствии с условиями сертификатов соответствия и эксплуатационной документацией.

3.18. Ведёт поэкземплярный учёт СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с требованиями Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации, утверждённой приказом ФАПСИ от 13.06.2001 № 152.

3.19. Контролирует соблюдение условий хранения СКЗИ и ключевых документов, исключающих несанкционированный доступ к ним. Хранение осуществляется в запираемых шкафах (сейфах), оборудованных индивидуальными замками.

3.20. Осуществляет контроль за уничтожением ключевых документов в порядке, установленном эксплуатационной документацией на СКЗИ, при их компрометации или по окончании срока действия.

В части мониторинга и контроля:

3.21. Осуществляет мониторинг событий информационной безопасности в ИСПДн, анализ журналов регистрации событий безопасности. Анализ журналов проводится не реже одного раза в месяц.

3.22. Выявляет попытки несанкционированного доступа к персональным данным и ИСПДн, фиксирует факты в журнале учёта нарушений информационной безопасности.

3.23. Проводит внутренние проверки (аудиты) соответствия обработки персональных данных в ИСПДн установленным требованиям не реже одного раза в год.

3.24. Контролирует размещение и использование технических средств ИСПДн в пределах контролируемой зоны Организации.

3.25. Контролирует выполнение резервного копирования персональных данных и баз данных ИСПДн. Резервное копирование осуществляется не реже одного раза в неделю. Восстановление из резервных копий тестируется не реже одного раза в квартал.

В части реагирования на инциденты:

3.26. При обнаружении инцидента информационной безопасности, связанного с персональными данными, незамедлительно принимает меры по локализации инцидента и минимизации его последствий.

3.27. Информирует Директора Организации о выявленном инциденте незамедлительно, но не позднее 2 часов с момента обнаружения.

3.28. Обеспечивает документирование инцидента: описание, время обнаружения, принятые меры, последствия. Акт расследования инцидента составляется в срок не позднее 72 часов с момента обнаружения инцидента.

3.29. Обеспечивает сохранение выгрузки из журнала регистрации событий ИСПДн за период, в котором произошёл инцидент, для приобщения к акту расследования инцидента.

В части обучения и инструктажа:

3.30. Проводит инструктаж работников Организации, допущенных к обработке персональных данных в ИСПДн, по вопросам обеспечения безопасности персональных данных при первичном допуске к работе с ИСПДн и далее не реже одного раза в год.

3.31. Ведёт журнал проведения инструктажей по вопросам обеспечения безопасности персональных данных. Журнал хранится в течение 3 лет с даты последней записи.

4. ПРАВА

4.1. Ответственный за безопасность ПДн имеет право:

- требовать от работников Организации соблюдения установленных требований по обеспечению безопасности персональных данных при работе в ИСПДн;
- запрашивать и получать от руководителей структурных подразделений Организации сведения, необходимые для выполнения задач, определённых настоящей Инструкцией;
- вносить предложения Директору Организации по совершенствованию организационных и технических мер обеспечения безопасности персональных данных в ИСПДн;
- инициировать проведение служебных проверок по фактам нарушений требований по обеспечению безопасности персональных данных;
- приостанавливать обработку персональных данных в ИСПДн в случае выявления нарушений требований к защите персональных данных, создающих угрозу безопасности персональных данных, с незамедлительным уведомлением Директора Организации;
- блокировать учётные записи пользователей ИСПДн при выявлении фактов нарушения требований по обеспечению безопасности персональных данных;

- получать доступ к журналам регистрации событий безопасности ИСПДн, журналам учёта средств защиты информации и иной документации, связанной с обеспечением безопасности персональных данных;
- участвовать в работе комиссий по определению уровня защищённости персональных данных и по уничтожению персональных данных;
- контролировать допуск работников к работе с СКЗИ и ключевыми документами;
- вносить предложения о привлечении к дисциплинарной ответственности работников, виновных в нарушении требований по обеспечению безопасности персональных данных.

5. ОТВЕТСТВЕННОСТЬ

5.1. Ответственный за безопасность ПДн несёт персональную ответственность за:

- надлежащее выполнение задач и функций, предусмотренных настоящей Инструкцией;
- обеспечение уровня защищённости персональных данных в ИСПДн не ниже УЗ-3;
- своевременное обнаружение и реагирование на инциденты информационной безопасности, связанные с обработкой персональных данных в ИСПДн;
- актуальность настроек средств защиты информации и правил разграничения доступа в ИСПДн;
- своевременное информирование Директора Организации о выявленных нарушениях требований по обеспечению безопасности персональных данных;
- сохранность конфиденциальности персональных данных и информации об организации системы защиты ИСПДн.

5.2. За неисполнение или ненадлежащее исполнение обязанностей, предусмотренных настоящей Инструкцией, Ответственный за безопасность ПДн несёт ответственность в соответствии с законодательством Российской Федерации и локальными нормативными актами Организации, в том числе:

- дисциплинарную ответственность — в соответствии со статьями 192–193 Трудового кодекса Российской Федерации;
- административную ответственность — в соответствии со статьями 13.11, 13.12, 13.14 Кодекса Российской Федерации об административных правонарушениях;
- уголовную ответственность — в соответствии со статьями 137, 272, 272.1 Уголовного кодекса Российской Федерации;
- гражданско-правовую ответственность — в соответствии с законодательством Российской Федерации в части возмещения ущерба, причинённого Организации или субъектам персональных данных.

6. ВЗАИМОДЕЙСТВИЕ

6.1. Ответственный за безопасность ПДн осуществляет взаимодействие:

6.2. С Директором Организации — по вопросам:

- утверждения организационно-распорядительных документов по обеспечению безопасности персональных данных;
- информирования о состоянии защищённости персональных данных в ИСПДн;
- информирования об инцидентах информационной безопасности;

— согласования мероприятий по обеспечению безопасности персональных данных и выделения ресурсов на их реализацию.

6.3. С Директором (ответственным за организацию обработки персональных данных) — по вопросам:

- координации мероприятий по обеспечению безопасности персональных данных и соблюдению требований законодательства;
- определения перечня лиц, допущенных к обработке персональных данных в ИСПДн, и актуализации матрицы доступа;
- организации уничтожения персональных данных при достижении целей обработки или по иным основаниям, предусмотренным Федеральным законом от 27.07.2006 № 152-ФЗ;
- совместного реагирования на обращения (запросы) субъектов персональных данных, затрагивающие вопросы безопасности обработки.

6.4. С Директором (ответственным за реагирование на инциденты) — по вопросам:

- выявления, регистрации и расследования инцидентов информационной безопасности;
- подготовки уведомлений в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) в сроки: первичное уведомление — не позднее 24 часов с момента обнаружения инцидента, уведомление о результатах расследования — не позднее 72 часов с момента обнаружения;
- разработки мер по предотвращению повторных инцидентов.

6.5. С работниками Организации, допущенными к обработке персональных данных в ИСПДн, — по вопросам:

- проведения инструктажей по вопросам обеспечения безопасности персональных данных при работе в ИСПДн;
- консультирования по правилам использования средств защиты информации;
- расследования фактов нарушения требований по обеспечению безопасности персональных данных.

6.6. С разработчиками и поставщиками средств защиты информации — по вопросам получения обновлений программного обеспечения СЗИ, технической поддержки и консультаций по эксплуатации.

6.7. С органом криптографической защиты (при его наличии) либо с лицензиатом ФСБ России — по вопросам организации эксплуатации СКЗИ, учёта ключевых документов и расследования случаев компрометации криптографических ключей.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящая Инструкция вступает в силу с даты утверждения приказом Директора Организации и действует до её отмены или замены новой редакцией.

7.2. Пересмотр настоящей Инструкции осуществляется не реже одного раза в 3 года, а также при:

- изменении законодательства Российской Федерации в области персональных данных и защиты информации;
- изменении уровня защищённости персональных данных в ИСПДн Организации;
- внедрении новых или модернизации существующих ИСПДн;

- выявлении по результатам контрольных мероприятий необходимости актуализации настоящей Инструкции;
- изменении состава угроз безопасности персональных данных.

7.3. Все изменения и дополнения к настоящей Инструкции утверждаются приказом Директора Организации.

7.4. Ответственный за безопасность ПДн подлежит ознакомлению с настоящей Инструкцией под подпись до начала выполнения возложенных обязанностей.

7.5. Настоящая Инструкция хранится постоянно (до замены новой редакцией). Документы, формируемые в ходе исполнения Инструкции (журналы учёта, акты проверок, протоколы инструктажей), хранятся в течение 3 лет с даты последней записи в условиях, исключающих несанкционированный доступ.

7.6. Вопросы, не урегулированные настоящей Инструкцией, разрешаются в соответствии с законодательством Российской Федерации в области персональных данных и защиты информации.

ЛИСТ ОЗНАКОМЛЕНИЯ

С настоящим документом ознакомлен(а) и обязуюсь выполнять его требования:

№	Фамилия, имя, отчество	Должность	Дата	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Лист согласования к документу № 396 от 06.07.2026
Инициатор согласования: Зайнеева О.В. Директор
Согласование инициировано: 06.07.2026 12:34

Лист согласования			Тип согласования: последовательное	
N°	ФИО	Срок согласования	Результат согласования	Замечания
1	Зайнеева О.В.		 Подписано 06.07.2026 - 12:34	-