

Инструкция
ответственного за обеспечение безопасности персональных данных в
информационных системах персональных данных
МБОУ «Махачкалинский многопрофильный лицей № 39 им. Б. Астемирова»

ОБЩИЕ ПОЛОЖЕНИЯ

Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных МБОУ «Махачкалинский многопрофильный лицей № 39 им. Б. Астемирова» (далее – Ответственный) назначается приказом МБОУ «Махачкалинский многопрофильный лицей № 39 им. Б. Астемирова» (далее – Лицей) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Лицея.

Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн.

В своей деятельности Ответственный руководствуется Политикой в отношении обработки персональных данных в Лицее, настоящей Инструкцией, рекомендациями Ответственного за организацию обработки персональных данных (далее – Ответственный за организацию обработки ПДн).

ОСНОВНЫЕ ФУНКЦИИ И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Функции Ответственного:

Ответственный изучает все стороны деятельности Лицей и вырабатывает рекомендации по защите ПДн при решении следующих основных вопросов:

проведение аналитической работы по комплексной защите и предупреждению утечки ПДн;

подготовка решений в отношении сведений о работах, выполняемых Лицеем, подлежащих защите;

координация внедрения и эксплуатации систем защиты и безопасности 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 с последующим предоставлением Ответственному за организацию обработки ПДн Лицей;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

обеспечение соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Лицей.

Ответственный обязан:

Соблюдать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн при их обработке в ИСПДн.

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

Осуществлять общее техническое сопровождение ИСПДн:

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

контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;

вести журнал учета и выдачи используемых материальных носителей ПДн;

контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;

проводить инструктаж работников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Лицей (далее – Пользователи ИСПДн) по правилам работы в ИСПДн.

Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн:

реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка работников, допущенных к работе в ИСПДн;

назначать пароли Пользователей ИСПДн;

контролировать плановую смену паролей Пользователями ИСПДн для доступа в ИСПДн;

своевременно удалять профиль Пользователя ИСПДн при увольнении или переводе работника;

вводить в базу данных системы защиты от несанкционированного доступа (далее – НСД) описания событий, подлежащих регистрации в системном журнале;

регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИСПДн;

своевременно информировать Ответственного за организацию обработки ПДн о несанкционированных действиях персонала для организации расследования попыток НСД.

Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИСПДн:

обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Лицей;

обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;

обеспечивать регулярное и своевременное создание резервных копий ИСПДн Лицей;

осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн.

Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн.

Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

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

Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

Контролировать выполнение Пользователями ИСПДн требований Инструкции пользователя информационных систем персональных данных Лицей, а также установленных требований для обеспечения уровней защищенности ПДн.

Контролировать правильность применения Пользователями ИСПДн средств защиты информации.

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 своих полномочий.

Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн:

антивирусного программного обеспечения;

средств защиты от несанкционированного доступа.

В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

Своевременно информировать Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИСПДн.

ПРАВА ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный имеет право:

Знакомиться с нормативными актами Лицей, регламентирующими процессы обработки и защиты ПДн.

Вносить предложения руководителю Лицей по совершенствованию существующей системы защиты информации.

Привлекать по согласованию с Ответственным за организацию обработки ПДн и руководителем Лицей к работе по созданию и совершенствованию системы защиты ПДн других работников Лицей.

Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных Лицей и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн.

Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн.

Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн.

Требовать прекращения работы в ИСПДн, как в целом, так и отдельных Пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн.

Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.