

Муниципальное автономное общеобразовательное учреждение

«Средняя общеобразовательная школа № 5»

СОГЛАСОВАНО

Протокол заседания

Педагогического совета

от 21.07.2025 г. № 56



УТВЕРЖДАЮ

Директор МАОУ СОШ № 5

И.Г. Попова

Приказ № 81/3-ПД

от 21.07.2025 г.

ПОЛОЖЕНИЕ

об информационной безопасности

в Муниципальном автономном общеобразовательном учреждении

«Средняя общеобразовательная школа № 5»

1. Общие положения

1.1. Настоящее положение разработано в соответствии с Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.), Федеральным законом от 07.07.2003 № 126-ФЗ «О связи», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ (с изм. и доп.) «О персональных данных», Федеральным законом от 28.12.2010 № 390-ФЗ «О безопасности».

1.2. Информационная безопасность является одним из составных элементов комплексной безопасности. Под информационной безопасностью МАОУ СОШ № 5 (далее – Учреждения) следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.3. К объектам информационной безопасности в Учреждении относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информация, защита которой предусмотрена законодательными актами РФ, в т.ч. персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.4. Система информационной безопасности должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);

- доступность (возможность получения пользователями информации в пределах их компетенции).

1.5. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита - это регламентация деятельности Учреждения и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2. Цели и задачи обеспечения безопасности информации

2.1. Главной целью обеспечения безопасности информации, циркулирующей в Учреждении, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Учреждения.

2.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Учреждении;
- предотвращение нарушений прав личности обучающихся, работников Учреждения на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

2.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Учреждения, нарушению нормального функционирования и развития Учреждения;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и

средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

- развитие и совершенствование защищенного юридически значимого электронного документооборота;
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;
- создание механизмов управления системой информационной безопасности.

3. Правовые нормы обеспечения информационной безопасности

3.1. Учреждение имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Учреждения, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

3.2. Учреждение обязано обеспечить сохранность конфиденциальной информации.

3.3. Администрация Учреждения:

- назначает ответственного за обеспечение информационной безопасности;
- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
- имеет право включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересов Учреждения со стороны государственных и судебных инстанций.

3.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Учреждения о назначении ответственного за обеспечение информационной безопасности;
- защищаемые информационные ресурсы и базы данных (КАИС ИРО, Поддержка ГИА, ФИС ОКО, ФИОКО, ФИС ФРДО, РБД, РБДО, Сервер статистики и т.д.);
- порядок рассмотрения запросов и предоставления информации сторонним организациям по их запросам (Приложение 1).

3.5. Порядок допуска сотрудников Учреждения к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и Учреждения об информационной безопасности и ответственности за разглашение информации

конфиденциального характера;

- инструктаж работника специалистом по информационной безопасности.

4. Организация системы обеспечения информационной безопасности

4.1. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в Учреждении устанавливаются:

- защита интеллектуальной собственности Учреждения;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т.ч. персональных данных работников и обучающихся Учреждения;
- учет всех носителей конфиденциальной информации;
- контроль за использованием электронных средств информационного обеспечения деятельности Учреждения по прямому назначению;
- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности Учреждения нелегализованных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;
- принятие мер к воспрепятствованию доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
- обучение персонала Учреждения по вопросам обеспечения информационной безопасности;
- контроль за правильностью использования имеющихся в Учреждении средств телефонной и радиосвязи.

5. Организация работы с информационными ресурсами и технологиями

5.1. Для организации делопроизводства приказом директора Учреждения назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Учреждения.

5.2. Система организации делопроизводства:

- учет всей документации Учреждения, в т.ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов Учреждения в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

53. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

53.1. Все документы передаются исполнителю под подпись в журнале учета документов.

53.2. Документы, дела и издания с персональными данными должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

53.3. Выданные для работы дела и документы с персональными данными подлежат возврату в канцелярию в тот же день.

53.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

53.5. Запрещается выносить документы с персональными данными за пределы Учреждения.

53.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

5.4. Срок данного Положения не ограничен. Данное положение действует до принятия нового.

Порядок рассмотрения запросов и предоставления информации сторонним организациям по их запросам

1. Запрос субъекта (представителя субъекта) персональных данных может быть направлен в МАОУ СОШ № 5:

- в письменной форме;
- в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации с использованием электронной почты МАОУ СОШ № 5.

2. Все поступившие запросы субъектов (представителей субъекта) персональных данных по вопросам обработки персональных данных регистрируются в Журнале входящей документации МАОУ СОШ № 5.

3. Ответственным лицом за ведение Журнала входящей документации является документовед.

4. После регистрации запроса ответственный за подготовку документа подготавливает мотивированный ответ на запрос и в случае необходимости направляет подготовленный ответ на рассмотрение всем задействованным лицам. Перечень лиц, привлекаемых для подготовки ответа, определяется ответственным за подготовку документа в зависимости от предмета обращения.

5. Лица, задействованные в подготовке ответа, должны соблюдать порядок и сроки обработки запросов, установленные законодательством Российской Федерации в зависимости от их типов.

6. После подготовки и отправки ответа на запрос, ответственный за подготовку ответа на запрос делает соответствующую отметку в Журнале исходящая документация МАОУ СОШ № 5 с указанием даты отправки.