

ПРИНЯТО
Протокол заседания
Педагогического совета
От 29.12.2020 № 5

УТВЕРЖДЕНО
Директор МАОУ «СОШ №12»
Л.В. Калина
Приказ от 30.12.2020 № 379



ПОЛОЖЕНИЕ

об информационной безопасности
в Муниципальном автономном общеобразовательном учреждении
«Средняя общеобразовательная школа № 12»

1. Общие положения

Данное Положение об информационной безопасности в Муниципальном автономном общеобразовательном учреждении «Средняя общеобразовательная школа № 12» (далее соответственно – Положение, МАОУ «СОШ № 12»), разработано в соответствии с Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.), Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" Информационная безопасность является одним из составных элементов комплексной безопасности школы.

Под информационной безопасностью школы 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.

К объектам информационной безопасности в МАОУ «СОШ № 12» относятся:

1. Перечень сведений, составляющих государственную тайну, в соответствии с Законом РФ от 21 июля 1993г. №5485-1 «О государственной тайне», утвержденных Указом Президента РФ;
2. информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
3. информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные;
4. средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

Система информационной безопасности (далее - СИБ) 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).

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 производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

2. Правовые нормы обеспечения информационной безопасности

- школа имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся, работников школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз;
- школа обязана обеспечить сохранность конфиденциальной информации;
- школа обязана обеспечить запрет на распространение информации, негативно влияющей на несовершеннолетних, запрещенной к распространению в соответствии с Федеральным законом №114-ФЗ от 25 июля 2002 «О противодействии экстремистской деятельности»;
- школа обязана обеспечить защиту информационных ресурсов сайта от размещения на них информации несовместимой с целями и задачами образовательного процесса.

Администрация школы:

- назначает ответственного за обеспечение информационной безопасности;
- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- 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 школы со стороны государственных и судебных инстанций.

Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ руководителя школы о назначении ответственного за обеспечение информационной безопасности;

- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников школы и др.

Кроме того, должен быть определен порядок допуска сотрудников школы к информации. Такой допуск предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Мероприятия по обеспечению информационной безопасности

3.1 Для обеспечения информационной безопасности в школе требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности школы;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся школы;
- учет всех носителей конфиденциальной информации.

3.2. Владелец информации, инженер-программист обязан обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

4. Организация работы с информационными ресурсами и технологиями

Система организации делопроизводства:

- учет всей документации школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов школы 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.

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

1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.
2. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.
3. Выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.
4. Передача документов исполнителю производится только через канцелярию или ответственного за организацию делопроизводства.
5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы ОУ.
6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

Для организации делопроизводства приказом руководителя ОУ назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной руководителем ОУ. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. Заключительные положения

5.1. Настоящее Положение принимается на Педагогическом совете «МАОУ СОШ № 12» и утверждается приказом директора МАОУ «СОШ № 12».

5.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

5.3. Настоящее Положение принимается на неопределенный срок.

5.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.