Утверждаю
И.о. директора МБОУ «Кесемская СОШ»
_____/В.А. Кириллова/
Приказ №23 от «3» 06 2022 г.

Положение об информационной безопасности МБОУ «Кесемская СОШ»

1. Общие положения

Информационная безопасность является одним из составных элементов комплексной безопасности образовательной организации. Под информационной безопасностью образовательной организации 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 образовательной организации 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.

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;

- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

2. Правовые нормы обеспечения информационной безопасности

Образовательная организация имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся, работников образовательной организации, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз;

Образовательная организация обязана обеспечить сохранность конфиденциальной информации;

Образовательная организация 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»;

Образовательная организация обязана обеспечить защиту информационных ресурсов сайта от размещения на них информации несовместимой с целями и задачами образовательного процесса.

Администрация образовательной организации:

- 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 образовательной организации со стороны государственных и судебных инстанций.

Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ руководителя образовательной организации 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 образовательной организации и др.

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

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и образовательной организации 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 образовательной организации требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности образовательной организации;

- 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 образовательной организации;

- учет всех носителей конфиденциальной информации.

3.2.Обладатель информации, оператор информационной системы 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 обеспечения уровня защищенности информации.

4. Организация работы с информационными ресурсами и технологиями

Система организации делопроизводства:

- учет всей документации образовательной организации, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов образовательной организации 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.

5.Нормативные документы

- Трудовой кодекс 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»