

• 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).

1.6 Обеспечение информационной безопасности осуществляется по следующим направлениям:

• правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

• организационная зашита - 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.

1. **Правовые нормы обеспечения информационной безопасности**

2.1. Центр образования имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Центра образования, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2.2. Центр образования обязан обеспечить сохранность конфиденциальной информации.

2.3. Администрация Центра образования:

· 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 Центра образования со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению

информационной безопасности:

· приказ директора Центра образования 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 Центра образования и др.

2.5. порядок допуска сотрудников Центра образования к информации предусматривает:

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

· ознакомление работника с нормами законодательства РФ и Центра образования об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

· инструктаж работника специалистом по информационной безопасности, заместителем директора по безопасности;

· контроль работника ответственным за информационную безопасность при

работе с информацией конфиденциального характера.

1. **Мероприятия по обеспечению информационной безопасности**

Для обеспечения информационной безопасности в Центре образования требуется проведение следующих первоочередных мероприятий:

· защита интеллектуальной собственности Центра образования;

· защита компьютеров, электронной почты, локальных сетей и сети подключения к системе Интернета;

· организация защиты конфиденциальной информации, в т. ч. персональных

данных работников и обучающихся Центра образования;

· учет всех носителей конфиденциальной информации.

**4. Организация работы с информационными ресурсами и технологиями**

4.1. Система организации делопроизводства:

· учет всей документации Центра образования, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

· регистрация и учет всех входящих (исходящих) документов Центра образования 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.

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

4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

4.2.2. 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.

4.2.3. Выданные для работы дела и документы с грифом "Для служебного

пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.

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

4.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы Центра образования.

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

4.3.Для организации делопроизводства приказом директора Центра образования назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Центра образования. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.