Рассмотрено
на заседании педагогического совета
от 24.12.2013 протокол № 4

Утверждаю
Директор
МБОУ гимназии №3
_____ А.М.Ананских
Приказ от 24.12. 2013. № 278

Положение
об информационной безопасности
МБОУ гимназии №3 г.Грязи Липецкой области

1. **Общие положения**

Информационная безопасность является одним из составных элементов комплексной безопасности ОУ.

Под информационной безопасностью ОУ 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 ОУ относятся:

- сведения, составляющие государственную тайну, в соответствии с Указом Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесённых к государственной тайне»;
- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и 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**

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

Администрация ОУ:

- 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 ОУ со стороны государственных и судебных инстанций.

Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ руководителя ОУ 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 ОУ.

и др.

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

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и ОУ 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.

1. Мероприятия по обеспечению информационной безопасности

Для обеспечения **информационной безопасности в ОУ требуется проведение следующих первоочередных мероприятий**:

- защита интеллектуальной собственности ОУ;
- защита компьютеров, локальных сетей, подключенных к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся ОУ;
- учет всех носителей конфиденциальной информации.

В соответствии с п.4 ст.16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», необходимо также обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение 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 защищённости информации.

2. Организация работы с информационными ресурсами и технологиями

Система организации делопроизводства:

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

3. 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"