Принято

на заседании педагогического совета
Протокол № 3 от 25.12.2019 г.

«Утверждаю»

Директор МАОУ «Гимназия»

_____ Т.И. Виноградова

ПОЛОЖЕНИЕ

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

в Муниципальном автономном общеобразовательном учреждении «Гимназия» городского округа город Урюпинск Волгоградской области

утверждено приказом МАОУ
«Гимназия» от 27.12.2020 года № 365

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности МАОУ «Гимназия» (далее – гимназия)

1.2. Данное Положение разработано в соответствии с:

- Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.);
- Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Федеральным законом «О защите детей от информации, причиняющий вред их здоровью и развитию» от 29.12.2010 № 436.

1.3. Под информационной безопасностью гимназии следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

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

1.5. К объектам информационной безопасности в гимназии относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, 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.

1.6. 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).

1.7. 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

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

2.2. Гимназия обязана обеспечить сохранность конфиденциальной информации.

2.3. Администрация гимназии:

- 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.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора гимназии 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 гимназии и др.

2.5.Порядок допуска сотрудников гимназии к информации предусматривает:

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

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

- защита интеллектуальной собственности гимназии;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся гимназии;

- учет всех носителей конфиденциальной информации;

- обеспечение контентной фильтрации для защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

4. ОРГАНИЗАЦИЯ РАБОТЫ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И ТЕХНОЛОГИЯМИ

4.1. Система организации делопроизводства:

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

- регистрация и учет всех входящих (исходящих) документов гимназии в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.).

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

4.2.1.передача документов исполнителю производится только через ответственного за организацию делопроизводства.

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

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ГИС «СЕТЕВОЙ ГОРОД. ОБРАЗОВАНИЕ»

5.1. ГИС «Сетевой Город. Образование» относится к группе многопользовательских информационных систем с разными правами доступа.

5.2. С учетом особенностей обрабатываемой информации, ГИС «Сетевой Город. Образование» соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.

5.3. ГИС «Сетевой Город. Образование» обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.

5.4. Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой в ГИС «Сетевой Город. Образование».

5.5. Участники образовательного процесса, имеющие доступ к ГИС «Сетевой Город. Образование», не имеют права передавать персональные логины и пароли для входа на ГИС «Сетевой Город. Образование» другим лицам.

5.6. Передача персонального логина и пароля для входа в ГИС «Сетевой Город. Образование» другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.

5.7. Участники образовательного процесса, имеющие доступ к ГИС «Сетевой Город. Образование», соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).

5.9. При проведении работ по обеспечению безопасности информации в ГИС «Сетевой Город. Образование» участники образовательного процесса, имеющие доступ к ГИС «Сетевой Город. Образование», обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.