Принято на заседании
Управляющего совета
МБОУ «ЦО – гимназия №11 им.
Александра и Олега Трояновских»
Протокол № 1
От 31.08.2020 года

«Утверждаю»
Директор
МБОУ «ЦО – гимназия №11 им.
Александра и Олега Трояновских»
_____ О.Н.Филина
Приказ от 31.08.2020 года №231-а

Положение об информационной безопасности муниципального бюджетного общеобразовательного учреждения «Центр образования – гимназия №11 им. Александра и Олега Трояновских»

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности МБОУ «ЦО – гимназия №11 им. Александра и Олега Трояновских» (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 от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

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

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

1.4. 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.

1.5. Система информационной безопасности Гимназии 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).

1.6 Обеспечение информационной безопасности Гимназии 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.

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 администратора информационной системы персональных данных;

- 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 Гимназии 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

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 школы;

- учет всех носителей конфиденциальной информации.

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.);

- 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. Выданные для работы дела и документы с грифом «Для служебного пользования» подлежат возврату в канцелярию в тот же день.

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

4.2.4. Запрещается выносить документы с грифом «Для служебного пользования» за пределы Гимназии.

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

4.3. Делопроизводство в Гимназии ведет специалист по кадрам. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Гимназии. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. Обеспечение безопасности при ведении Электронного журнала

5.1. Электронный журнал относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.

Электронный журнал обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.

Для настройки прав пользователей в системе Электронного журнала созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой в Электронном журнале.

5.2. Регламент общих ограничений для участников образовательного процесса при работе с Электронным журналом

5.2.1.Участники образовательного процесса, имеющие доступ к Электронному журналу, не имеют права передавать персональные логины и пароли для входа в Электронный журнал другим лицам. Передача персонального логина и пароля для входа в Электронный журнал другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.

5.2.2.Участники образовательного процесса, имеющие доступ к Электронному журналу, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).

5.2.3.Участники образовательного процесса, имеющие доступ к Электронному журналу, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не более чем одного

рабочего дня со дня получения информации о таком нарушении руководителя ОО, службу технической поддержки Электронного журнала.

5.2.4.Все операции, произведенные участниками образовательного процесса, имеющими доступ к Электронному журналу, с момента получения информации руководителем ОО и службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.

5.2.5.При проведении работ по обеспечению безопасности информации в Электронном журнале участники образовательного процесса, имеющие доступ к Электронному журналу, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.