Принято на Совете ОУ

Протокол № 1

от «30» 08 2019 г.

Утверждаю

Директор МОУ «Средняя школа №20

Кащеева Н.В.

«2» сентября 2019 г.

Приказ № 277

Положение
об информационной безопасности.

1.Общие положения

1.1.Информационная безопасность является одним из элементов комплексной безопасности.

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», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Под информационной безопасностью школы 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.

1.4.К объектам информационной безопасности относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ, в том числе персональные данные;
- средства и системы информации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющих прием, обработку, хранение и передачу информации с ограниченным доступом.

1.5. 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).

1.6. 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. Школа 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. Школа обязана обеспечить сохранность конфиденциальной информации.

2.3. Администрация школы:

- назначает ответственного за обеспечение информационной безопасности;
- издает нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы его защиты;
- имеет право включать требования по обеспечении информационной безопасности в коллективный договор;
- имеет право включать требования по обеспечении информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора школы 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 по их запросам, а также по правам доступа к ней сотрудников школы и др.

2.5. Порядок доступа сотрудников школы к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника по ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3.Мероприятия по обеспечению информационной безопасности.

Для обеспечения информационной безопасности в школе требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности школы;
- защита компьютеров, локальных сетей и сети подключения к системе Интернет;
- 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 школы, в т.ч. и на электронных носителях с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т.д.);
- особый режим уничтожения документов.

4.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:
- все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.
- документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.
- выданные для работы документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.
- передача документов исполнителю производится только через ответственного за организацию делопроизводства;
- запрещается выносить документы с грифом «Для служебного пользования» («Ограниченного пользования») за пределы школы;
- при смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема- передачи документов;
- для организации делопроизводства приказом директора школы назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы.

5. Обеспечение безопасности в электронном журнале и сайте школы.

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

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

Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением решений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой в электронном журнале и на сайте школы.

5.2.Регламент общих ограничений для участников образовательного процесса при работе с электронным журналом и сайтом школы, обеспечивающей Услуги.
- участники образовательного процесса, имеющие доступ к электронному журналу и сайту школы, не имеют права передавать персональные логины и пароли для входа на электронный журнал и сайт школы другим лицам. Передача персонального логина и пароля для входа на электронный журнал и сайт школы другим лицам влечет за собой ответственность в соответствии с законодательством РФ о защите персональных данных.
- участники образовательного процесса, имеющие доступ к электронному журналу и сайту школы, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль);
- участники образовательного процесса, имеющие доступ к электронному журналу и сайту школы, 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 образовательного организации, службу технической поддержки электронного журнала и сайта школы;
- все операции, произведенные участниками образовательного процесса, имеющими доступ к электронному журналу и сайту школы, с момента получения информации руководителем образовательной организации и службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.

- при проведении работ по обеспечению безопасности в электронном журнале и сайте школы участники образовательного процесса, имеющие доступ к электронному журналу и сайту школы, обязаны соблюдать требования законодательства РФ в области защиты персональных данных.