УТВЕРЖДЕНО
приказом директора
МБОУ «Балахоновская ОШ»
От 09 января 2023. № 3

ПОЛОЖЕНИЕ
об информационной безопасности

1. Общие положении

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности в МБОУ «Балахоновская ОШ» (далее— Школа), порядок организации работ по её созданию и функционированию.

1.2. Данное положение разработано в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации" п. 3 ст. 47 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" и имеет статус локального нормативного акта образовательной организации.

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. Использование сети Интернет в образовательной организации подчинено следующим принципам:

соответствие образовательным целям; способствование гармоничному формированию и развитию личности;

уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;

приобретение новых навыков и знаний; расширение применяемого спектра учебных и наглядных пособий;

социализация личности, введение в информационное общество.

1.5. К объектам информационной безопасности в Школе относятся:

информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;

информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. персональные данные;

средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

1.6. Система информационной безопасности (далее - СПБ) 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 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. ***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;

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 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;

перечень защищаемых информационных ресурсов и баз данных.

2.5. Порядок допуска 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 со специалистом по информационной безопасности;

контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Использование сети Интернет

3.1. Использование сети Интернет в Школе осуществляется в целях образовательного процесса.

3.2. ***Работники Школы вправе:***

размещать информацию в сети Интернет на интернет-ресурсах Школы;

иметь учетную запись электронной почты на интернет-ресурсах Школы.

3.3. ***Работникам Школы запрещено*** размещать в сети Интернет и на образовательных ресурсах информацию, противоречащую требованиям законодательства РФ и локальным нормативным актам Школы, не относящуюся к образовательному процессу и не связанную с деятельностью Школы, нарушающую нравственные и этические нормы, требования профессиональной этики.

3.4. ***Обучающиеся Школы вправе:***

использовать ресурсы, размещенные в сети Интернет, в том числе интернет-ресурсы Школы, в порядке и на условиях, которые предусмотрены настоящим Положением.

размещать информацию и сведения на интернет-ресурсах Школы.

3.5. ***Обучающимся запрещено:***

находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и / или нарушает законодательство РФ;

осуществлять любые сделки через интернет;

загружать файлы на компьютер Школы без разрешения уполномоченного лица;

распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Школы.

3.6. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

3.7. ***Уполномоченное лицо обязано:***

принять сообщение пользователя;

принять меры по отключению выхода на данный ресурс с интернет ресурсов Школы;

4. Мероприятия по обеспечению информационной безопасности

4.1. Для обеспечения информационной безопасности в Школе требуется проведение следующих первоочередных мероприятий:

защита интеллектуальной собственности Школы;

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.

5. Организация работы с информационными ресурсами и технологиями

5.1. 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 Школы 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.

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

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

5.2.2. 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.

5.2.3. Выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.

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

5.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы школы.

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

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

6. О системном администрировании и обязанностях ответственного за информационную безопасность

6.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора (вменено в обязанности учителя информатики, администратора АИС) в МБОУ «Балахоновская ОШ»

6.2. Для решения задач информационной безопасности системный администратор обязан:

следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;

обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;

обеспечивать нормальное функционирование системы резервного копирования.

7. Антивирусная защита

7.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения.