Положение об информационной безопасности

1. Общие положении
   1. Информационная безопасность является одним из составных элементов комплексной безопасности.

# Данное положение разработано в соответствии с Трудовым кодексом Российской Федерации от 30.12.2001 г. № 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», Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»; Распоряжением Правительства Российской Федерации от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей», Постановлением Правительства РФ № 781 от 17.11.2007 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Постановление П. РФ № 687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановление П. РФ № 582 от 10.07.2013 «Об утверждении Правил размещения на официальном сайте ОУ в информационно-телекоммуникационной сети “ИНТЕРНЕТ” и обновления информации об образовательной организации»; Приказ Федеральной службы по надзору в сфере образования и науки от 29 мая 2014 г. N 785 "Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления на нем информации" (с изменениями и дополнениями), Федеральным законом от 29.12. 2010 № 436-ФЗ “О защите детей от информации, причиняющей вред их здоровью и развитию”; Федеральным законом от 25.07.2002 № 114-ФЗ “О противодействии экстремистской деятельности” Федеральный закон от 21 июля 2014 г. 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" Постановление П. РФ от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; П. Федеральной службы от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Постановление П. РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” Приказ Минфина РФ от 21.07.2011г. № 86н “Об утверждении порядка предоставления информации государственным (муниципальным) учреждением, её размещения на официальном сайте в сети Интернет и ведения указанного сайта”.

* 1. Под информационной безопасностью образовательной организации 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. К объектам информационной безопасности в образовательной организации относятся:
* информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера:
* информацию, защита которой предусмотрена законодательными актами Российской Федерации, 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. 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 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.
* 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. Правовые нормы обеспечения информационной безопасности

1. Образовательная организация имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников образовательной организации, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.
2. Образовательная организация обязана обеспечить сохранность конфиденциальной информации.
3. Администрация образовательной организации:

* назначает ответственного за обеспечение информационной безопасности;

1. Организационные и функциональные документы по обеспечению информационной безопасности:

* приказ директора образовательной организации 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 школы и др.

1. порядок допуска сотрудников школы к информации предусматривает:

* принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
* ознакомление работника с нормами законодательства Российской Федерации и школы 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
   1. Для обеспечения информационной безопасности в образовательной организации требуется проведение следующих первоочередных мероприятий:

* защита интеллектуальной собственности образовательной организации;
* защита компьютеров, локальных сетей и сети подключения к системе Интернета;
* организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся образовательной организации;
* учет всех носителей конфиденциальной информации.
  1. Использование сети Интернет работниками образовательной организации допускается только в целях исполнения ими своих должностных обязанностей и в целях образовательного процесса, использование сети Интернет обучающимися допускается только в целях образовательного процесса.
  2. Использование сети Интернет в образовательной организации в личных целях работниками и обучающимися не допускается.
  3. В целях своевременного выявления угроз, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, в образовательной организации проводится периодический контроль состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет, в том числе контроль функционирования технических средств контентной фильтрации и антивирусной защиты.  
      Периодичность такого контроля и состав мероприятий по контролю устанавливается руководителем образовательной организации.
  4. Обучающиеся в случае выявления наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, незамедлительно информирует преподавателя, ведущего занятие, или иного ответственного работника образовательной организации.
  5. Педагогический работник, ведущий занятие, иной ответственный работник образовательной организации обязан осуществлять постоянный контроль использования технических средств, применяемых при организации доступа к сети Интернет (программных, программно-аппаратных), в том числе контроль функционирования технических средств контентной фильтрации, а также контроль доступа обучающихся к ресурсам сети Интернет.  
      При получении информации от обучающихся о получении доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, или в случае самостоятельного выявления наличия доступа к таким ресурсам сети Интернет, незамедлительно принимать меры, направленные на прекращение и ограничение доступа обучающихся к такой информации, а также информировать об инциденте работника образовательной организации, ответственного за организацию доступа к сети Интернет.
  6. При организации доступа и использовании сети Интернет в образовательной организации работники образовательной организации несут персональную ответственность в соответствии действующим законодательством Российской Федерации.
  7. Обучающиеся и их родители (законные представители) несут ответственность за неправомерное использование сети Интернет в порядке, установленном в образовательной организации, и в соответствии с действующим законодательством Российской Федерации.

1. Организация работы с информационными ресурсами и технологиями
   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.

4.2. 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 ответственного за организацию делопроизводства.
5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы образовательной организации.
6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

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

1. Обеспечение безопасности в Автоматизированной информационной системе
   1. Автоматизированная информационная система 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.

Автоматизированная информационная система обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.

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

* 1. Регламент общих ограничений для участников образовательного процесса при работе с Автоматизированной информационной системой, обеспечивающей предоставление Услуги.
     1. Участники образовательного процесса, имеющие доступ к Автоматизированной информационной системе, не имеют права передавать персональные логины и пароли для входа в Автоматизированную информационную систему другим лицам. Передача персонального логина и пароля для входа в Автоматизированную информационную систему другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.
     2. Участники образовательного процесса, имеющие доступ к Автоматизированной информационной системе, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).
     3. Участники образовательного процесса, имеющие доступ к Автоматизированной информационной системе, 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 образовательной организации, службу технической поддержки Автоматизированной информационной системы.
     4. Все операции, произведенные участниками образовательного процесса, имеющими доступ к Автоматизированной информационной системе, с момента получения информации руководителем образовательной организации и службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.
     5. При проведении работ по обеспечению безопасности информации в Автоматизированной информационной системе участники образовательного процесса, имеющие доступ к Автоматизированной информационной системе, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.