ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

" БРЯНКОВСКАЯ СПЕЦИАЛИЗИРОВАННАЯ ШКОЛА № 1"

(ГОУ ЛНР «Брянковская СШ № 1»)

УТВЕЖДАЮ

Директор школы

\_\_\_\_\_\_\_\_\_Н.Н.Ганжара

**Положение об**[**информационной безопасности**](http://www.pandia.ru/text/category/informatcionnaya_bezopasnostmz/)

**1.        Общие положении**

Информационная безопасность является одним из составных элементов комплексной безопасности

Данное положение разработано в соответствии с Трудовым кодексом РФ ФЗ (с изм. и доп.).  Федеральным законом ФЗ "Об информации, [информационных технологиях](http://pandia.ru/text/category/informatcionnie_tehnologii/) и о [защите информации](http://pandia.ru/text/category/zashita_informatcii/)". Федеральным законом ФЗ "О персональных данных”.

Под [информационной безопасностью](http://pandia.ru/text/category/bezopasnostmz_informatcionnaya/) школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Система [информационной безопасности](http://www.pandia.ru/text/category/informatcionnaya_bezopasnostmz/) направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

К объектам [информационной безопасности](http://pandia.ru/text/category/bezopasnostmz_informatcionnaya/) в школе относятся:

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

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

• средства и системы информатизации, программные средства, [автоматизированные системы](http://www.pandia.ru/text/category/avtomatizirovannie_sistemi/) управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

Система информационной безопасности (далее - СИБ) должна обязательно обеспечивать:

• конфиденциальность ([защиту информации](http://pandia.ru/text/category/zashita_informatcii/) от несанкционированного раскрытия или перехвата):

• целостность (точность и полноту информации и компьютерных программ);

• доступность (возможность получения пользователями информации в пределах их компетенции).

Обеспечение информационной безопасности осуществляется по следующим направлениям:

• правовая зашита - это специальные законы, другие [нормативные акты](http://pandia.ru/text/category/akt_normativnij/), правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе:

• организационная зашита - это регламентация производственной деятельности и [взаимоотношений](http://www.pandia.ru/text/category/vzaimootnoshenie/) исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба:

•        инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

Правовые нормы обеспечения информационной безопасности.

ГОУ ЛНР «Брянковская СШ №1» 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. 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](http://www.pandia.ru/text/category/kollektivnie_dogovora/); имеет право включать требования по защите информации в договоры по всем [видам деятельности](http://www.pandia.ru/text/category/vidi_deyatelmznosti/); разрабатывает перечень сведений конфиденциального характера;

• имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

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 специалистом по информационной безопасности;

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

**Мероприятия по обеспечению информационной безопасности**

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

• защита [интеллектуальной собственности](http://pandia.ru/text/category/intellektualmznaya_sobstvennostmz/) 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.

**Обеспечение безопасности в Школьном портале**

Школьный портал 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.

Школьный портал 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 в Школьном портале.

Регламент общих ограничений для участников образовательного процесса при работе со «Школьным порталом», обеспечивающей предоставление Услуги.

Участники образовательного процесса, имеющие доступ к Школьному порталу, не имеют права передавать персональные логины и пароли для входа на Школьный портал другим лицам. Передача персонального логина и пароля для входа в Школьный портал другим лицам влечет за собой ответственность в соответствии с [законодательством Российской Федерации](http://www.pandia.ru/text/category/zakoni_v_rossii/) о защите персональных данных.

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

Участники образовательного процесса, имеющие доступ к Школьному порталу, 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 Школьного портала.

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

При проведении работ по обеспечению безопасности информации в Школьном портале участники образовательного процесса, имеющие доступ к Школьному порталу, обязаны соблюдать требования [законодательства Российской Федерации](http://www.pandia.ru/text/category/zakoni_v_rossii/) в области защиты персональных данных