Республика Саха (Якутия)
Муниципальное бюджетное
общеобразовательное учреждение
«Средняя общеобразовательная школа № 4
п.Нижний Куранах»
МО «Алданский район»
678940 Республика Саха (Якутия) Алданский район, пос.Нижний Куранах,
ул. Школьная, д. 19, тел: (41145) 62-315, факс: (41145) 62-315, school4-sakha@mail.ru
Сайт: **http://www.school4- sakha.ucoz.com**

«Утверждаю»

Принято на заседании
Педагогического совета
Протокол № 4
от «28» 12 2018 г.

Директор МБОУ СОШ № 4
Л.В. Мухина
«28» 12 2018 г.

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МБОУ «СОШ №4 п. Нижний Куранах»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Информационная безопасность является одним из составных 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 «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Федеральным законом «О защите детей от информации, причиняющий вред их здоровью и развитию» от 29.12.2010 № 436.

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

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

1.5. К объектам информационной безопасности в школе 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.

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

- конфиденциальность (защиту информации):
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.2. 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. Образовательная организация 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. Образовательная организация 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 защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора ОУ о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных.

2.5. Порядок допуска сотрудников образовательной организации к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и образовательной организации 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

3.1. Для обеспечения информационной безопасности в образовательной организации 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;
- присвоение и размещение знака информационной продукции и (или) текстового предупреждения об информационной продукции, запрещенной для детей.

4. ОРГАНИЗАЦИЯ РАБОТЫ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И ТЕХНОЛОГИЯМИ

4.1. Система организации делопроизводства:

- учет всей документации образовательной организации, 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.);
- особый режим уничтожения документов.

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

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ШКОЛЬНОМ ПОРТАЛЕ

5.1. Школьный портал относится к группе многопользовательских информационных систем с разными правами доступа.

5.2. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.

5.3. Школьный портал обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.

5.4. 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.

5.5. Регламент общих ограничений для участников образовательного процесса при работе со Школьным порталом, обеспечивающим предоставление Услуги.

5.6. Участники образовательного процесса, имеющие доступ к Школьному порталу, не имеют права передавать персональные логины и пароли для входа на Школьный портал другим лицам.

5.7. Передача персонального логина и пароля для входа в Школьный портал другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.

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

5.9. 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.

5.10. 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.

5.11. При проведении работ по обеспечению безопасности информации в Школьном портале участники образовательного процесса, имеющие доступ к Школьному порталу, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.