

Муниципальное казенное общеобразовательное учреждение  
«Средняя общеобразовательная школа №2» с.п. Кахун  
Урванского муниципального района КБР

РАССМОТРЕНО  
на заседании  
педагогического совета  
МКОУ СОШ №2 с.п. Кахун  
протокол от 28 августа 2017г.



«УТВЕРЖДАЮ»

Директор МКОУ СОШ №2 с.п. Кахун

Гетоков Х.Х.

28.09.2017 год

с.п. Кахун

**ИНСТРУКЦИЯ**  
**пользователя по обеспечению информационной безопасности**  
**автоматизированного рабочего места, выделенного для обработки конфиденциальной**  
**информации (персональных данных)**  
**в МКОУ СОШ № 2 с.п.Кахун**

В Инструкции пользователя по обеспечению информационной безопасности при работе с базами данных школы (далее – Инструкция пользователя) использованы следующие термины и определения:

1. База данных (далее - АИС) - централизованное хранилище информации, оптимизированное для многопользовательского доступа и работающее под управлением системы управления базами данных .

2. Комплекс программных средств (далее - КПС) - система или приложение, использующее непосредственный доступ к АИС.

3. Идентификатор (учетное имя или login) - присвоенная пользователю индивидуально буквенно-числовая последовательность, используемая для идентификации пользователя при установлении доступа к АИС и позволяющая однозначно определять работу конкретного пользователя в АИС.

4. Пароль - секретная персональная последовательность символов, известная только пользователю, которая используется совместно с идентификатором для доступа в АИС и позволяет подтвердить, что доступ к АИС осуществляет именно конкретный пользователь.

5. Пользователи - должностные лица **МКОУ СОШ № 2 с.п.Кахун** , а также все другие лица и организации, работающие с АИС школы.

6. Администратор АИС - должностное лицо **МКОУ СОШ № 2 с.п.Кахун**, уполномоченные для выполнения административных функций и обеспечивающие функционирование АИС и ее безопасность соответственно.

7. Локально-вычислительная сеть (далее - ЛВС) - группа компьютеров, а также периферийное оборудование, объединенные одним или несколькими автономными каналами передачи

цифровых данных в пределах одного или нескольких близлежащих зданий.

8. Политика информационной безопасности - комплекс организационно-технических мероприятий, правил и условий использования информационных систем **МКОУ СОШ № 2 с.п.Кахун**, определяющих нормальное функционирование систем и обеспечение безопасности информации, обрабатываемой в школе

Настоящий документ разработан на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»,

утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, с целью совершенствования методического обеспечения деятельности в данной области государственных и муниципальных органов, юридических и физических лиц, организующих и (или) осуществляющих обработку персональных данных (ПДн), определяющих цели и содержание обработки ПДн (операторов), а также заказчиков и разработчиков информационных систем персональных данных (ИСПДн) при решении ими задач по обеспечению безопасности ПДн.

### **Общие положения по организации доступа к конфиденциальной информации в МКОУ СОШ № 2 с.п.Кахун**

Инструкция пользователя определяет комплекс организационно - технических мероприятий по обеспечению безопасности конфиденциальной информации, хранящейся на компьютерах школы в АИС и обрабатываемой с помощью средств вычислительной техники в МКОУ СОШ № 2 с.п.Кахун

1. Инструкция пользователя является частью политики информационной безопасности МКОУ СОШ № 2 с.п.Кахун, предназначена для обеспечения эффективной организации и управления доступом пользователей к конфиденциальной информации, хранящейся на компьютерах школы и в АИС МКОУ СОШ № 2 с.п.Кахун, и содержит требования по обеспечению информационной безопасности учреждения в части выполнения операций со конфиденциальной информацией и по организации и управлению доступом к АИС.

2. Требования Инструкции пользователя обязательны для выполнения всеми пользователями, которым предоставляется доступ к конфиденциальной информации МКОУ СОШ № 2 с.п.Кахун.

3. Доступ к конфиденциальной информации школы предоставляется исключительно пользователям, утверждённым приказом администрации школы через предоставленный системным администратором школы пароль.

4. Решение задач, связанных с организацией и управлением доступом должностных лиц школы к конфиденциальной информации, осуществляется системным администратором школы.

При возникновении ситуаций, не включенных в положения настоящей Инструкции пользователя, решение принимает системный администратор.

5. Для доступа к АИС школы у каждого пользователя должен иметь свой уникальный идентификатор и пароль доступа к АИС.

6. Доступ к АИС школы может быть предоставлен с любого компьютера административной локальной сети.

7. Доступ к АИС предоставляется пользователям на срок действия их трудовых отношений и исполнения служебных обязанностей в МКОУ СОШ № 2 с.п.Кахун

### **Обязанности и ответственность пользователей автоматизированных рабочих мест, выделенных для обработки конфиденциальной информации.**

1. Перед началом первой работы с конфиденциальной информацией пользователь обязан изучить Инструкцию пользователя и ознакомиться с ответственностью за выполнение требований Инструкции пользователя при работе с конфиденциальной информацией под роспись.

2. Пользователю запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа к конфиденциальной информации другим лицам. Запрещается хранение пароля в общедоступных местах, позволяющих другим лицам получить информацию о пароле.

3. Пользователь конфиденциальной информации обязан обеспечивать правильность ввода и коррекции данных, за которые он отвечает.

4. Пользователь обязан закрывать соединение с АИС школы на время своего отсутствия у рабочей места, или вообще выходить по доступу к ресурсам компьютера с конфиденциальными данными из своего идентификатора (*например, teacher, secret, adminic и т.п., через Пуск\_Завершить сеанс Имя идентификатора*).

5. В случае выявления инцидентов с доступом к ресурсам компьютера с конфиденциальными данными (фактов несанкционированного доступа посторонними людьми,

людьми без допуска к конфиденциальным данным) пользователь обязан незамедлительно сообщить об этом системному администратору школы.

6. В случае выявления инцидентов с доступом к АИС школы (фактов несанкционированного доступа к АИС, блокировки доступа, утери или компрометации пароля и т.п.) пользователь обязан незамедлительно сообщить об этом администратору АИС

7. Установку и конфигурирование программного обеспечения на компьютерах с доступом к конфиденциальным данным школы выполняет системный администратор или администратор АИС школы. Пользователям данных рабочих мест запрещается самостоятельно устанавливать какое-либо программное обеспечение.

8. Пользователю запрещается использовать информацию, полученную в результате доступа к конфиденциальным данным школы, в целях, не предусмотренных его функциональными обязанностями и технологическими схемами. Он не вправе разглашать, использовать в личных целях, либо передавать третьим лицам, в том числе государственным органам, конфиденциальную информацию, за исключением случаев, установленных законами Российской Федерации.

9. При нарушениях правил, связанных с информационной безопасностью, пользователь несет ответственность, установленную действующим законодательством Российской Федерации.

10. Пользователь несет ответственность за все действия, совершенные от имени его идентификатора, учетной записи или логина, если не доказан факт несанкционированного использования таковых.