Принято На педагогическом совете МБОУ Лукашевская СОШ 31 августа 201 г.	Утверждаю Директор школы _____ (Монахова И.А.) 31 августа 201 года. МБОУ Лукашевская СОШ

ИНСТРУКЦИЯ
пользователю МБОУ «Лукашевская СОШ» по обеспечению безопасности информации

1. Общие обязанности пользователей по обеспечению безопасности информации в автоматизированной системе

1.1. Каждый сотрудник МБОУ «Лукашевской средней общеобразовательной школы» участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным (в дальнейшем именуемый Пользователь), несет персональную ответственность за свои действия при работе с информационными ресурсами автоматизированной системы (далее - АС) и обязан:

- При работе с документами, содержащими конфиденциальную информацию, руководствоваться локальным актом МБОУ «Лукашевской средней общеобразовательной школы» «Положение о работе с документами и другими физическими носителями информации «Для служебного пользования».
- Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС.
- Знать и строго выполнять правила работы со средствами защиты информации, установленными на АС.
- Хранить в тайне свой пароль (пароли). В соответствии с правилами обращения с парольной защитой с установленной периодичностью менять свой пароль (пароли).
- Выполнять требования инструкции «Об организации антивирусной защиты в автоматизированной системе , используемой МБОУ «Лукашевской средней общеобразовательной школой» в работе» в части, касающейся действий пользователей АС.
- Следить за правильным разграничением доступа к информации (объектам информационного обмена), с которой он работает.
- Немедленно ставить в известность директора МБОУ «Лукашевской средней общеобразовательной школы» и ответственного за защиту информации в МБОУ «Лукашевской средней общеобразовательной школе» и вызывать специалиста, назначенного для обслуживания АС, при подозрении компрометации пароля, а также при обнаружении:
  - фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к защищенной АС;
  - несанкционированных изменений в конфигурации программных или аппаратных средств АС;
  - отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АС, выхода из строя или неустойчивого функционирования узлов АС или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
  - некорректного функционирования установленных на АС технических средств защиты;
  - непредусмотренных формуляром АС отводов кабелей и подключенных устройств.

2. Пользователям АС категорически ЗАПРЕЩАЕТСЯ:

- Использовать компоненты программного и аппаратного обеспечения АС в неслужебных целях.
- Записывать пароль на любые носители, в том числе бумажные, кроме зарегистрированного журнала учета паролей установленной формы.
- Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АС или устанавливать дополнительно любые программные и аппаратные средства.
- Осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц.
- Записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.).
- Оставлять включенным в свое отсутствие персональный компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры).
- Оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения).
- Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок необходимо ставить в известность специалиста, обслуживающего АС.
- Разрешать работу на АС лицам, не допущенным приказом директора МБОУ от «____» _____ № ____.

3. Правила работы на персональном компьютере

3.1. Пользователь не имеет права работать под чужим персональным идентификатором (именем пользователя АС).

3.2. Пользователю запрещается самостоятельно вносить изменения в программную и аппаратную конфигурацию компьютера. Все изменения производятся на основании заявок, поданных на имя директора МБОУ «Лукашевской средней общеобразовательной школы» .

3.3. Пользователь не имеет права нарушать парольную защиту, установленную на BIOS.

3.4. В случае возникновения неисправности персонального компьютера пользователь должен прекратить работу и незамедлительно обратиться к руководителю подразделения и специалисту, ответственному за работу АС.

3.5. Покидая свое рабочее место, пользователь обязан выключить персональный компьютер.

4. Правила ограничения доступа к ресурсам АС

4.1. Пользователь несет ответственность за разграничение доступа к файлам, директориям и другим объектам АС, если он наделен такими полномочиями. Создавая новый объект файловой системы, он обязан убедиться, что только он и те, кому это положено, имеют права на доступ к этому ресурсу в соответствии с их потребностями (Чтение / Редактирование и т.д.).

4.2. Пользователь должен периодически самостоятельно отслеживать права доступа к ресурсам, с которыми он работает. В случае обнаружения в списке доступа записей, которые он не вносил, пользователь обязан немедленно оповестить руководителя подразделения.

4.3. Допуск обслуживающего персонала к программно-аппаратным средствам осуществляется под контролем пользователя АС.