

УТВЕРЖДАЮ
Директор МБОУ Ли
**** М.
Приказ № 24 от 14.0

Протокол № 6 от 09.08.2024г.

Приказ № 24 от 14.08.2024г.

- установка в подразделении новой ПЭВМ;
- замена ПЭВМ;
- изъятие ПЭВМ;
- добавление устройства (узла, блока) в состав конкретной ПЭВМ;
- замена устройства (узла, блока) в составе конкретной ПЭВМ;
- изъятие устройства (узла, блока) из состава конкретной ПЭВМ;

- установка (развертывание) на конкретной ПЭВМ программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данной ПЭВМ);

- обновление (замена) на конкретной ПЭВМ программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

- удаление с конкретной ПЭВМ программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной ПЭВМ).

8. В заявке указываются условные наименования (шифр) развернутых ПЭВМ в соответствии с Перечнем технических средств. В случае развертывания новой ПЭВМ ее наименование в заявке указывать не требуется, оно устанавливается позднее приказом «О внесении изменений в состав ОИ...». Наименования задач указываются в соответствии с формулярами задач или перечнем задач архива эталонных дистрибутивов (АЭД), которые можно решать с использованием АС.

9. Заключение о технической возможности осуществления затребованных изменений, о возможности совмещения решения новых задач (обработки информации) на указанных в заявке ПЭВМ выдается ответственным администратором защиты информации.

10. После чего заявка передается администратору защиты информации для непосредственного исполнения работ по внесению изменений в конфигурацию ПЭВМ.

11. Ответственный за обеспечение безопасности допускает уполномоченных исполнителей к внесению изменений в состав аппаратных средств и программного обеспечения только по предъявлении последними утвержденной заявки на осуществление данных изменений.

12. Установка, изменение (обновление) и удаление системных и прикладных программных средств, установка, снятие, и внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на ПЭВМ осуществляется уполномоченными администраторами. Работы производятся в присутствии ответственного за ПЭВМ пользователя.

13. Подготовка модификаций программного обеспечения серверов и рабочих станций, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов и другие необходимые действия производится согласно утвержденным положениям и инструкциям.

14. Установка или обновление подсистем должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

15. Модификация программного обеспечения (далее — ПО) на ПЭВМ осуществляется уполномоченным администратором обязательно в присутствии ответственного за обеспечение безопасности информации. После установки модифицированных модулей на ПЭВМ администратор безопасности в присутствии ответственного за обеспечение безопасности информации устанавливает защиту целостности модулей на ПЭВМ (производит пересчет контрольных сумм эталонов модулей с помощью соответствующих сертифицированных средств). После проведения модификации программного обеспечения на ПЭВМ проводится антивирусный контроль.

16. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

17. После установки (обновления) ПО, администратор защиты информации должен произвести настройку средств управления доступом СЗИ НСД к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром и совместно

с ответственным пользователем ПЭВМ должен проверить работоспособность ПО и правильность настройки средств защиты.

18. После завершения работ по внесению изменений в состав аппаратных средств защищенной ПЭВМ ее системный блок должен закрываться и опечатываться (пломбироваться, защищаться специальной наклейкой).

19. Уполномоченные исполнители работ должны произвести соответствующую запись в «Журнале учета нештатных ситуаций, выполнения профилактических работ, установки и модификации аппаратных и программных средств. делают отметку о выполнении (на обратной стороне заявки) и передают исполненную заявку ответственному за информационную безопасность для хранения вместе с формуляром данной ПЭВМ.

20. При изъятии ПЭВМ из состава АС ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как администратор безопасности снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом согласно «Порядку уничтожения информации конфиденциального характера и остаточной информации с машинных носителей информации и уничтожения машинных носителей информации».

21. Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется согласно «Инструкции по внесению изменений в списки пользователей системы и наделению пользователей полномочиями доступа к ресурсам АС...».

22. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств ПЭВМ с отметками о внесении изменений в состав аппаратно-программных средств должны храниться вместе с оригиналами формуляров ПЭВМ и «Журналом учета нештатных ситуаций...» у ответственного за обеспечение безопасности.

23. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на ПЭВМ. В данной ситуации сотрудник подразделения ставит в известность руководство организации и ответственного за обеспечение безопасности. Факт внесения изменений в ПО ПЭВМ фиксируется актом. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), проводившее изменения. Если это необходимо, администратор вносит необходимые корректировки в настройки системы контроля целостности ПО ПЭВМ. Факт модификации ПО и корректировки настроек системы защиты фиксируется в «Журнале учета нештатных ситуаций...».

24. В течение следующего дня после составления акта ответственным за обеспечение безопасности при участии сотрудников подразделения выясняются причины и состав проведенных экстренных изменений и принимается решение о необходимости подготовки исправительной модификации ПО или восстановления ПО ПЭВМ с эталонной копии. Необходимость участия в разбирательстве сотрудника подразделения определяется руководством.

25. Настоящая Инструкция доводится до ответственных сотрудников под подпись.

26. Настоящая Инструкция вступает в силу с момента её утверждения руководителем образовательного учреждения.

ТИПОВАЯ ФОРМА

Руководителю организации

ЗАЯВКА

на внесение изменений в состав аппаратно-программных средств АС

Прошу произвести следующие изменения конфигурации аппаратно-программных средств
автоматизированной системы _____

наименование подразделения

развернуть новую рабочую станцию и установить на (обновить на / снять с) нее _____
_____ компоненты, необходимые для решения следующих задач:

наименование задач

Должность

Подпись

Инициалы, Фамилия

« ____ » _____ 20 ____ г.

ТИПОВАЯ ФОРМА

Руководителю организации

ЗАЯВКА

на допуск сотрудников к аппаратно-программным средствам АС

В связи с необходимостью _____
обоснование причины внесения изменений

прошу допустить установленным порядком сотрудников: _____

фамилии исполнителей

для выполнения необходимых работ в _____
наименование подразделения

по установке рабочей станции (обновлению / снятию с ПЭВМ _____ компонентов),
необходимых для решения следующих задач: _____
наименование задач

_____ Должность _____ Подпись _____ Инициалы, Фамилия

« ____ » _____ 20 ____ г.

Отметка о выполнении

(о внесении изменений в состав аппаратно-программных средств АС)

В соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и технических средств...» рабочей группой в составе:

от ответственного за обеспечение безопасности: _____

от администратора безопасности: _____

указанные в заявке изменения внесены (не внесены по следующей причине):

краткое пояснение причины

Изменения в технический паспорт и соответствующие журналы внесены.

должность

должность

подпись, фамилия

подпись, фамилия

« ____ » _____ 20 ____ г.

« ____ » _____ 20 ____ г.

ПОРЯДОК
технического обслуживания и ремонта технических средств
автоматизированных систем МБОУ Лицей г. Бирска

Настоящий порядок технического обслуживания и ремонта разработан в дополнение к Положению «Об организации и проведении работ по обеспечению безопасности конфиденциальной информации при их автоматизированной обработке в информационных системах» и является руководящим документом для всех сотрудников МБОУ Лицей г. Бирска (далее- учреждение). Требования настоящего порядка технического обслуживания и ремонта должны выполняться во всех режимах функционирования автоматизированной системы.

Техническое обслуживание и ремонтные работы на технических средствах ПЭВМ должны осуществляться только уполномоченными сотрудниками, назначенными ответственными за их обслуживание (сопровождение). Их вызов осуществляется сотрудниками подразделения, эксплуатирующего ПЭВМ, при возникновении нештатных ситуаций.

К нештатным ситуациям относятся:

- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (например, дисковод, принтера);
- выход из строя системы электроснабжения РС.

Техническое обслуживание и регламентные работы могут проводиться в плановом порядке. В этом случае работы проводятся на основании утвержденных руководством и согласованных с ответственным за обеспечение безопасности заявок.

Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на ПЭВМ возлагается на администратора безопасности.

Уполномоченные сотрудники (администратор) имеют право доступа к ПЭВМ для разбора нештатных ситуаций при обнаружении сбоев в их работе для тестирования ПЭВМ с использованием, установленных на ПЭВМ (в сети) тестовых средств.

О факте выполнения данных работ уполномоченный сотрудник (администратор) делает соответствующую отметку в «Журнале учета нештатных ситуаций...» с указанием признаков проявления ситуации и содержания выполненных работ по ее устранению.

При необходимости осуществления изменений аппаратно-программной конфигурации ПЭВМ соответствующие работы выполняются с соблюдением требований «Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы... ».

ПОРЯДОК
проверки работоспособности системы защиты после установки (обновления)
программных средств ас и внесения изменений в списки пользователей

Настоящий порядок проверки работоспособности разработан в дополнение к Положению «Об организации и проведении работ по обеспечению безопасности конфиденциальной информации при их автоматизированной обработке в информационных системах» и является руководящим документом для всех сотрудников МБОУ Лицей г. Бирска (далее- учреждение). Требования настоящего порядка проверки работоспособности должны выполняться во всех режимах функционирования автоматизированной системы.

После установки (обновления) программных средств ПЭВМ или внесения изменений в списки пользователей системы администратор СЗИ НСД обязан проверить работоспособность ПЭВМ и правильность настройки средств защиты, установленных на компьютере.

При установке нового (обновлении существующего) программного средства администратор безопасности обязан:

- установить права доступа пользователей системы к файлам программного средства таким образом, как это указано в формуляре на программное средство (задачу);

- средствами системы СЗИ НСД и (или) сертифицированными программными средствами подсчитать контрольные суммы файлов программных средств (при наличии указаний в формуляре);

- если для пользователя, использующего установленное программное средство, установлен режим замкнутой программной среды, необходимо средствами системы СЗИ НСД добавить в список разрешенных ему для запуска программ исполняемые модули данного пакета.

После осуществления данных действий необходимо проверить корректность функционирования системы защиты, для чего требуется произвести следующие действия:

- для каждого пользователя ПЭВМ, для которого установлен режим замкнутой программной среды, требуется проверить работоспособность установленного программного средства и сохранение режима замкнутой программной среды;

- в режиме обычного пользователя необходимо проверить возможность удаления вновь установленных (обновленных) файлов.

ЛИСТ

ознакомления с инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированных систем

[illegible]