МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ГИМНАЗИЯ №42»

ИНСТРУКЦИЯ

о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав автоматизированной системы МБОУ «Гимназия №42»

Перечень использованных сокращений, единиц и терминов

АС	–	автоматизированная система
АСО	–	активное сетевое оборудование
АРМ	–	автоматизированное рабочее место
АЭД	–	архив эталонных дистрибутивов
ИБ	–	информационная безопасность
ИС	–	информационная система
ИТ (IT)	–	информационные технологии
КИС	–	корпоративная информационная система
КИ	–	конфиденциальная информация
ЛВС	–	локальная вычислительная сеть
НСД	–	несанкционированный доступ
АИБ	–	администратор информационной безопасности
ПК	–	персональный компьютер
ПО	–	программное обеспечение
ПЭВМ	–	персональная электронная вычислительная машина
СБ	–	служба безопасности
СЗИ	–	средства защиты информации
СУБД	–	система управления базами данных
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю
ЭД	–	эксплуатационная документация

Администратор информационной безопасности – сотрудник МБОУ «Гимназия №42», который выполняет функции администратора информационной безопасности.

1. Введение.

1.1. Данная инструкция регламентирует взаимодействие структурных подразделений Полное Муниципальное Бюджетное Общеобразовательное Учреждение «Гимназия №42» (далее - МБОУ «Гимназия №42) по вопросам обеспечения безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники и при возникновении нештатных ситуаций в работе АС.

2. Порядок внесения изменений в конфигурации технических и программных средств АС МБОУ «Гимназия №42».

2.1. Права и обязанности структурных подразделений МБОУ «Гимназия №42» **по внесению изменений в конфигурацию технических и программных средств АС.**

2.1.1. Все изменения должны производиться только на основании заявок начальников структурных подразделений МБОУ «Гимназия №42» согласованных с администратором информационной безопасности. Перечень изменений, на которые требуется оформление заявки, приведен в пункте 2.2.3. настоящей инструкции.

2.1.2. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций и серверов АС предоставляется системному администратору, программисту, ответственному за информатизацию:

- в отношении системных и прикладных программных средств;
- в отношении аппаратных средств;
- в отношении программно-аппаратных средств;
- в отношении программно-аппаратных средств телекоммуникации;

Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме системномного администратора, программиста, ответственного за информатизацию, **ЗАПРЕЩЕНО**.

2.2. Порядок оформления заявок.

2.2.1. Процедура внесения изменений в конфигурацию аппаратных и программных средств серверов и рабочих станций инициируется заявкой ответственному по информатизации. Форма заявки приведена в Приложении 1.

2.2.2. Заявка на изменение конфигурации АРМ, оформляется на ответственного по информатизации.

2.2.3. В заявках могут быть указаны следующие изменения в составе аппаратных и программных средств АРМ и серверов подразделения:

- установка в подразделении новой ПЭВМ (развертывание новой АРМ или сервера);
- замена ПЭВМ (АРМ или сервера подразделения);
- изъятие ПЭВМ (АРМ или сервера подразделения);
- добавление устройства (узла, блока) в состав конкретного АРМ или сервера подразделения;
- замена устройства (узла, блока) в составе конкретного АРМ или сервера подразделения;
- изъятие устройства (узла, блока) из состава конкретного АРМ или сервера;
- обновление (восстановление) системного ПО;
- установка (развертывание) на конкретное АРМ или сервера программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данном АРМ или сервере), за исключением офисного ПО.

В заявке указываются условные наименования развернутых АРМ и серверов в соответствии с их формулярами. В случае развертывания нового АРМ его наименование в заявке указывать не

требуется (оно устанавливается позднее при заполнении формуляра нового АРМ). Наименования задач указываются в соответствии с формулярами задач или перечнем задач архива эталонных дистрибутивов, которые можно решать с использованием АС.

2.2.4. Заключение о технической возможности осуществления затребованных изменений выдается системным администратором (на основании формуляров задач и формуляров, соответствующих АРМ или серверов).

Заключение о возможности совмещения решения новых задач (обработки информации) на указанных в заявке АРМ или серверах в соответствии с требованиями по безопасности выдается администратором информационной безопасности, которому заявка передается на согласование (одновременно с этим производится определение новых категорий защищенности указанных АРМ или серверов).

После этого заявка передается системному администратору для непосредственного исполнения работ по внесению изменений в конфигурацию АРМ или серверов АС.

2.3. Порядок производства работ.

2.3.1. Руководитель структурного подразделения МБОУ «Гимназия №42»_рп допускает уполномоченных исполнителей к внесению изменений в состав аппаратных средств и программного обеспечения только по предъявлении ими утвержденной заявки на осуществление данных изменений.

2.3.2. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится уполномоченными специалистами. Если АРМ или сервер относится к защищаемым рабочим станциям, то установка, снятие, и внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов (при их использовании) на АРМ осуществляется администратором информационной безопасности. В случае необходимости работы производятся в присутствии пользователя данной АРМ.

2.3.4. Подготовка модификаций программного обеспечения защищенных серверов и АРМ, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов МБОУ «Гимназия №42» и другие необходимые действия производятся сотрудниками, согласно утвержденным инструкциям.

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

2.3.5. Модификация ПО серверов осуществляется системным администратором. При использовании СЗИ, после установки модифицированных модулей на сервер администратор информационной безопасности устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью средств СЗИ).

2.3.6. Установка и обновление общего ПО (системного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, а прикладного ПО - с эталонных копий программных средств (при реализации сетевого архива эталонных дистрибутивов программ – из него).

Все добавляемые программные и аппаратные компоненты должны быть установленным порядком предварительно проверены на работоспособность.

2.3.7. После установки (обновления) ПО администратор информационной безопасности должен произвести настройку СЗИ от НСД в соответствии с ее (его) формуляром. Настройка должна осуществляться совместно ответственным пользователем АРМ. Администратор информационной безопасности должен проверить работоспособность ПО и правильность настройки средств защиты.

После завершения работ по внесению изменений в состав аппаратных средств защищаемой АРМ ее системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) администратором информационной безопасности.

2.3.8. Исполнители работ должны сделать соответствующую запись в формуляре АРМ, отметку о выполнении (на обратной стороне заявки) и передать исполненную заявку директору.

2.3.9. Изъятие АРМ из состава рабочих станций подразделения при ее передаче на склад, в ремонт или в другое подразделение осуществляется только после того, как администратор информационной безопасности снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для удаления защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью *ответственный за информатизацию*. Форма Акта приведена в Приложении 2.

2.3.10. Допуск новых пользователей к решению задач с использованием вновь установленного ПО (либо изменение их полномочий доступа) осуществляется согласно «Политике предоставления доступа к информационному ресурсу».

2.3.11. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств АРМ с отметками о внесении изменений в состав аппаратно-программных средств, должны храниться у директора. Они могут использоваться в следующих случаях:

– для восстановления конфигурации АРМ после аварий;

– для контроля правомерности установки на конкретной АРМ средств для решения соответствующих задач при разборе конфликтных ситуаций;

– для проверки правильности установки и настройки средств защиты АРМ.

2.3.12. Регулярные и внеплановые проверки на исправность и техническое обслуживание технических средств и средств защиты отражать в «Журнал проверки исправности и технического обслуживания».

3. Экстренная модификация (обстоятельства форс-мажор).

3.1. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на рабочей станции. В данной ситуации сотрудник отдела Наименование отдела_рп ставит в известность своего начальника о необходимости такого изменения.

3.2. Факт внесения изменений в ПО АРМ оформляется актом за подписями ответственного за информатизацию и пользователя данной АРМ. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), осуществившее изменения. При необходимости проводится изменение ПО загрузочного раздела сервера. Если это необходимо, администратор информационной безопасности вносит необходимые корректировки в настройки системы контроля целостности ПО АРМ и сервера (при их использовании). Факт модификации ПО и корректировок настроек системы защиты фиксируется на АРМ (сервере).

3.3. В течение следующего дня после составления акта, администратор информационной безопасности при участии сотрудников подразделения выясняют причины и состав проведенных экстренных изменений и принимают решение о необходимости подготовки исправительной модификации ПО или восстановления ПО АРМ (сервера) с эталонной копии (из АЭД).

4. Порядок технического обслуживания и ремонта технических средств АРМ (серверов) АС.

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

4.2. К нештатным ситуациям относятся:

– выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (например, дисковода, принтера) АРМ;

– выход из строя системы электроснабжения АРМ.

4.3. Техническое обслуживание и регламентные работы могут проводиться в плановом порядке.

Уполномоченные сотрудники имеют право доступа к АРМ для разбора нештатных ситуаций без участия администратора информационной безопасности при обнаружении сбоев в их работе только для тестирования ПЭВМ с использованием установленных на АРМ (в сети) тестовых средств.

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

4.5. При необходимости осуществления изменений аппаратно-программной конфигурации АРМ соответствующие работы выполняются с соблюдением требований данной инструкции.

5. Порядок проверки работоспособности системы защиты после установки (обновления) программных средств внесения изменений в списки пользователей.

После установки (обновления) программных средств АРМ или внесения изменений в списки пользователей системы администратор информационной безопасности обязан проверить работоспособность АРМ и правильность настройки средств защиты, установленных на компьютере в соответствии с инструкциями на конкретные СЗИ.

После осуществления данных действий необходимо проверить корректность функционирования системы защиты.

Приложение 1

Резолюция

«___» _____ 200_ г.

ЗАЯВКА
на внесение изменений в состав аппаратно-программных средств АС

Прошу произвести следующие изменения конфигурации аппаратно-программных средств ПЭВМ_____
_____
(наименование подразделения)
(развернуть новую рабочую станцию и установить на (обновить на/снять с) нее _____ компоненты), необходимые для решения следующих задач:
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Начальник _____
(наименование структурного подразделения)

«___» _____ 200__ г. _____ _____
(подпись) (фамилия и инициалы)

Согласовано _____*Должность, отдел_рд*_____

«___» _____ 200__ г. _____ _____
(подпись) (фамилия и инициалы)

Обратная сторона заявки

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 АРМ *Наименование системы* рабочей группой в составе:

от ____________________________

____

от подразделения (отдела) ____

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

____

краткое пояснение причины

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

________Изменения в формуляр АРМ (ссылка на данную заявку) внесены.

От подразделения _____________________

____

(подпись, фамилия)

«___» _______________ 200__ года

От _______________________

____

(подпись, фамилия)

«___» _______________ 200__ года

Приложение 2

Утверждаю
Ответственный за информатизацию
_____ _____

«___» _____ 200_ г.

АКТ

об удалении остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД №_____, передаваемого
_____
(с какой целью)

_____
(Кому: должность, Ф.И.О.)

системного блока ПЭВМ марки _____ серийный №_____
уничтожены (затерты) посредством программы
_____

Аадминистратор информационной безопасности
_____
(Ф.И.О.)

_____ _____
(Подпись) (Дата)