Некоммерческая организация Межрегиональная ассоциация
«Центр дополнительного образования «Лидер»

УТВЕРЖДАЮ
Директор Центра «Лидер»
_____
Н. А. Бабиева
«11» января 2010 г.

С Б О Р Н И К И Н С Т Р У К Ц И Й

по обеспечению безопасности информационной системы Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер»

Ставрополь, 2010

Оглавление

И Н С Т Р У К Ц И Я

оператора информационной системы Центра «Лидер» по обеспечению безопасности защищаемой информации

1. Общие положения

1.1. Инструкция оператора по обеспечению безопасности информационной системы Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящая Инструкция определяет требования по организации порядка работы оператора в информационной системе Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер») с целью обеспечения безопасности информационных ресурсов Центра.

1.3. Оператор информационной системы Центра «Лидер» (далее – Оператор) осуществляет обработку персональных данных в информационной системе персональных данных.

1.4. Оператором является каждый сотрудник Центра «Лидер», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной или неавтоматизированной обработки информации и имеющий доступ к персональным данным, аппаратным средствам, программному обеспечению, средствам защиты.

1.5. Оператор несет персональную ответственность за свои действия.

1.6. Оператор в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами ФСТЭК России, регламентирующими документами Центра «Лидер» по защите информации.

1.7. Методическое руководство работой Оператора осуществляется ответственным за обеспечение информационной безопасности.

1.8. Непосредственную ответственность за надлежащее выполнение инструкции всеми сотрудниками Центра «Лидер» несет директор Центра.

1.9. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Лидер» и не исключает обязательного выполнения их требований.

1.10. Ознакомление сотрудников с настоящей инструкцией осуществляется под роспись по форме согласно Приложению.

1.11. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Должностные обязанности

Оператор обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены функциональными обязанностями.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.5. Надежно хранить и никому не передавать номерную печать и использовать ее только для опечатывания помещения.

2.6. При отсутствии визуального контроля за рабочей станцией блокировать доступ к компьютеру.

2.7. В случае возникновения внештатных или аварийных ситуаций в рамках возложенных функций принимать меры по ликвидации их последствий.

2.8. Обо всех выявленных нарушениях, связанных с информационной безопасностью Центра «Лидер», а так же для получений консультаций по вопросам информационной безопасности, обращаться к ответственному за информационную безопасность.

2.9. Для получения консультаций по вопросам работы и настройке элементов ИСПДн обращаться к Администратору информационной безопасности.

Оператору запрещается:

2.10. Разглашать защищаемую информацию третьим лицам.

2.11. Использовать компоненты программного и аппаратного обеспечения информационной системы Центра «Лидер» в неслужебных целях.

2.12. Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

2.13. Самостоятельно устанавливать, тиражировать, или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.14. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

2.15. Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

2.16. Отключать (блокировать) средства защиты информации.

2.17. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав Оператора по доступу к ИСПДн.

2.18. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.19. Записывать и хранить информацию, содержащую сведения ограниченного распространения, на неучтенных носителях информации.

2.20. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

2.21. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение информационной безопасности.

3. Организация парольной защиты

3.1. Работа Оператора с паролями должна осуществляться в соответствии с Инструкцией по организации парольной защиты.

3.2. Личный пароль доступа к элементам ИСПДн формируется Оператором самостоятельно.

3.3. Полная плановая смена паролей проводится не реже одного раза в год.

3.4. Правила ввода пароля:

– Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

– Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

− Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

− Запрещается сообщать другим лицам личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны своевременно сообщать ответственному за информационную безопасность об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего пользования

4.1. Работа в сетях общего пользования Оператора ИСПДн должна осуществляться в соответствии с Инструкцией по обеспечению защиты информации при взаимодействии пользователей с информационными сетями общего пользования.

4.2. При работе в Сети запрещается:

− осуществлять работу при отключенных средствах защиты (антивирус и других);

− передавать по Сети защищаемую информацию без использования средств защиты каналов связи;

− посещать сайты, содержание которых не связано с выполняемыми Оператором функциональными обязанностями.

И Н С Т Р У К Ц И Я

об охранном режиме помещений Центра «Лидер»

1. Общие положения

1.1. Инструкция об охранном режиме помещения (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ "О персональных данных".

1.2. Инструкция разработана в целях упорядочения организации работы по охране помещения Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер»).

1.3. Охранный режим Центра «Лидер» обеспечивается комплексом мер по обеспечению помещений Центра средствами охранной сигнализации, физической охраной после окончания рабочего дня, опечатыванию помещений, хранению ключей от помещения и номерных печатей.

1.4. Непосредственную ответственность за надлежащее обеспечение охранного режима несет директор Центра «Лидер».

1.5. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Лидер» и не исключает обязательного выполнения их требований.

1.6. Ознакомление сотрудников с настоящей инструкцией осуществляется под роспись по форме согласно приложению.

1.7. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Учет и хранение ключей и номерных печатей

2.1. Замки дверей помещений и кабинетов должны иметь рабочие и запасные экземпляры ключей.

2.2. Запасные экземпляры ключей от помещений, в которых находится защищаемая информация, должны храниться в опечатанных конвертах в сейфе ответственного за обеспечение мероприятий по защите персональных данных субъектов Центра «Лидер».

2.3. Запасные экземпляры ключей от прочих помещений хранятся у заместителя директора по АХЧ.

2.4. Рабочие экземпляры ключей от помещений, в которых находится защищаемая информация, в нерабочее время хранятся у сотрудников Центра «Лидер», определенных приказом директора.

2.5. Рабочие экземпляры ключей от прочих помещений в нерабочее время хранятся на стенде в кабинете секретаря или на рабочем месте администратора Центра «Лидер».

2.6. Наличие неучтенных ключей от помещений, в которых находится защищаемая информация, недопустимо.

2.7. Все экземпляры ключей от защищаемых помещений учитываются в журнале регистрации ключей к замкам помещений. В указанном журнале отмечается ФИО работников, имеющих ключи от каждого из помещений, с распиской работника в получении экземпляра ключа.

2.8. В случае утраты рабочих или запасных экземпляров ключей от защищаемых помещений об этом немедленно ставиться в известность ответственного за обеспечение мероприятий по защите персональных данных субъектов Центра «Лидер».

2.9. Выдача номерных печатей должностным лицам, определенным приказом директора, производится под расписку в специальном журнале.

2.10. Должностные лица, имеющие номерные печати и ключи от защищаемых помещений, несут персональную ответственность за их сохранность.

2.11. Регулярно должна проводиться проверка фактического наличия ключей от помещений и номерных печатей.

2.12. Список должностных лиц, осуществляющих сдачу помещения под охрану, его опечатывания и вскрытия, утверждается приказом директора Центра «Лидер».

3. Порядок сдачи помещений под охрану, их опечатывания и снятия с охраны

3.1. Должностные лица, осуществляющие сдачу помещений под охрану и их опечатывание:

– перед закрытием проверяют работоспособность средств охранной сигнализации. При обнаружении неисправности информируют руководство и не покидают помещение до устранения неисправности и передачи помещения под охрану;

– в конце рабочего дня проверяют, чтобы в помещении не остались сотрудники, были выключены источники света, закрыты все форточки, закрыты (при необходимости опечатаны) двери кабинетов, затем закрывают и опечатывают помещение;

– печать проставляется на тонкий слой пластилина или специальной мастики таким образом, чтобы оттиск невозможно было снять и восстановить;

– хранят и несут ответственность за сохранность ключей и номерных печатей;

– в случае срабатывания сигнализации в нерабочее время по вызову службы охраны прибывают для осмотра помещения и передачи его под охрану.

3.2. При снятии помещения с охраны или открытия опечатанных помещений ответственные должностные лица:

– проверяют целостность печатей на дверях и замках;

− при обнаружении повреждения замков, дверей и т.д., не вскрывая помещения, вызывают представителей органа охраны и руководство Центра «Лидер» для составления акта в установленном порядке.

И Н С Т Р У К Ц И Я
о порядке доступа к персональным данным и иной конфиденциальной информации, обрабатываемой в информационной системе персональных данных «ASTRA» Центра «Лидер»

1. Общие положения

1.1. Инструкция о порядке доступа к персональным данным и иной конфиденциальной информации, обрабатываемой в информационной системе персональных данных «Astra» Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящая Инструкция определяет порядок доступа к персональным данным и иной конфиденциальной информации, обрабатываемой в информационной системе персональных данных «Astra» в Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер»), и устанавливает основные права и обязанности пользователей при работе с персональными данными.

1.3. Перечень персональных данных и иной конфиденциальной информации, обрабатываемой в информационной системе персональных данных «Astra», и изменения к нему утверждаются директором Центра «Лидер».

1.4. Защита информации осуществляется подсистемой обеспечения информационной безопасности, представляющей собой комплекс программно-технических средств и организационных мер защиты информации от несанкционированного изменения или доступа к ней.

1.5. Управление подсистемой обеспечения информационной безопасности и организацию обеспечения доступа к персональной информации осуществляет администратор информационной безопасности, утверждённый приказом директора Центра «Лидер».

1.6. Методическое руководство работой пользователя в информационной системе персональных данных «Astra» осуществляется администратором информационной безопасности.

1.7. Непосредственную ответственность за надлежащее выполнение Инструкции всеми сотрудниками Центра «Лидер» несет директор Центра.

1.8. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Лидер» и не исключает обязательного выполнения их требований.

1.9. Ознакомление сотрудников с настоящей Инструкцией осуществляется под роспись по форме согласно приложению.

1.10.Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Организация доступа к защищаемой информации автоматизированной системы «Astra»

2.1. Доступ к защищаемой информации предоставляется пользователям администратором, обеспечивающим эксплуатацию информационной системы персональных данных «Astra», по списку пользователей, допущенных к работе с защищаемой информацией, обрабатываемой в комплексах средств автоматизации Центра «Лидер».

2.2. На основании списка администратор информационной системы персональных данных «Astra» разрабатывает матрицу разграничения доступа к

защищаемой информации, обрабатываемой в комплексах средств автоматизации Центра «Лидер».

2.3. Матрица доступа составляется как на электронном, так и на бумажном носителях. На бумажном носителе матрица доступа составляется в двух экземплярах: подлинник (контрольный экземпляр) и рабочий экземпляр.

2.4. Администратор информационной системы персональных данных «Astra» на основании матрицы доступа предоставляет пользователям доступ к информационным ресурсам Центра «Лидер» и проверяет на автоматизированном рабочем месте пользователя (далее – АРМ) заданные возможности доступа.

2.5. Администратор информационной системы персональных данных «Astra», иные пользователи информационной системы персональных данных «Astra», имеют право предоставлять защищаемую информацию только лицам, имеющим право получать указанные сведения.

3. Обязанности пользователей, допущенных к защищаемой информации автоматизированной системы «Astra»

3.1.Лица, допущенные к защищаемой информации, обязаны:

- не сообщать защищаемую информацию лицам, не имеющим права доступа к ней;
- обеспечивать сохранность материалов с защищаемой информацией;
- не делать неучтенных копий на бумажных и электронных носителях;
- не оставлять включенными АРМ с предоставленными правами доступа, после окончания работы (в перерывах) не оставлять материалы с защищаемой информацией на рабочих столах. Покидая рабочее место, пользователь обязан убрать документы и электронные носители с защищаемой информацией в закрываемые на замок сейфы, шкафы, столы, и т.п.;

– при работе с документами, содержащими защищаемую информацию, исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;

– не выносить документы и иные материалы с защищаемой информацией, а также их копии из служебных помещений, предназначенных для работы с ними;

– не вносить изменения в настройку средств защиты информации в строгом соответствии с эксплуатационной документацией;

– немедленно сообщать администратору информационной безопасности об утрате, утечке или искажении защищаемой информации, об обнаружении неучтенных материалов с указанной информацией;

– не допускать действий, способных повлечь утечку защищаемой информации;

– предъявлять для проверки лицам, наделенным необходимыми полномочиями в соответствии с законодательством Российской Федерации, по их требованию все числящиеся и имеющиеся в наличии документы с защищаемой информацией.

4. Порядок доступа пользователей к защищаемым информационным ресурсам автоматизированной системы «Astra»

4.1. Центр «Лидер» предоставляет Пользователю право авторизованного доступа к информационной системе «Astra» и ко всем её разделам.

4.2. Право доступа к защищаемым ресурсам информационной системы «Astra», содержащей персональные данные, имеют Пользователи, чьи функциональные обязанности предполагают работу с персональными данными.

4.3. Авторизованный доступ Пользователей к защищаемым ресурсам информационной системы «Astra» осуществляется на основании приказа директора Центра «Лидер».

И Н С Т Р У К Ц И Я

по организации антивирусной защиты автоматизированной системы Центра «Лидер»

1. Общие положения

1.1. Инструкция по организации антивирусной защиты автоматизированной системы (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер») с целью предотвращения заражения компьютерными вирусами информационных ресурсов Центра.

1.3. Настоящая Инструкция определяет требования к организации защиты автоматизированной системы (далее – АС) Центра «Лидер» от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей, работников, эксплуатирующих автоматизированные рабочие места (далее – АРМ), и сопровождающих АС, за её выполнение.

1.4. Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему АРМ при выполнении работ в АС.

1.5. Техническое обслуживание средств вычислительной техники проводится сотрудниками, ответственными за техническое обслуживание компьютерной техники (далее – уполномоченными сотрудниками).

1.6. Непосредственную ответственность за надлежащее выполнение Инструкции всеми пользователями АС Центра «Лидер» несет директор Центра.

1.7. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Лидер» и не исключает обязательного выполнения их требований.

1.8. Ознакомление сотрудников с настоящей Инструкцией осуществляется под роспись по форме согласно приложению.

1.9. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Установка антивирусного программного обеспечения

2.1. К использованию в Центре допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

2.2. Установка антивирусного ПО осуществляется уполномоченными сотрудниками Центра в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств» индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

2.3. Настройка параметров средств антивирусного контроля осуществляется уполномоченными сотрудниками Центра в соответствии с руководствами по применению конкретных антивирусных средств.

2.4. Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.

2.5. Ярлык для запуска антивирусного ПО должен быть вынесен на "Рабочий стол" операционной системы или на панель быстрого запуска.

3. Применение средств антивирусного контроля

3.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме.

3.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных, лазерных дисках, USB флеш-накопителях, SSD-накопителях и т.п.).

3.3. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема.

3.4. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3.6. Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

3.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

3.8. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на защищаемых серверах и АРМ уполномоченными сотрудниками Центра.

3.9. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение.

4. Порядок обновления антивирусных баз

4.1. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети Центра, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений.

4.2. Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети Центра, должно осуществляться с использованием маркированных съемных носителей информации, в обязательном порядке проверяемых антивирусным ПО перед их использованием или принудительным подключением к локальной сети.

4.3. Проверка критических областей защищаемого компьютера, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

4.4. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети, контролируется пользователем самостоятельно ежедневно. В случае нарушения актуализации пользователь, не предпринимая самостоятельно никаких мер, должен сообщить об этом ответственному за информационную безопасность или уполномоченному сотруднику Центра.

5. Действия при обнаружении вирусов

5.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь или уполномоченный сотрудник должен провести внеочередной антивирусный контроль рабочей станции.

5.2. В случае обнаружения файлов, зараженных компьютерными вирусами, работник Центра обязан:

- приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом ответственного за техническое обслуживание компьютерной техники специалиста Центра, владельца зараженных файлов, а также других работников, использующих эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов самостоятельно или вместе с уполномоченным сотрудником.

6. Ответственность

6.1. Ответственность за организацию антивирусной защиты АС Центра возлагается на ответственного за обеспечение безопасности информации.

6.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями АС.

6.3. Периодический контроль за состоянием антивирусной защиты и за соблюдением установленного порядка антивирусного контроля сотрудниками Центра осуществляется ответственным за обеспечение безопасности информации.

И Н С Т Р У К Ц И Я

по обеспечению защиты информации при взаимодействии пользователей Центра «Лидер» с информационными сетями общего пользования

1. Общие положения

1.1. Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ "О персональных данных".

1.2. Инструкция по обеспечению защиты информации, содержащейся в информационных ресурсах Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер»), при взаимодействии пользователей с информационными сетями общего пользования (далее – Инструкция) определяет условия и порядок подключения рабочих станций Центра «Лидер» к информационным сетям общего пользования (далее – Сетям), а также мероприятия по обеспечению безопасности информации, содержащейся в информационных ресурсах Центра «Лидер», при подключении и взаимодействии пользователей с этими сетями.

1.3. Положения Инструкции определены, исходя из следующих основных угроз безопасности информации, возникающих при взаимодействии с информационными сетями общего пользования:

– несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних локальных вычислительных сетях (серверах, рабочих станциях) или на автономных рабочих станциях, как из Сетей, так и из внутренних локальных вычислительных сетей (далее – ЛВС);

– несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, серверу, Web/Proxy серверу), соединяющему внутренние ЛВС Центра «Лидер» с Сетями;

– несанкционированного доступа к данным, передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;

– заражения программного обеспечения компьютерными "вирусами" из Сети, как посредством приема "зараженных" файлов, так и посредством E-mail;

– внедрения программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;

– несанкционированной передачи защищаемой информации из ЛВС в Сеть.

1.4. Непосредственную ответственность за надлежащее выполнение Инструкции всеми сотрудниками Центра «Лидер» несет директор Центра.

1.5. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Лидер» и не исключает обязательного выполнения их требований.

1.6. Ознакомление сотрудников с настоящей Инструкцией осуществляется под роспись по форме согласно приложению.

1.7. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Условия подключения абонентов к Сети

2.1. Подключение к Сети рабочей станции осуществляется по решению директора Центра «Лидер» на основании наличия функциональных обязанностей, требующих подобного подключения.

2.2. Подключение к Сети рабочей станции, осуществляющей обработку информации с открытым доступом, может осуществляться без оборудования средствами защиты информации от НСД.

2.3. Подключение к Сети рабочих станций, на которых обрабатывается информация, не разрешенная к открытому опубликованию, осуществляется только после установки на них средств защиты информации от НСД.

3. Порядок подключения и взаимодействия пользователей с Сетью

3.1. Подключение рабочей станции к Сети должно осуществляться в установленном порядке через провайдера Сети.

3.2. Подключение локальной вычислительной сети Центра «Лидер» к Сети должно осуществляться через средства разграничения доступа в виде межсетевых экранов. Не допускается подключение ЛВС к Сети в обход межсетевых экранов (далее – МЭ).

3.3. Доступ к МЭ, к средствам его конфигурирования может осуществляться только администратором информационной безопасности.

3.4. На технических средствах рабочих станций должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в функциональных обязанностях сотрудника Центра.

3.5. Установку программного обеспечения, обеспечивающего функционирование рабочей станции, могут выполнять только уполномоченные специалисты Центра «Лидер» или специалисты сторонних организаций под контролем администратора информационной безопасности.

3.6. Пользователи рабочих станций не имеют права производить самостоятельную установку и модификацию программного обеспечения, однако могут обращаться к администратору для проведения его экспертизы на предмет улучшения характеристик, наличия "вирусов", замаскированных возможностей выполнения непредусмотренных действий.

3.7. Ответственность за установку на рабочей станции программ, не включенных в состав рекомендованного к использованию программного обеспечения, целиком ложится на пользователя.

3.8. При обнаружении фактов использования произвольных программ, не включенных в состав рекомендованного к использованию на рабочей станции программного обеспечения, администратор обязан отключить рабочую станцию от Сети и ЛВС и поставить об этом в известность ответственного за обеспечение мероприятий по защите персональных данных субъектов Центра «Лидер».

3.9. Средства защиты информации, устанавливаемые на автономные ПЭВМ, рабочие станции и серверы внутренней ЛВС при обработке на них защищаемой информации, должны осуществлять идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;

3.10. Модификация конфигурации программного обеспечения рабочей станции должна быть доступна только со стороны администратора информационной безопасности.

3.11. Средства регистрации и регистрируемые данные должны быть недоступны для пользователя.

3.12. Web-серверы, почтовые серверы должны размещаться в отдельном защищаемом помещении, доступ в которое имеет ограниченный круг лиц, определенный приказом директора Центра «Лидер».

3.13. При предоставлении пользователям прикладных сервисов следует исходить из принципа минимальной достаточности. Тем пользователям, которым не требуются услуги Сети, не предоставлять их. Пользователям, которым необходима только электронная почта, предоставлять только доступ к ней. Максимальный перечень предоставляемых прикладных сервисов ограничивать E-mail, FTP, HTTP, Telnet.

3.14. Эффективно использовать имеющиеся в маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа.

3.15. К работам в Сети с соответствующими полномочиями допускаются сотрудники, ознакомленные с требованиями по взаимодействию с другими абонентами Сети.

3.16. Абоненты Сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;
- знать правила работы со средствами защиты информации, установленными на рабочих станциях;
- уметь пользоваться средствами антивирусной защиты.

3.17. При работе в Сети пользователю категорически запрещается:

- подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;
- изменять состав и конфигурацию программных и технических средств рабочей станции;
- производить отправку защищаемых данных без соответствующего разрешения.

3.18. Ведение учета пользователей, подключенных к Сети, осуществляется администратором информационной безопасности Центра «Лидер».

3.19. Администратор информационной безопасности обязан контролировать использование ресурсов Сети сотрудниками Центра «Лидер» и вносить предложения об изменении списка доступных ресурсов.

3.20. Доступ к ресурсам Сети может быть блокирован администратором информационной безопасности без предварительного уведомления, при возникновении нештатных ситуаций, либо в иных случаях предусмотренных организационными документами.

3.21. Контроль за выполнением мероприятий по обеспечению безопасности информации на рабочих станциях возлагается на администратора информационной безопасности.

4. Работа с корпоративной электронной почтой

4.1. Электронная почта является собственностью компании и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

4.2. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

4.3. Доступ к серверу электронной почты может быть блокирован администратором информационной безопасности без предварительного уведомления, при возникновении нештатных ситуаций, либо в иных случаях предусмотренных организационными документами.

4.4. При работе с корпоративной системой электронной почты запрещается:

- использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с администратором информационной безопасности;
- публиковать свой адрес, либо адреса других сотрудников компании в открытом доступе;
- отправлять сообщения с вложенными файлами, общий объем которых превышает 5 Мегабайт;
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами;
- осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с администрацией Центра «Лидер»;
- рассылать материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или

телекоммуникационного оборудования, программы для осуществления несанкционированного доступа;

– рассылать серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Сети, а также ссылки на вышеуказанную информацию;

– распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

– распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством;

– распространять информацию ограниченного доступа;

– предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.

И Н С Т Р У К Ц И Я

по организации парольной защиты автоматизированной системы Центра «Лидер»

1. Общие положения

1.1. Инструкция по организации парольной защиты автоматизированной системы Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер»), а также контроль за действиями пользователей системы при работе с паролями.

1.3. Непосредственную ответственность за надлежащее выполнение инструкции всеми сотрудниками Центра «Лидер» несет директор Центра.

1.4. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Лидер» и не исключает обязательного выполнения их требований.

1.5. Ознакомление сотрудников с настоящей инструкцией осуществляется под роспись по форме согласно приложению.

1.6. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Генерация и смена паролей

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированной системы (далее – АС) Центра «Лидер», контроль за действиями пользователей системы при работе с паролями возлагается на администратора информационной безопасности.

2.2. Личные пароли пользователей АС должны генерироваться и распределяться централизованно, либо выбираться пользователями самостоятельно с учетом следующих требований:

– Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

– Пароль должен состоять не менее чем из 6 символов.

– В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

– Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации об Операторе.

– Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

– Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

– Запрещается выбирать пароли, которые уже использовались ранее.

– При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

2.3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

2.4. Для генерации паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления ответственных за информационную безопасность с паролями других сотрудников Центра «Лидер».

2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.

2.6. Внеплановая смена личного пароля или удаление учетной записи пользователя АС в случае прекращения его полномочий должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов информационной безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

2.8. В случае компрометации личного пароля, пользователь АС должен немедленно сообщить об этом администратору информационной безопасности.

3. Хранение паролей

3.1. Не допускается хранение паролей на бумажных носителях в зоне свободного доступа.

3.2. Хранение пользователем значений своих паролей на бумажном носителе допускается в сейфе у заместителя директора по информационным и коммуникационным технологиям.

3.3. Контроль за действиями пользователей АС при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора информационной безопасности.

И Н С Т Р У К Ц И Я

администратора информационной безопасности Центра «Лидер»

1. Общие положения

1.1. Инструкция администратора информационной безопасности (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ "О персональных данных".

1.2. Настоящая инструкция определяет функции, права и обязанности администратора информационной системы по вопросам обеспечения информационной безопасности при работе с персональными данными в информационной системе Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер») класса К2.

1.3. Администратор безопасности информации (далее – Администратор) назначается приказом директора Центра «Лидер» из числа сотрудников.

1.4. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Центра «Лидер».

1.5. Администратор обеспечивает правильность использования и нормальное функционирование установленных систем защиты информации.

1.6. Методическое руководство работой Администратора осуществляется директором Центра «Лидер».

1.7. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных и не исключает обязательного выполнения их требований.

1.8. Ознакомление сотрудников с настоящей инструкцией осуществляется под роспись по форме согласно приложению.

1.9. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Основные функции администратора безопасности

2.1. Обеспечение функционирования и поддержание работоспособности средств и систем защиты информации в пределах возложенных функций:

– установка, настройка и своевременное обновление элементов информационных систем;

– обеспечение работоспособности элементов ИСПДн и локальной вычислительной сети;

– контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных.

2.2. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в ИСПДн:

– реализация полномочий доступа для каждого пользователя к элементам защищаемых информационных ресурсов;

– ввод описаний пользователей информационных систем, используемых в Центре «Лидер», в информационную базу автоматизированной системы;

– своевременное удаление описаний пользователей из информационной базы автоматизированной системы при изменении списка лиц, допущенных к работе с информационными системами.

2.3. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

– введение в базу данных автоматизированной системы описания событий, подлежащих регистрации в системном журнале;

– регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

– своевременное информирование руководителя учреждения о несанкционированных действиях персонала и проведение расследования попыток несанкционированного доступа к информации.

2.4. Сопровождение подсистемы обеспечения целостности информации в ИСПДн:

– периодическое тестирование функций установленных средств защиты информации от НСД, особенно при изменении программной среды и полномочий исполнителей;

– проведение комплекса мероприятий по восстановлению работоспособности программной среды, программных средств и настроек средств защиты информации при сбоях;

– поддержание установленного порядка и правил антивирусной защиты информации в ИСПДн;

– периодическое обновление установленных антивирусных средств (баз данных);

– резервное копирование персональных данных на резервный накопитель;

– регулярный анализ защищённости ИСПДн.

3. Обязанности администратора безопасности

3.1. Знание и выполнение требований настоящей инструкции, действующих нормативных и руководящих документов, а также внутренних инструкций, положений по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.2. Ведение документации на ИСПДн в соответствии с требованиями нормативных документов.

3.3. Проведение инструктажа пользователей по правилам работы в ИСПДн.

3.4. Присутствие при выполнении технического обслуживания элементов ИСПДн сторонними физическими людьми и организациями.

3.5. Обобщение результатов своей деятельности и подготовка предложений по ее совершенствованию.

3.6. Анализ причин возникновения нарушений и принятие мер по предотвращению подобных нарушений в дальнейшем.

3.7. Своевременное сообщение директору Центра «Лидер» о неправомерных действиях пользователей, приводящих к нарушению требований по защите персональных данных.

3.8. Составление служебной записки на имя директора Центра «Лидер» по факту нарушения информационной безопасности с указанием причин нарушения и принятых мер.

4. Полномочия администратора безопасности

4.1. Требование от пользователей ИСПДн соблюдения установленных технологий обработки информации, выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн.

4.2. Контроль за выполнением работниками Центра «Лидер» требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты персональных данных при их обработке в ИСПДн.

4.3. Контроль доступа лиц в помещения, где установлены серверы, в соответствии со списком сотрудников, ответственных за техническое обслуживание компьютерной техники.

4.4. Контроль за регулярным проведением смены паролей доступа пользователями автоматизированной системы Центра «Лидер».

4.5. Контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования.

4.6. Прекращение обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4.7. Участие в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4.8. Инициирование проведения служебных проверок по фактам нарушения установленных требований обеспечения безопасности информации, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

4.9. Контроль монтажа оборудования учреждения специалистами сторонних организаций.

И Н С Т Р У К Ц И Я

по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы Центра «Лидер»

1. Общие положения

1.1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящая Инструкция регламентирует организацию мероприятий по обеспечению безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники и при возникновении нештатных ситуаций в работе автоматизированной системы Некоммерческой организации Межрегиональной ассоциации «Центр дополнительного образования «Лидер» (далее – Центр «Лидер»).

1.3. Непосредственную ответственность за надлежащее выполнение инструкции всеми сотрудниками Центра «Лидер» несет директор Центра.

1.4. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Лидер» и не исключает обязательного выполнения их требований.

1.5. Ознакомление сотрудников с настоящей инструкцией осуществляется под роспись по форме согласно приложению.

1.6. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Оформление заявок на изменения конфигурации

2.1. Все изменения конфигурации технических и программных средств рабочих станций и серверов АС Центра «Лидер» должны производиться только на основании заявок работников Центра «Лидер» (Приложение 1).

2.2. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций и серверов АС Центра «Лидер» предоставляется только сотрудникам, ответственными за техническое обслуживание компьютерной техники (далее – уполномоченным сотрудникам).

2.3. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме уполномоченных сотрудников, строго запрещено.

2.13. Заявка на изменения конфигурации рабочей станции оформляется на имя ответственного за обеспечение мероприятий по защите персональных данных субъектов Центра «Лидер».

2.4. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью ответственного за информационную безопасность Центра «Лидер».

2.5. В заявках могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств рабочих станций и серверов:

- установка в подразделении новой рабочей станции или сервера;
- замена рабочей станции или сервера;
- изъятие рабочей станции или сервера;

– добавление устройства (узла, блока) в состав конкретной рабочей станции или сервера;

– замена устройства (узла, блока) в составе конкретной рабочей станции или сервера;

– изъятие устройства (узла, блока) из состава конкретной рабочей станции или сервера;

– установка (развертывание) на конкретной рабочей станции или сервере программных средств, необходимых для решения определенной задачи;

– обновление (замена) на конкретной рабочей станции или сервере программных средств, необходимых для решения определенной задачи;

– удаление с конкретной рабочей станции или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи).

2.6. В заявке указываются инвентарные номера рабочих станций и серверов.

2.7. В случае развертывания новой рабочей станции ее наименование в заявке указывать не требуется.

2.8. Заключение о технической возможности осуществления затребованных изменений выдается специалистами по информационной безопасности на основании новых задач и технических возможностей соответствующих рабочих станций или серверов.

2.9. Заключение о возможности совмещения решения новых задач (обработки информации) на указанных в заявке рабочих станциях или серверах в соответствии с требованиями по безопасности выдается специалистами по информационной безопасности, которым заявка передается на согласование. Одновременно с этим производится определение новых категорий защищенности указанных рабочих станций или серверов.

2.10. После принятия решения о возможности осуществления новых задач на рабочих станциях или серверах заявка передается уполномоченному лицу для непосредственного исполнения работ по внесению изменений в их конфигурацию.

3. Изменения конфигурации технических и программных средств

3.1. Ответственный за информационную безопасность допускает уполномоченных специалистов сторонних организаций к внесению изменений в состав аппаратных средств и программного обеспечения только по предъявлении последними утвержденной заявки на осуществление данных изменений.

3.2. Установка, изменение (обновление) и удаление системных и прикладных программных средств рабочих станций и серверов производится уполномоченными сотрудниками Центра.

3.3. Если рабочая станция или сервер относится к защищаемым рабочим станциям, то установка, снятие и внесение необходимых изменений в настройки средств защиты и средств контроля целостности файлов осуществляется уполномоченными сотрудниками, ответственными за информационную безопасность.

3.4. После проведения модификации программного обеспечения на рабочих станциях уполномоченный сотрудник проводит антивирусный контроль.

3.5. Установка и обновление общего ПО (системного, тестового и т.п.) на рабочие станции и серверы производится с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств.

3.6. После установки (обновления) ПО уполномоченный сотрудник должен произвести настройку средств управления доступом к компонентам

данной задачи (программного средства) и совместно с пользователем должен проверить работоспособность ПО и правильность настройки средств защиты.

3.7. После завершения работ по внесению изменений в состав аппаратных средств защищенной рабочей станции, ее системный блок должен закрываться уполномоченным сотрудником Центра на ключ (при наличии штатных механических замков) или опечатываться (пломбироваться, защищаться) специальной наклейкой.

3.8. Уполномоченные исполнители работ должны произвести соответствующую запись в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств РС подразделения», сделать отметку о выполнении (на обратной стороне заявки, Приложение 2).

3.9. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств рабочей станции с отметками о внесении изменений в состав аппаратно-программных средств, должны храниться вместе с «Журналом учета…» у сотрудника, ответственного за техническое обслуживание рабочих станций.

3.10. Заявки в дальнейшем могут использоваться:

- для восстановления конфигурации РС после аварий;
- для контроля правомерности установки на конкретной рабочей станции средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты РС.

4. Техническое обслуживание и ремонт

4.1. При изъятии рабочей станции из состава рабочих станций учреждения, ее передача на техническое обслуживание, склад, в ремонт

осуществляется только после того, как уполномоченный специалист снимет с данной рабочей станции средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

4.2. Факт уничтожения защищаемых данных, находившихся на диске компьютера, оформляется актом за подписью ответственного за информационную безопасность (Приложение 3).

4.3. О факте выполнения данных работ ответственный за информационную безопасность учреждения делает соответствующую отметку в «Журнале учета…» с указанием признаков проявления ситуации, содержания выполненных работ по ее устранению или о необходимости привлечения к ремонту сотрудников сторонних организаций.

ПРИЛОЖЕНИЕ 1

Зам. директора Центра «Лидер»

_____
(резолюция)

“ _____ “ _____ 201__ года

ЗАЯВКА
на внесение изменений в состав аппаратно-программных средств рабочей станции

В связи с необходимостью _____

_____

_____

_____
(наименование задач)

на рабочей станции с инвентарным № _____ прошу произвести следующие изменения конфигурации аппаратно-программных средств

_____

_____

_____
(наименование изменений)

«___» _____ 201__ г.

Пользователь РС _____ _____
(подпись) (фамилия, инициалы)

Согласовано:

Ответственный за обеспечение информационной безопасности _____ _____
(подпись) (фамилия, инициалы)

ПРИЛОЖЕНИЕ 2

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 РС АС Центра «Лидер» рабочей группой в составе: _____

_____

_____

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

_____

краткое пояснение причины

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____	_____	_____
(должность)	(подпись)	(фамилия, инициалы)
_____	_____	_____
(должность)	(подпись)	(фамилия, инициалы)
_____	_____	_____
(должность)	(подпись)	(фамилия, инициалы)

ПРИЛОЖЕНИЕ 3

А К Т

о затирании остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД системного блока с инвентарным №_____, передаваемого с целью

_____
(цель передачи)

_____

_____
(куда и / или кому)

уничтожены посредством программы _____

«___» _____ 201__ г.

Ответственный за обеспечение информационной безопасности _____ _____
(подпись) (фамилия, инициалы)

ПРИЛОЖЕНИЕ № 4
к Сборнику инструкций
по обеспечению безопасности информационной
системы Некоммерческой организации
Межрегиональной ассоциации «Центр
дополнительного образования «Лидер»

ЛИСТ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ

С инструкциями ознакомлен:

№ п/п	Фамилия, имя, отчество работника	Дата	Подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			